Guía del usuario de

AWS Centro de seguridad

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Centro de seguridad: Guía del usuario de

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Las marcas comerciales y la imagen comercial de Amazon no se pueden utilizar en relación con ningún producto o servicio que no sea de Amazon, de ninguna manera que pueda causar confusión entre los clientes y que menosprecie o desacredite a Amazon. Todas las demás marcas registradas que no son propiedad de Amazon son propiedad de sus respectivos propietarios, que pueden o no estar afiliados, conectados o patrocinados por Amazon.

Table of Contents

¿Qué son Security Hub y el CSPM de Security Hub? ... 1
AWS Centro de seguridad ... 2
Características ... 2
Integraciones ... 3
Acceso a Security Hub ... 4
Conceptos ... 4
Estimador de costos ... 10
Acceso por tipo de cuenta ... 11
Requisitos previos ... 12
Configuración del acceso entre cuentas ... 13
Uso del estimador de costos ... 16
Notas importantes ... 24
Información relacionada ... 24
Habilitación de Security Hub ... 25
Habilite Security Hub para un AWS Organización ... 25
Habilitación de Security Hub en una cuenta independiente ... 28
Designación de un administrador delegado ... 29
Creación de la política de administrador delegado ... 30
Administrar la configuración de las cuentas de los miembros ... 32
Eliminación de un administrador delegado ... 37
Re-enabling Centro de seguridad ... 38
Recomendaciones ... 39
Cobertura de cuenta ... 40
Página de cobertura de cuentas ... 41
Widget de cobertura de seguridad ... 43
Plan extendido ... 43
Permisos para el plan extendido ... 43
Inscribirse para ser socios del plan Extended ... 44
Darse de baja de un socio ... 44
Cross-Region agregación ... 45
Tipos de datos que se agregan ... 45
Agregación de cuentas de administrador y de miembros ... 47
Reglas de automatización y agregación interregional ... 47
Habilitación de agregación ... 48

Revisión de la configuración de agregación ... 49
Actualización de la configuración de agregación ... 49
Eliminar la agregación ... 50
Integración con Azure ... 51
¿Cómo AWS Config se usa ... 53
Información adicional ... 53
Requisitos previos ... 54
Configuración de Azure ... 56
Configuración de Security Hub ... 67
Eliminar un conector de Azure ... 80
Panel Resumen ... 81
Consideraciones ... 81
Widgets disponibles ... 82
Filtros disponibles ... 96
Visualización de detalles sobre los recursos en Security Hub ... 97
Formato de búsqueda: OCSF ... 99
Descripción general de OCSF ... 99
Recursos relacionados ... 99
AWS extensión para OCSF ... 100
Resultados de cobertura ... 122
Hallazgos de cobertura para AWS CSPM de Security Hub ... 123
Hallazgos de cobertura para Amazon GuardDuty ... 123
Resultados de cobertura para Amazon Inspector ... 124
Resultados de cobertura de Amazon Macie ... 124
Supresión de los hallazgos de cobertura ... 125
Inventario de IA ... 125
Requisitos previos para el descubrimiento de IA autohospedado ... 126
Tipos de recursos de IA compatibles ... 126
Cómo encontrar recursos de IA en la página de recursos ... 127
Uso de la página de inventario de IA ... 128
Consideraciones ... 129
Acceder al inventario de IA con la API ... 129
Resultados de exposición ... 131
Cómo funcionan los resultados de exposición ... 132
Componentes de un hallazgo de exposición ... 132
Clasificación de gravedad ... 134

Beneficios de los hallazgos relacionados con la exposición 135
Fuentes de exposición: hallazgos 135
Prácticas recomendadas 136
Recursos admitidos 137
Condiciones admitidas 138
Generación de resultados de exposición 140
Cómo determinar el nivel de gravedad de un resultado de exposición 145
Cómo revisar los resultados de exposición 147
Gráfico de ruta potencial de ataque 149
Corrección de resultados de exposición 150
Resultados de acceso sin utilizar 261
Cómo funciona el análisis de acceso no utilizado 261
Tipos de búsqueda de acceso no utilizados 261
Service-linked analizador 262
Visualización de los resultados de acceso no utilizados 262
El acceso no utilizado aparece en los resultados de exposición 263
Recomendaciones de políticas para los permisos no utilizados 263
Precios 264
Recomendaciones de políticas 264
Cómo funcionan las recomendaciones de políticas 264
¿Quién puede generar recomendaciones 265
Ciclo vital de recomendaciones 265
Casos de error 265
Uso de la consola 266
Referencia de la API 266
Escaneo de red 266
Tipos de recursos admitidos 267
Habilite el escaneo de red 267
Cómo funciona el escaneo en red 269
Hallazgos del escaneo de redes 269
Escanea las pruebas 272
Excluir los recursos del escaneo 273
Puertos compatibles 273
Multi-cloud soporte 273
Disponibilidad por región 274
Deshabilite el escaneo de red 274

Automatizaciones ... 275
Reglas de automatización ... 276
EventBridge reglas de automatización ... 295
Third-party integraciones ... 3
Jira Cloud ... 304
ServiceNow ... 310
Políticas clave de KMS para las integraciones de venta de entradas ... 317
Probando las integraciones de venta de entradas ... 321
Aplicación MCP (versión preliminar) ... 323
Ejemplos de la aplicación MCP ... 324
Conceptos clave ... 327
Requisitos previos ... 328
Configuración del servidor MCP ... 328
Uso del diagnóstico del conector ... 329
Herramientas disponibles ... 330
Supervisar el uso y los costos ... 331
¿Quién puede acceder a la página de uso ... 331
Resumen de costos de la organización y la cuenta ... 332
Vista de capacidad ... 333
Vista de la cuenta ... 334
Estrategias de optimización de costos ... 335
Recursos relacionados ... 335
Deshabilitación de Security Hub ... 335
Desactivar Security Hub para una sola cuenta ... 335
Deshabilitar Security Hub en una organización ... 336
Seguridad ... 338
Protección de datos ... 339
Identity and Access Management ... 342
Validación de conformidad ... 376
Resiliencia ... 376
Seguridad de la infraestructura ... 376
Puntos de conexión de VPC (AWS PrivateLink) ... 377
Registro de llamadas a la API ... 379
Información sobre Security Hub en CloudTrail ... 379
Ejemplo: entradas del archivo de registros de Security Hub ... 380
AWS Centro de seguridad CSPM ... 384

Beneficios del CSPM de Security Hub ... 385
Acceso al CSPM de Security Hub ... 386
Servicios relacionados ... 388
Prueba gratuita, uso y precios del CSPM de Security Hub ... 388
Visualización de los detalles de uso ... 388
Información sobre precios ... 389
Conceptos ... 389
Habilitación del CSPM de Security Hub ... 395
Verificación de los permisos necesarios ... 396
Habilitación del CSPM de Security Hub con la integración de Organizations ... 396
Habilitación manual del CSPM de Security Hub ... 398
Próximos pasos: gestión de la posición e integraciones ... 400
Configurando AWS Config ... 401
Configuración local ... 407
Configuración centralizada ... 408
Administración de varias cuentas ... 459
Administrar cuentas conAWS Organizations ... 459
Administración manual de cuentas mediante invitación ... 460
Recomendaciones para entornos de varias cuentas ... 461
Administrar cuentas con AWS Organizations ... 463
Administración de cuentas por invitación ... 480
Acciones permitidas en las cuentas de administrador y de miembro ... 495
Efecto de las acciones de la cuenta en los datos ... 502
Agregar datos en las regiones ... 505
Tipos de datos que se agregan ... 506
Agregación de cuentas de administrador y de miembros ... 508
Configuración centralizada y agregación ... 509
Habilitación de agregación ... 510
Revisión de la configuración de agregación ... 512
Actualización de la configuración de agregación ... 514
Detención de la agregación ... 516
Estándares ... 518
Referencia de estándares ... 519
Habilitación de un estándar ... 617
Revisión de los detalles de un estándar ... 624
Desactivar los estándares con habilitación automática ... 628

Desactivación de un estándar ... 629
Controles ... 632
Vista de controles consolidados ... 633
Puntuación general de seguridad de los controles ... 634
Referencia de controles ... 635
Permisos para configurar los controles ... 1612
Habilitación de controles ... 1613
Deshabilitación de controles ... 1621
Controles y puntuaciones de seguridad ... 1633
Categorías de controles ... 1710
Cómo revisar los detalles de los controles ... 1714
Controles de filtrado y clasificación ... 1717
Parámetros de control ... 1718
Revisión y administración de resultados de controles ... 1734
Integraciones ... 1762
Revisión de una lista de integraciones ... 1764
Habilitación del flujo de resultados desde una integración ... 1765
Deshabilitación del flujo de resultados desde una integración ... 1766
Visualizar resultados desde una integración ... 1767
Servicio de AWS integraciones ... 1768
Third-party integraciones ... 1791
Integraciones de productos personalizados ... 1827
Integración con Azure ... 1829
¿Cómo AWS Config se usa ... 1831
Tipos de conectores ... 1831
Requisitos previos ... 1832
Configuración de Azure ... 1834
Configuración de Security Hub (CSPM) ... 1841
Eliminar un conector de Azure ... 1865
Hallazgos ... 1866
BatchImportFindings para encontrar proveedores ... 1868
BatchUpdateFindings para los clientes ... 1872
Revisión de los detalles y el historial de resultados ... 1875
Filtrado de resultados ... 1881
Agrupación de hallazgos ... 1883
Configuración del estado de flujo de trabajo de los resultados ... 1884

Envío de hallazgos a una acción personalizada 1887
Formato de resultados: ASFF 1888
Información 2189
Revisión de los productos de información y medidas al respecto 2190
Conocimientos administrados 2193
Información personalizada 2204
Automatizaciones 2212
Reglas de automatización 2213
Respuesta y corrección automatizadas 2239
Panel Resumen 2257
Widgets disponibles para el panel Resumen 2257
Filtrado del panel 2261
Personalización del panel de 2263
Límites regionales 2264
Cross-Region restricciones de agregación 2264
Disponibilidad de las integraciones por región 2265
Disponibilidad de los estándares por región 2267
Disponibilidad de los controles por región 2267
Límites regionales de los controles 2268
Crear recursos con CloudFormation 2558
Security Hub (CSPM) yCloudFormationplantillas 2559
Obtenga más información sobreCloudFormation 2559
Suscripción a los anuncios 2560
Formato de los mensajes de Amazon SNS 2565
Cómo desactivar el CSPM de Security Hub 2567
Seguridad 2570
Protección de datos 2571
Identity and Access Management 2572
Validación de conformidad 2609
Resiliencia 2609
Seguridad de la infraestructura 2609
Puntos de conexión de VPC (AWS PrivateLink) 2610
Registro de llamadas a la API 2612
Información sobre CSPM de Security Hub en CloudTrail 379
Ejemplo: entradas de archivos de registro del CSPM de Security Hub 380
Etiquetado de recursos 2616

Conceptos básicos del etiquetado 2616
Uso de etiquetas en políticas de IAM 2618
Adición de etiquetas a recursos 2619
Edición de etiquetas para recursos 2622
Revisión de etiquetas para recursos 2624
Eliminación de etiquetas de recursos 2626
Cuotas 2629
Cuotas máximas 2629
Cuotas de tarifas 2629
Historial de revisión 2630
..... mmdcclvii

¿Qué son Security Hub y el CSPM de Security Hub?

AWSSecurity Hub y AWS Security Hub CSPM Servicios de AWS protegen su entorno de nube. Estos servicios se complementan entre sí. Cuando se utilizan juntos, proporcionan información valiosa sobre el estado de seguridad de su AWS entorno.

El CSPM de Security Hub proporciona una visión integral de la posición de seguridad y ayuda a evaluar el entorno en la nube en relación con estándares y prácticas recomendadas del sector de la seguridad. Security Hub ofrece una experiencia unificada que permite priorizar y responder a problemas de seguridad críticos. Los resultados del CSPM de Security Hub se envían automáticamente a Security Hub, donde se correlacionan con resultados de otros servicios de seguridad, como Amazon Inspector, para generar exposiciones. Esto ayuda a identificar los riesgos más críticos en el entorno. Security Hub también ofrece funcionalidades de flujo de trabajo automatizado, que permiten incorporar los resultados del CSPM de Security Hub a los flujos de trabajo operativos.

Recomendamos habilitar ambos servicios. Puede habilitar el CSPM de Security Hub sin habilitar Security Hub si el objetivo principal es identificar configuraciones incorrectas y evaluar la posición de seguridad. Sin embargo, si habilita Security Hub sin habilitar el CSPM de Security Hub, Security Hub no podrá utilizar los resultados del CSPM de Security Hub para proporcionar información sobre riesgos y exposiciones en el entorno de AWS. Para una experiencia óptima, recomendamos no solo habilitar Security Hub y Security Hub CSPM, sino también habilitar estos otros servicios de seguridad: Amazon GuardDuty, Amazon Inspector y Amazon Macie.

Introducción a AWS Centro de seguridad

AWS Security Hub es una solución de seguridad en la nube unificada que prioriza sus problemas de seguridad críticos y le ayuda a responder a escala. Security Hub detecta los problemas de seguridad al correlacionar y enriquecer automáticamente las señales de seguridad de múltiples fuentes. Estas fuentes incluyen la gestión de la postura, la gestión de vulnerabilidades (Amazon Inspector), los datos confidenciales (Amazon Macie) y la detección de amenazas (Amazon). GuardDuty Utilice Security Hub para priorizar los riesgos activos en su entorno de nube mediante análisis automatizados y análisis contextuales. Mediante visualizaciones intuitivas, Security Hub transforma señales de seguridad complejas en información práctica que facilita la toma de decisiones fundamentadas sobre la posición de seguridad con rapidez. Security Hub también incorpora flujos de trabajo de respuesta automatizada que permiten remediar riesgos, mejorar la productividad de los equipos y reducir interrupciones operativas.

Características

Solución de seguridad unificada

Obtenga una mayor visibilidad del entorno en la nube mediante una administración centralizada dentro de una solución unificada de seguridad en la nube.

Información de seguridad procesable

Acceda a información de seguridad procesable con análisis avanzados que permiten identificar los riesgos asociados con el entorno.

Tiempos de respuesta reducidos

Optimice los tiempos de respuesta con flujos de trabajo automatizados y un sistema de tickets completamente integrado.

Resultados de exposición

Security Hub correlaciona los hallazgos de las comprobaciones de control del CSPM de Security Hub, Amazon Inspector y otros datos Servicios de AWS para detectar las exposiciones asociadas a los recursos. AWS

Análisis de acceso no utilizado

Security Hub identifica automáticamente las funciones, los usuarios, las claves de acceso y los permisos de IAM que no se han utilizado en un período retrospectivo de 90 días. Cuando habilitas Security Hub, el servicio crea un analizador de acceso de IAM vinculado a un servicio en tu cuenta. Los datos sobre el acceso no utilizado ayudan a implementar el acceso con privilegios mínimos al destacar los principales de IAM sobreaprovisionados. En el caso de los permisos no utilizados, Security Hub puede generar recomendaciones de políticas con privilegios mínimos que muestren una política de reemplazo limitada.

Los resultados usan el formato del Marco de Esquemas de Ciberseguridad Abiertos (OCSF)

Security Hub genera los hallazgos en OCSF y recibe los hallazgos en OCSF del CSPM de Security Hub y otros: Servicios de AWS

- Amazon GuardDuty
- Amazon Macie
- Amazon Inspector

Panel de control

La consola de Security Hub ofrece una vista completa de las exposiciones, amenazas, cobertura de seguridad y recursos. También incluye una visualización interactiva denominada gráfico de rutas de ataque, que muestra cómo los atacantes podrían acceder a recursos asociados con un resultado de exposición y tomar control de ellos.

Integraciones con productos de terceros

Puede fortalecer la posición de seguridad mediante las integraciones de Security Hub. Por ejemplo, si usa Jira Cloud o ServiceNow ITSM, puede usar esta característica para crear tickets a partir de los resultados.

Integraciones

Security Hub recibe las siguientes Servicios de AWS conclusiones.

- AWS Security Hub (CSPM).
- Amazon GuardDuty
- Amazon Inspector
- Amazon Macie

- Analizador de acceso de IAM

Acceso a Security Hub

Security Hub está disponible en la mayoría de AWS las regiones. Para obtener una lista de todas las regiones en las que Security Hub se encuentra actualmente disponible, consulte Puntos de conexión y cuotas de Security Hub en la Referencia general de AWS. Para obtener información sobre la administración Regiones de AWS de su cuenta Cuenta de AWS, consulte Especificar qué Regiones de AWS cuenta puede usar en la Guía de AWS Account Management referencia.

Puede habilitar Security Hub para cuentas individuales o para todas las cuentas de la organización. En cada región, puede acceder y utilizar Security Hub de cualquiera de las siguientes formas:

Consola de Security Hub

La consola Security Hub es una interfaz basada en un navegador que puede usar para crear y administrar AWS recursos. En esta consola, puede acceder a la cuenta, datos y recursos.

API de Security Hub

La API de Security Hub proporciona acceso mediante programación a la cuenta, datos y recursos. Puede enviar solicitudes HTTPS directamente a Security Hub.

AWS CLI

Con ella AWS CLI, puede ejecutar comandos en la línea de comandos del sistema para realizar tareas y crear scripts para realizar tareas. En algunos casos, AWS CLI puede resultar más útil que la consola de Security Hub.

AWS SDK

AWS Los SDK constan de bibliotecas y código de muestra para varios lenguajes de programación y plataformas (C++, Go, Java, .NET y Python). Proporcionan acceso programático a Security Hub y a otros Servicios de AWS en el idioma que prefieras y pueden ayudarte a gestionar tareas como la gestión de errores, la firma de solicitudes y el reintento de solicitudes.

Conceptos de Security Hub

En Security Hub, nos basamos en AWS conceptos y terminología comunes y utilizamos estos términos adicionales.

Cuenta

La AWS cuenta estándar que contiene tus AWS recursos. Inicie sesión AWS con su AWS cuenta para activar Security Hub.

Si su cuenta está inscrita AWS Organizations, su organización designa una cuenta de administrador de Security Hub. Esta cuenta puede habilitar otras cuentas de la organización como cuentas de miembro.

Una organización solo puede tener una cuenta administradora. Una cuenta no puede ser simultáneamente una cuenta administradora y una cuenta de miembro.

Security Hub es compatible con los siguientes tipos de cuentas:

- Cuenta de administración de la organización: una AWS cuenta que administra una AWS organización.
- Cuenta de administrador delegado: una AWS cuenta que administra el uso de una cuenta Servicio de AWS para una AWS organización.
- Cuenta de miembro: una AWS cuenta que es miembro de una AWS organización.
- Cuenta independiente: una AWS cuenta no AWS Organizations habilitada.

Cuenta de administrador

Este tipo de AWS cuenta puede ver los resultados de las cuentas de los miembros asociadas.

Este tipo de AWS cuenta se convierte en una cuenta de administrador cuando una cuenta de administración de la organización la designa como cuenta de administrador de Security Hub. La cuenta de administrador de Security Hub puede habilitar cualquier cuenta de la organización como cuenta de miembro y también puede invitar a otras cuentas a convertirse en cuentas de miembro.

Una organización solo puede tener una cuenta administradora. Una cuenta no puede ser simultáneamente una cuenta administradora y una cuenta de miembro.

Región de agregación

Una región de agregación le permite ver los resultados de seguridad de varias Regiones de AWS en un solo panel.

La región de agregación es Región de AWS donde puede ver y administrar los hallazgos. Los resultados se agregan en la región de agregación desde las regiones vinculadas. Los resultados actualizados se replican en las regiones.

En la región de agregación, las páginas del panel y del inventario incluyen datos de todas las regiones vinculadas. La página de automatizaciones solo se puede usar para definir reglas de automatización en la región de agregación. Third-party las integraciones de venta de entradas solo se pueden configurar en la región de agregación.

Resultado archivado

Un resultado con estado `ARCHIVED`. Estos resultados indican que el proveedor del resultado, o el cliente que investiga el resultado, considera que el resultado ya no es relevante.

Los proveedores que buscan pueden archivar los hallazgos que crean. Los clientes pueden archivar cualquier hallazgo que consideren que ya no es relevante utilizando la BatchUpdateFindingsV2 API de Security Hub o actualizando el estado en la consola de Security Hub.

En la consola de Security Hub, la configuración predeterminada de los filtros excluye los resultados archivados de las listas y tablas de resultados. Puede actualizar los filtros para incluir los resultados archivados. Si recupera los hallazgos mediante la operación GetFindings V2, la operación recupera los hallazgos archivados y activos. El siguiente ejemplo muestra cómo excluir resultados archivados de la salida.

```
{
    "StringFilters":
    [
        {
            "FieldName": "status",
            "Filter":
            {
                "Value": "Archived",
                "Comparison": "EQUALS"
            }
        }
    ]
}
```

Cross-Region agregación

La agregación de resultados y recursos de regiones vinculadas se dirige a una región de agregación. Puede ver todos los datos desde la región de agregación y actualizar los resultados desde la región de agregación.

Cuenta de administrador delegado

En AWS Organizations, la cuenta de administrador delegado de un servicio puede administrar el uso de un servicio para la organización.

En Security Hub, la cuenta de administrador de Security Hub también es la cuenta de administrador delegado de Security Hub. Cuando la cuenta de administración de la organización designa por primera vez la cuenta de administrador de Security Hub, Security Hub solicita a las organizaciones que conviertan esa cuenta en la cuenta de administrador delegado.

A continuación, la cuenta de administración de la organización debe elegir la cuenta de administrador delegado como cuenta de administrador de Security Hub en todas las regiones.

Exposure

Las exposiciones son debilidades más amplias en los controles de seguridad, errores de configuración u otras áreas que podrían aprovechar las amenazas activas.

Algunos ejemplos de exposiciones son:

- Plano de control mal configurado para un recurso.
- Presencia de una vulnerabilidad de software que tiene un alto potencial de explotación.
- Recurso de acceso público (red o API).

Resultado de exposición

Un tipo de resultado describe una exposición presente en el entorno. Un resultado de exposición incluye condiciones y señales. Una señal puede incluir uno o varios tipos de condiciones de exposición. AWS Security Hub genera un hallazgo de exposición cuando las señales de AWS Security Hub CSPM, Amazon Inspector, Amazon GuardDuty, Amazon Macie u otros AWS servicios indican la presencia de una exposición. Un recurso puede estar involucrado en uno o más hallazgos de exposición. Si un recurso no tiene ningún rasgo de exposición o tiene rasgos insuficientes, Security Hub no genera un resultado de exposición para ese recurso.

Un ejemplo de detección de exposición es: una instancia EC2 a la que se puede acceder desde Internet y que presenta vulnerabilidades de software que tienen una alta probabilidad de explotación.

Resultado

El registro observable de un control de seguridad o una detección relacionada con la seguridad. Security Hub genera y actualiza resultados al correlacionar otros resultados de seguridad. Estos

se conocen como resultados de exposición. Las conclusiones también pueden provenir de integraciones con productos de otros Servicios de AWS fabricantes o de terceros.

Ingesta de resultados

La importación de resultados a Security Hub. Los eventos de ingesta de resultados incluyen tanto resultados nuevos como actualizaciones de resultados existentes.

Región vinculada

Cuando habilita la agregación entre regiones, una región vinculada es aquella que envía los resultados y el inventario de recursos a la región de agregación.

En una región vinculada, el panel de control y las páginas de inventario solo contienen los resultados correspondientes. Región de AWS

Marco de ciberseguridad abierto (OCSF)

El marco del esquema abierto de ciberseguridad (OCSF) es un esfuerzo colaborativo AWS y de código abierto realizado por los principales socios del sector de la ciberseguridad. El OCSF proporciona un esquema estándar para los eventos de seguridad comunes, define los criterios de control de versiones para facilitar la evolución del esquema e incluye un proceso de autogobierno para los productores y consumidores de registros de seguridad. Para obtener más información, consulte Resultados en OCSF en Security Hub.

Cuenta de miembro

Y Cuenta de AWS que otorgó permiso a una cuenta de administrador para ver sus hallazgos y tomar medidas al respecto. Este tipo de cuenta Cuenta de AWS se convierte en una cuenta de miembro cuando la cuenta de administrador de Security Hub la habilita como cuenta de miembro.

Señales

Un resultado que contribuye a un resultado de exposición. Una señal puede denominarse un resultado que contribuye. Una señal puede originarse en Security Hub CSPM o en otro AWS Config Servicios de AWS, como Amazon Inspector.

Service-linked grabadora de configuración

Tipo de AWS Config grabador que se usa para registrar datos de configuración en recursos específicos de un servicio. Security Hub utiliza estas grabadoras con un enfoque basado en eventos para obtener elementos de configuración de recursos para el análisis de la exposición, la cobertura, los informes del inventario de recursos y las evaluaciones del control de la gestión de las posturas. Esta función se ofrece a todos los clientes de Security Hub como parte de los

precios del plan Essential. Después de habilitar Security Hub, se crean los siguientes grabadores de configuración vinculados a servicios en su cuenta:

- En cada uno Cuenta de AWS de ellos Región de AWS, se crea un grabador de configuración vinculado a un servicio denominado. `AWSConfigurationRecorderForSecurityHubAssets`
- Para los tipos de recursos globales, se crea un grabador de configuración vinculado a un servicio adicional denominado en el `AWSConfigurationRecorderForSecurityHubAssetsGlobal` us-east-1. Región de AWS
- Si Security Hub y Security Hub CSPM están habilitados en un Cuenta de AWS y Región de AWS, se crea un grabador de configuración vinculado a un servicio denominado. `AWSConfigurationRecorderForSecurityHubCSPM`

Para obtener más información, consulte Consideraciones sobre los grabadores de configuración vinculados a servicios y sobre el registro de recursos regionales y globales. https://docs.aws.amazon.com/config/latest/developerguide/select-resources.html#select-resources-all

Service-linked analizador

Un analizador de acceso de IAM que Security Hub crea y administra en su nombre. Al habilitar Security Hub, crea automáticamente un analizador de acceso no utilizado vinculado a un servicio para identificar las funciones, los usuarios, las claves de acceso y los permisos de IAM que no se han utilizado en un período retrospectivo de 90 días. El analizador funciona en el este de EE. UU. (Virginia del Norte) porque IAM es un servicio global. Security Hub replica los datos de acceso no utilizados en todas las regiones en las que haya activado Security Hub. No es necesario que habilites IAM Access Analyzer por separado ni que realices ninguna acción adicional. Esta función se ofrece a todos los clientes de Security Hub como parte de los precios del plan Essential. Puede ver el analizador vinculado al servicio en la consola de IAM Access Analyzer, pero no puede modificarlo ni eliminarlo mientras Security Hub esté activado. Security Hub elimina el analizador cuando se desactiva el servicio en todas las regiones de un. Cuenta de AWS Para obtener más información, consulte the section called “Resultados de acceso sin utilizar”.

Rasgo

Una desviación de seguridad que produce un resultado de exposición. Los tipos de condiciones incluyen: capacidad de asumir, configuración incorrecta, alcance, información confidencial y vulnerabilidad. Una condición se asocia con una señal, y una señal puede incluir varias condiciones. Por ejemplo, un control del CSPM de Security Hub indica que una política administrada por el cliente permite controlar el acceso administrativo. Esta señal incluye una condición de configuración incorrecta.

Resultado de acceso sin utilizar

Hallazgo que identifica un rol, usuario, clave de acceso o conjunto de permisos de IAM que no se ha utilizado en un período retrospectivo de 90 días. Security Hub genera los datos de acceso no utilizados mediante un analizador de acceso de IAM vinculado a un servicio. Hay cuatro tipos de hallazgos de acceso no utilizados: funciones de IAM no utilizadas, claves de acceso de usuario de IAM no utilizadas, contraseñas de usuario de IAM no utilizadas y permisos no utilizados.

AWS Estimador de costos de Security Hub

El estimador de costos de Security Hub es una función de consola que proporciona estimaciones de las capacidades de Security Hub en todo su entorno. AWS El estimador de costos le muestra cuáles son sus costos de servicio individuales en AWS Security Hub CSPM, Amazon Inspector y Amazon GuardDuty y cuáles serían sus costos estimados en Security Hub con los planes de precios simplificados de Security Hub. Puedes ajustar el uso estimado y el recuento de recursos para que coincidan con tu AWS uso y así aumentar la precisión de tu estimación. La calculadora de costos está disponible en todas las regiones en las que Security Hub está disponible.

El estimador de costos calcula los costos mensuales de las capacidades de seguridad mediante dos modelos de precios:

- Precios de servicios individuales: pague cada función de seguridad por separado (Amazon InspectorGuardDuty, Security Hub CSPM).
- Precios simplificados de Security Hub: precios unificados en 3 planes de precios: el plan Essentials con precios por recurso, el análisis de amenazas con precios por evento y registro por GB y el escaneo de código Lambda con precios por recurso.

El estimador usa los datos cuando están disponibles. AWS Cost Explorer Cuando los datos de Cost Explorer no estén disponibles, puede introducir manualmente los datos de uso. Las estimaciones de costos se basan en el uso observado y proporcionado por el usuario, así como en la información de precios públicos. Es posible que las estimaciones no reflejen los descuentos empresariales.

Los beneficios clave del estimador de costos incluyen:

- Vea cómo el costo de los precios unificados, al habilitar Security Hub, se compara con el costo de un servicio individual sin habilitar Security Hub
- Calcule los costos antes de habilitar las funcionalidades

- Ajuste los parámetros de uso para modelar diferentes escenarios
- Exporte las estimaciones en formato PDF para que las partes interesadas las revisen

Acceso por tipo de cuenta

> **Note**
>
> En el caso de las cuentas de administradores y miembros delegados, el estimador de costes se abre en modo de edición de forma predeterminada, lo que permite introducir inmediatamente los datos de uso. La cuenta de administración y las cuentas independientes se abren en modo de visualización cuando los datos de Cost Explorer están disponibles.

Esta función recupera automáticamente la información sobre el uso real en el pasado para estimar el costo de ciertos tipos de cuentas. Consulta la siguiente tabla para obtener detalles sobre cada uno de los tipos de cuenta y los datos disponibles para cada tipo de cuenta.

Permisos de acceso por tipo de cuenta

Account Type	Datos de Cost Explorer	Entrada de datos	Alcance
Cuenta de administración (MA)	Auto-populated	Anulación manual disponible	Organization-wide
Administrador delegado (DA)	Auto-populated mediante una función multicuenta*	La anulación manual está disponible	Organization-wide
Cuenta de miembro	Auto-populated mediante una función multicuenta*	La anulación manual está disponible	Organization-wide
Cuenta independiente (SA)	Auto-populated	Está disponible la anulación manual	Cuenta única

* Requiere la configuración de roles de IAM multicuenta en la cuenta de administración. Consulta la Configuración del acceso entre cuentas sección siguiente.

Requisitos previos

Permisos de IAM necesarios

Para usar todas las funciones del estimador de costos, el director de IAM debe tener los siguientes permisos:

Permisos de IAM necesarios para Cost Estimator

Operación de API	Servicio	Finalidad
`ce:GetCostAndUsage`	AWS Explorador de costos	Recupere datos históricos de uso y costos
`pricing:GetProducts`	AWS ¿Precios	Obtenga las tarifas de precios actuales
`organizations:ListAccounts`	AWS Organizaciones	Cuenta las cuentas de la organización
`organizations:DescribeOrganization`	AWS Organizaciones	Determine el tipo de cuenta
`securityhub:ListOrganizationAdminAccounts`	Centro de seguridad	Listar las cuentas de administrador de la organización
`iam:GetRole`	IAM	Comprueba la existencia de roles multicuenta (solo en la cuenta de administración) *
`sts:AssumeRole`	IAM	Asume el rol multicuenta (solo en la administrator/Member cuenta delegada) **

* Solo es obligatorio para que los usuarios de cuentas de administración verifiquen el estado de las funciones multicuenta.

** Solo es obligatorio para las cuentas de administrador delegado y miembros de la organización que utilizan el acceso multicuenta.

Requisitos adicionales

Explorador de costos

Debe estar habilitada para la reposición automática de datos (demora de procesamiento de 24 horas después de la activación).

Configuración del acceso entre cuentas

Los administradores delegados y las cuentas de los miembros pueden acceder a los AWS Cost Explorer datos de toda la organización desde la cuenta de administración mediante la configuración de una función de IAM multicuenta. Esta configuración permite a estas cuentas ver los datos de uso reales sin tener que cambiar a la cuenta de administración.

Requisitos previos

Se necesitan los siguientes elementos e información antes de configurar el acceso multicuenta al estimador de costos:

- La cuenta de administración debe estar habilitada. AWS Cost Explorer
- Permisos de IAM para crear funciones en la cuenta de administración.
- Conocer el ID de la cuenta de miembro o administrador delegado a la que se concederá el acceso multicuenta.

Pasos de configuración

El estimador de costos proporciona instrucciones de configuración guiadas directamente en la consola. Para acceder a las instrucciones, diríjase a la página del estimador de costos en https://console.aws.amazon.com/securityhub/v2/home #/CostEstimator en la cuenta de administración de su organización. Busque la sección de Cross-account acceso y siga los pasos descritos para configurar la función multicuenta.

Configuración de roles

El acceso multicuenta al estimador de costes requiere configurar una función de IAM con una política de confianza y una política de permisos. El rol multicuenta se debe crear en la cuenta de administración con la siguiente configuración:

Nombre del rol (se requiere el nombre exacto) — AwsSecurityHubCostEstimatorCrossAccountRole

Política de confianza recomendada:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
            "AWS": "arn:aws:iam::{ACCOUNT_ID}:role/{ROLE_NAME}"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Edite la política sustituyendo los siguientes valores en el ejemplo de política:

- *{ACCOUNT_ID}*Sustitúyalo por el ID de la cuenta de administrador delegado o miembro a la que está concediendo acceso multicuenta.
- *{ROLE_NAME}*Sustitúyalo por el nombre del rol de IAM en la cuenta de miembro o administrador delegado a la que está concediendo acceso.

Política de permisos recomendada:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ce:GetCostAndUsage",
            "Resource": "*"
        }
```

```
    ]
}
```

> **Note**
>
> La política de confianza restringe el acceso a una cuenta y un rol específicos. Solo el director de IAM especificado puede asumir esta función, lo que impide el acceso no autorizado.

Verificación

Tras crear el rol en la cuenta de administración, siga los pasos siguientes para confirmar que la configuración funciona.

1. Inicie sesión en la cuenta de administrador delegado o miembro.
2. Diríjase al estimador de costos de Security Hub en #/CostEstimator https://console.aws.amazon.com/securityhub/v2/home
3. La página debería:
   a. Detecta la cuenta de administración de tu organización.
   b. Asume la función multicuenta.
   c. Cargue los datos de Cost Explorer para usarlos en toda la organización.

Si se realiza correctamente, aparecen los datos de uso reales en lugar de los campos de entrada manual.

Resolución de problemas

En esta sección se describen los problemas y las soluciones más comunes que pueden surgir al configurar el acceso entre cuentas.

Los datos de uso organizacional no están disponibles para esta cuenta

Esta alerta indica que no se puede acceder al rol multicuenta. Las posibles causas de esta alerta son:

1. El rol no existe: la cuenta de administración aún no ha creado el rol.

- Solución: póngase en contacto con el administrador de su cuenta de administración para crear el rol siguiendo las instrucciones de configuración.

2. El nombre del rol no coincide: el nombre del rol no coincide exactamente.

   - Solución: compruebe que el nombre del rol `esAwsSecurityHubCostEstimatorCrossAccountRole`.

3. Política de confianza incorrecta: la política de confianza no permite que su cuenta asuma la función.

   - Solución: compruebe que la política de confianza incluya el identificador de su cuenta y el nombre del rol.

4. Falta el AssumeRole permiso: su director de IAM no `sts:AssumeRole` lo tiene.

   - Solución: póngase en contacto con el administrador para añadir el `sts:AssumeRole` permiso.

Para ver las instrucciones de configuración detalladas: seleccione Ver instrucciones en la alerta para abrir un modal con plantillas de políticas y guías paso a paso.

Solución alternativa: Puedes seguir usando el estimador de costos introduciendo manualmente los valores de uso en el modo de edición.

Uso del estimador de costos

Acceder al estimador de costos

Para acceder al estimador de costos desde la página de inicio de Security Hub

1. Inicie sesión en su AWS cuenta con las credenciales de la cuenta de administración delegada o de administración de su AWS organización. Abra la consola de Security Hub en la región us-east-1 en. https://console.aws.amazon.com/securityhub/v2/home
2. En la página de inicio, localiza la tarjeta de precios.
3. Selecciona Estimar el costo.

Para acceder al estimador de costos durante los pasos de activación y configuración de Security Hub

1. Busque los precios en la nueva tarjeta de Security Hub de la interfaz de incorporación.

2. Selecciona Ver estimaciones.

Para acceder al estimador de costos desde las consolas GuardDuty CSPM de Amazon Inspector o Security Hub

1. Diríjase al panel de control del servicio o a la página de resumen.
2. Selecciona Comparar precios en la tarjeta de información de precios.

Comprender la interfaz del estimador de costos

Diseño de página

La página del estimador de costos contiene tres secciones principales:

- Sección de información general: explica los beneficios de la administración unificada de la seguridad y la optimización de costos.
- Información de precios: panel ampliable con categorías de capacidad y niveles de precios.
- Tabla comparativa de precios: comparación de Side-by-side costos con detalles de capacidad.

Tabla de comparación de precios

El encabezado de la tabla incluye controles de view/edit modo y una opción de reinicio. La tabla muestra los costos en dos columnas:

- Servicios individuales: costos actuales o estimados de los distintos servicios de seguridad.
- Security Hub: costos estimados mediante un modelo de precios simplificado.

Región de precios

La primera columna muestra la información contextual de precios, incluida una nota en la que se indica que las estimaciones utilizan los precios de us-east-1 para los cálculos. Una insignia indica que los descuentos empresariales no están incluidos en las estimaciones.

Visualización de las estimaciones de costos

Al usar el estimador de costos, puede ver, editar, restablecer y exportar las estimaciones.

El estimador de costos se abre en modo de visualización de forma predeterminada.

Para ver las estimaciones de costos

1. Acceda al estimador de costos mediante uno de los métodos descritos en. Acceder al estimador de costos
2. Revise los costos mensuales totales en la fila de resumen.
3. Revise los grupos de capacidades y sus desgloses detallados de costos.
4. Elija los nombres de las capacidades para ver las descripciones en una ventana emergente.

Fuentes de datos en modo de visualización

El estimador muestra datos de varias fuentes, indicadas mediante etiquetas:

- Predeterminado: datos de AWS Cost Explorer (los últimos 30 días).
- $-/mes: los datos de costos no están disponibles (se muestran cuando el acceso a Cost Explorer no está disponible).
- Uso personalizado: valores. User-entered
- No habilitado: se muestra cuando los permisos de Cost Explorer no existen.

Account-specific comportamiento

A continuación se describe cómo funciona el estimador de costos en diferentes tipos de cuentas y configuraciones.

Cuentas de administrador y miembro delegados

Con el acceso multicuenta configurado:

- Los datos de Cost Explorer están disponibles para su uso en toda la organización.
- Se abre en modo de visualización de forma predeterminada (igual que la cuenta de administración). Puede cambiar al modo de edición para modificar las estimaciones.

Sin configurar el acceso entre cuentas:

- Aparece la alerta: «Los datos de uso de la organización no están disponibles para esta cuenta».
- Se abre en modo de edición de forma predeterminada para la entrada manual.
- Selecciona Ver instrucciones en la alerta para obtener información sobre la configuración.

Cuenta de administración

Con la función multicuenta creada:

- La sección «Cross-account acceso» muestra el estado configurado.
- Muestra las políticas recomendadas para la verificación.
- Proporciona un enlace para ver el rol en la consola de IAM.

Sin crear un rol multicuenta:

- La sección «Cross-account acceso» muestra la guía de configuración.
- Proporciona instrucciones paso a paso con políticas rellenadas previamente.
- Enlace directo a la consola de IAM para la creación de funciones.

No se puede verificar el estado del rol:

- Si no hay permiso para llamar`iam:GetRole`, la consola no puede determinar si ha creado el rol necesario.
- Muestra el mensaje «No se puede verificar» con el mensaje de error correspondiente.

Cuenta independiente

Sin la creación de un rol multicuenta:

- Sin cambios en el comportamiento existente.
- Los datos de Cost Explorer están disponibles cuando están habilitados.
- Se abre en modo de visualización de forma predeterminada.

Edición de valores de uso

El modo de edición le permite modificar los valores de las dimensiones y ver las actualizaciones de costos en tiempo real.

Para editar los valores de uso

1. Seleccione Editar en el encabezado de la tabla.

2. Introduzca valores en los campos de entrada de dimensiones.
3. Vea los costos actualizados automáticamente.
4. Seleccione Ver para volver al modo de visualización.

> **Important**
>
> - Las modificaciones no se guardan al salir de la página del estimador de costos
> - Las estimaciones modificadas utilizan los precios de EE. UU. (Virginia del Norte) y no incluyen descuentos para empresas
> - La edición en el modo «Mostrar solo el costo actual» vuelve automáticamente al modo estimado

Restablecer el estimador

Esta acción borra todos los valores personalizados y vuelve a cargar los datos predeterminados del Explorador de costos.

Para restablecer todos los valores a los valores predeterminados

1. Seleccione Restablecer en la cabecera de la tabla.
2. En el cuadro de diálogo de confirmación, seleccione Restablecer.

Exportación de estimaciones

Mientras esté en el estimador de costos, los datos de su estimación se pueden exportar a un archivo PDF.

Para exportar las estimaciones de costos

1. Asegúrese de estar en modo de visualización.
2. Selecciona Descargar PDF en el encabezado de la página.

El PDF se descarga automáticamente con el nombre del archivo:`SecurityHub-Cost-Estimate-YYYY-MM-DD.pdf`.

Resolución de problemas

En esta sección se describen los problemas y las soluciones más comunes que pueden surgir al usar el estimador de costos

No hay datos disponibles en Cost Explorer

Problema

La alerta muestra el mensaje «No hay datos de costo disponibles para su cuenta».

Soluciones por tipo de cuenta

La solución depende del tipo de cuenta:

Soluciones para los datos faltantes de Cost Explorer

Account Type	Solución
Cuenta de administración	Habilite Cost Explorer y espere 24 horas para que se procesen los datos
Administrador delegado	Póngase en contacto con el administrador de la cuenta de administración para solicitar el acceso
Cuenta de miembro	Póngase en contacto con la cuenta de administración o con el administrador delegado para acceder
Cuenta independiente	Habilite Cost Explorer y espere 24 horas para procesar los datos

Solución

Introduzca valores personalizados en el modo de edición.

Cross-account el acceso no funciona

Problema

La cuenta de administrador delegado o miembro muestra la alerta «Los datos de uso de la organización no están disponibles para esta cuenta».

Revisa las siguientes causas comunes y sus soluciones:

Cross-account el rol no existe en la cuenta de administración

Póngase en contacto con el administrador de la cuenta de administración para crear el rol. El estimador de costos proporciona instrucciones de configuración guiadas para los usuarios de cuentas de administración.

El nombre del rol no coincide exactamente

Nombre de rol requerido:`AwsSecurityHubCostEstimatorCrossAccountRole`. Verifique que el nombre del rol en la consola de IAM coincida exactamente (distingue entre mayúsculas y minúsculas).

La política de confianza no permite tu cuenta

Verifique que el director de la política de confianza incluya su ID de cuenta y su nombre de rol. Formato: `arn:aws:iam::{YOUR_ACCOUNT_ID}:role/{YOUR_ROLE_NAME}`.

Falta el AssumeRole permiso

Compruebe que el director de IAM tiene `sts:AssumeRole` permiso. Póngase en contacto con su AWS administrador para añadir este permiso.

Solución:

Introduzca valores personalizados en el modo de edición para estimar los costos manualmente sin los datos de Cost Explorer.

Obtener instrucciones detalladas

- Selecciona Ver las instrucciones de la alerta para abrir un modal con:
  - Step-by-step guía de configuración
  - Plantillas de política de Pre-populated
  - Consejos para la solución de problemas específicos para su error

Errores de permisos

Problema

Error de «acceso denegado» para operaciones de API específicas.

Para resolver errores de permisos

1. Observe la operación denegada que aparece en el mensaje de error (por ejemplo,`ce:GetCostAndUsage`).
2. Seleccione Copiar para copiar los detalles del error.
3. Envíe los detalles del error a su AWS administrador.
4. Solicita los permisos de IAM necesarios que figuran enPermisos de IAM necesarios.

> **Note**
>
> Puedes seguir usando el modo de edición para introducir valores de forma manual cuando falten los permisos, excepto cuando se deniegue el acceso a la API de precios (lo que impide cualquier estimación de costes).

La función muestra el mensaje «No habilitada»

Problema

La capacidad muestra el estado «No habilitada».

Explicación

Este estado aparece cuando tiene acceso a Cost Explorer, pero la capacidad no está activa actualmente. Si en su lugar aparece $-/mes, significa que los datos de Cost Explorer no están disponibles para su tipo de cuenta.

Para ver las estimaciones de costos

1. Seleccione Editar para entrar en el modo de edición.
2. Introduzca los valores de dimensión de la capacidad.
3. Vea las estimaciones de costos actualizadas.

La capacidad muestra «No aplicable»

Problema

La capacidad muestra el mensaje «No aplicable» en la columna de servicios individuales.

Explicación

Esta capacidad solo está disponible a través de los precios simplificados de Security Hub, no como un servicio independiente.

Los costos modificados no coinciden con Cost Explorer

Problema

Los costos editados difieren de los valores originales del Explorador de costos.

Explicación

Las estimaciones modificadas utilizan las tarifas de precios de EE. UU. (Virginia del Norte) y no incluyen los descuentos para empresas. Los datos de Cost Explorer reflejan los costos reales con los descuentos aplicables.

Notas importantes

- Las estimaciones se basan en el uso observado y proporcionado por el usuario, y en la información pública sobre precios. Los costos reales pueden variar según los patrones de uso y los acuerdos empresariales
- Análisis retrospectivo de 30 días: los datos de Cost Explorer reflejan los últimos 30 días de uso
- Región de precios: todas las estimaciones utilizan las tarifas de EE. UU. East-1 (Virginia del Norte)
- Sin impacto en la configuración: los cambios en el estimador no afectan a las configuraciones actuales de Security Hub o de los servicios
- Descuentos para empresas: las estimaciones modificadas no incluyen los descuentos para empresas; solo los datos de Cost Explorer reflejan los costos con descuento reales
- Actualización de datos: los datos de Cost Explorer se actualizan a diario; actualiza la página para ver los datos más recientes

Información relacionada

- AWS Precios de Security Hub
- AWS Guía del usuario de Cost Explorer
- AWS Referencia de la API de precios

- Activación de Security Hub

Habilitación de Security Hub

Puede habilitar Security Hub para cualquier Cuenta de AWS. En esta sección de la documentación se describen todos los pasos necesarios para habilitar Security Hub para una AWS organización o una cuenta independiente.

Para ver una breve demostración de cómo habilitar Security Hub, vea el siguiente vídeo: Tutorial y demostración de la incorporación de Security Hub.

Habilite Security Hub para un AWS Organización

Esta sección incluye tres pasos:

- En el paso 1, la cuenta de administración de la AWS organización designa un administrador delegado para su AWS organización, crea la política de administrador delegado y, de forma opcional, habilita Security Hub para su propia cuenta.
- En el paso 2, el administrador delegado de la organización habilita Security Hub para su propia cuenta.
- En el paso 3, el administrador delegado de la organización configura todas las cuentas de los miembros de la organización para Security Hub y otros servicios de seguridad compatibles.

Paso 1. Delegar una cuenta de administrador y, si lo desea, habilitar Security Hub en AWS cuenta de administración de la organización

> **Note**
>
> Complete este paso en una región de la cuenta de administración de la organización.

Al asignar la cuenta de administrador delegado a Security Hub, la cuenta que puede elegir para su administrador delegado depende de cómo haya configurado un administrador delegado para Security Hub CSPM. Si ha configurado un administrador delegado para Security Hub CSPM y esa cuenta no es la cuenta de administración de la organización, esa cuenta se establece automáticamente como administrador delegado de Security Hub y no se puede elegir una cuenta diferente. Si la cuenta de administrador delegado para Security Hub CSPM está configurada como la cuenta de administración de la organización o no está configurada en absoluto, puede elegir qué cuenta asignar como cuenta de administrador delegado de Security Hub, excepto la cuenta de administración de la organización.

Para obtener información sobre cómo designar un administrador delegado en Security Hub, consulte Cómo designar una cuenta de administrador delegado en Security Hub. Para obtener información sobre cómo crear la política del administrador delegado en Security Hub, consulte Creación de la política del administrador delegado en Security Hub.

Para designar un administrador para Security Hub

1. Inicia sesión en tu AWS cuenta con las credenciales de la cuenta de administración de tu AWS organización. Abra la consola de Security Hub en https://console.aws.amazon.com/securityhub/v2/home.
2. En la página de inicio de Security Hub, seleccione Security Hub y, a continuación, elija Comenzar.
3. En la sección Administrador delegado, elige una cuenta de administrador según las opciones proporcionadas. Como práctica recomendada, utilice el mismo administrador delegado en todos los servicios de seguridad para lograr una gobernanza uniforme.
4. Seleccione la casilla Acceso confiable. Al elegir esta opción, la cuenta de administrador delegado puede configurar determinadas funciones, como la protección contra GuardDuty malware, en las cuentas de los miembros. Si desmarca esta opción, Security Hub no podrá habilitar estas funciones en su nombre y deberá habilitarlas directamente a través del servicio al que esté asociada la función.

5. (Opcional) Para habilitar la cuenta, selecciona la casilla para habilitar Security Hub en tu cuenta. AWS
6. En el caso de la política de administrador delegado, elige una de las siguientes opciones para añadir la declaración de política.
   a. (Opción 1) Seleccione Actualizar esto por mí. Seleccione la casilla situada debajo de la declaración de política para confirmar que Security Hub crea automáticamente una política de delegación que otorga todos los permisos necesarios al administrador delegado.
   b. (Opción 2): Elija Quiero asociar esto manualmente. Elija Copiar y asociar. En la AWS Organizations consola, en Administrador delegado para AWS Organizations, seleccione Delegar y pegue la política de recursos en el editor de políticas de delegación. Seleccione Crear política. Abra la pestaña donde se encuentra en la consola de Security Hub.
7. Elija Configurar.

Paso 2. Habilitación de Security Hub en la cuenta del administrador delegado

La cuenta de administrador delegado completa este paso. Una vez que la cuenta de administración de la AWS organización designe a un administrador delegado para su organización, el administrador delegado debe habilitar Security Hub para su propia cuenta antes de habilitarlo para toda la AWS organización.

Para habilitar Security Hub en la cuenta del administrador delegado

1. Inicie sesión en su AWS cuenta con sus credenciales de administrador delegado. Abra la consola de Security Hub en https://console.aws.amazon.com/securityhub/v2/home.
2. En la página de inicio de Security Hub, seleccione Comenzar.
3. En la sección de capacidades de seguridad se describen las funciones que se habilitan automáticamente y se incluyen en el precio base por recurso de Security Hub.
4. (Opcional) En Etiquetas, determine si desea agregar un par clave–valor durante la configuración de la cuenta.
5. Seleccione Habilitar Security Hub para terminar de habilitar Security Hub.
6. (Recomendado) en la ventana emergente, seleccione Configurar mi organización y continúe con el paso 3.

Paso 3. Creación de una política que habilite Security Hub en todas las cuentas de miembro

Tras habilitar Security Hub en la cuenta de administrador delegado de una organización, debe crear una política que defina qué servicios y capacidades están habilitados en las cuentas de los miembros de la organización. Para obtener más información, consulte Habilitar una configuración con un tipo de política.

Después de habilitar Security Hub, se crean los siguientes recursos en su cuenta:

- Un rol vinculado a un servicio llamado. AWSServiceRoleForSecurityHubV2
- Service-linked grabadoras de configuración. Consulte la Service-linked grabadora en la documentación conceptual de Security Hub para obtener más información.
- Un analizador vinculado a un servicio. Consulte el Service-linked analizador en la documentación conceptual de Security Hub para obtener más información.

Habilitación de Security Hub en una cuenta independiente

Este procedimiento describe cómo habilitar Security Hub en una cuenta independiente. Una cuenta independiente es aquella Cuenta de AWS que no ha habilitado AWS a las organizaciones.

Para habilitar Security Hub en una cuenta independiente

1. Inicia sesión en tu AWS cuenta con las credenciales de tu cuenta. Abra la consola de Security Hub en https://console.aws.amazon.com/securityhub/v2/home.
2. En la página de inicio de Security Hub, seleccione Comenzar.
3. En la sección Capacidades de seguridad, realice una de las siguientes acciones:
   a. (Opción 1) Elija Habilitar todas las capacidades. Esto activa todas las capacidades esenciales de Security Hub, el análisis de amenazas y las capacidades adicionales.
   b. (Opción 2) Elija Personalizar capacidades. Seleccione las funciones que desee activar en las secciones Administración de la seguridad, Análisis de amenazas y Gestión de vulnerabilidades. No puede deseleccionar ninguna de las funciones que formen parte de las funciones esenciales del plan Security Hub.
4. En la sección Regiones, elija Habilitar todas las regiones o Habilitar regiones específicas. Si selecciona Habilitar todas las regiones, puede decidir si desea habilitar automáticamente las

nuevas regiones. Si eliges Habilitar regiones específicas, debes elegir qué regiones quieres habilitar.

5. (Opcional) En el caso de las etiquetas de recursos, añada etiquetas como pares clave-valor para poder identificar fácilmente la configuración.
6. Seleccione Habilitar Security Hub.

Después de habilitar Security Hub, se crean los siguientes recursos en cada cuenta en la que haya habilitado el servicio:

- Un rol vinculado a un servicio llamado. AWSServiceRoleForSecurityHubV2
- Service-linked grabadoras de configuración. Consulte la Service-linked grabadora en la documentación conceptual de Security Hub para obtener más información.
- Un analizador vinculado a un servicio. Consulte el Service-linked analizador en la documentación conceptual de Security Hub para obtener más información.

Designación de un administrador delegado en Security Hub

En la cuenta de administración de la AWS organización, puedes designar un administrador delegado para tu organización. Como práctica recomendada, utilice el mismo administrador delegado en todos los servicios de seguridad para lograr una gobernanza uniforme.

El procedimiento de este tema describe cómo designar un administrador delegado en Security Hub. Se presupone que se ha habilitado previamente Security Hub, pero no se ha designado un administrador delegado durante el flujo de trabajo de habilitación.

Consideraciones

Considere lo siguiente al designar un administrador delegado en Security Hub:

- La cuenta de administración de la AWS organización puede designarse a sí misma como administradora delegada en Security Hub CSPM, pero no puede designarse a sí misma como administradora delegada en Security Hub. En este escenario, la cuenta de administración debe designar a otro Cuenta de AWS como administrador delegado en Security Hub.
- Si la cuenta de administración de la AWS organización designa a un administrador delegado en Security Hub CSPM, ese administrador delegado se convierte automáticamente en administrador delegado en Security Hub. En este escenario, Security Hub solo permite que esta persona Cuenta de AWS actúe como administrador delegado.

> **Note**
>
> Al eliminar al administrador delegado mediante la consola CSPM de Security Hub, la consola de Security Hub o la AWS Organizations API, se elimina de ambos servicios. Cuando el administrador delegado se elimina del CSPM de Security Hub, Central Configuration se desactiva automáticamente.

Designación de un administrador delegado después de habilitar Security Hub

Este procedimiento debe completarse con la cuenta de administración de AWS la organización. Supone que la cuenta de administración de la AWS organización habilitó anteriormente Security Hub, pero no designó a un administrador delegado durante el flujo de trabajo de activación.

> **Note**
>
> Después de completar este procedimiento, debe crear una política que permita al administrador delegado de la organización configurar Security Hub y realizar acciones específicas en AWS Organizations. Para obtener más información, consulte Creación de la política de administrador delegado en Security Hub.

Para designar un administrador delegado en Security Hub

1. Inicie sesión en su AWS cuenta con las credenciales de la cuenta de administración de su organización y abra la consola de Security Hub en. https://console.aws.amazon.com/securityhub/v2/home
2. En el panel de navegación, seleccione General.
3. En Administrador delegado, elija Configurar. Selecciona una de las indicadas Cuentas de AWS o introduce el Cuenta de AWS número de 12 dígitos del número Cuenta de AWS que quieres designar como administrador delegado de tu organización. Seleccione Save.

Creación de la política de administrador delegado en Security Hub

La cuenta de administración de la AWS organización puede crear una política que permita al administrador delegado configurar Security Hub y realizar acciones específicas en él AWS Organizations. El procedimiento de este tema describe cómo crear la política. Al completar

el procedimiento, puede: permitir que Security Hub cree la política en su nombre, o crearla manualmente. Permita que Security Hub cree la política, a menos que desee personalizarla para un caso de uso concreto.

Complete este procedimiento solo si la cuenta de administración de la organización habilitó Security Hub y designó a un administrador delegado, pero omitió la creación de la política durante el flujo de trabajo de activación. Para obtener información sobre cómo actualizar esta política, consulte Actualización de una política de delegación basada en recursos con AWS Organizations en la Guía del usuario de AWS Organizations .

> **Note**
>
> Tras completar este procedimiento, el administrador delegado puede crear una política para administrar las cuentas de los miembros de su organización. Para obtener más información, consulte Creación de una política como administrador delegado para administrar cuentas de miembro.

Para crear la política de administrador delegado

1. Inicia sesión en tu AWS cuenta con las credenciales de la cuenta de administración de tu organización. Abra la consola de Security Hub en https://console.aws.amazon.com/securityhub/v2/home.
2. En el panel de navegación, seleccione General.
3. En Política de administrador delegado, haga una de las siguientes acciones:
   - Elija Crear política. Seleccione la casilla situada debajo de la declaración de política para confirmar que Security Hub crea automáticamente una política de delegación que otorga todos los permisos necesarios al administrador delegado.
   - Abra la política . Elija Copiar y asociar. En la AWS Organizations consola, en Administrador delegado para AWS Organizations, seleccione Delegar y pegue la política de recursos en el editor de políticas de delegación. Seleccione Crear política. Abra la pestaña en la que se encuentra en la consola de Security Hub y elija Configurar.

Administrar la configuración de las cuentas de los miembros en un AWS Organización

El administrador delegado de una AWS organización puede configurar las capacidades de seguridad en las cuentas de los miembros y las regiones. Hay dos tipos de configuraciones disponibles: políticas e implementaciones. Las políticas generan políticas de AWS organización para cuentas y regiones para AWS Security Hub y Amazon Inspector. Las implementaciones son una acción que se realiza una sola vez para habilitar la capacidad de seguridad en las cuentas y regiones seleccionadas de Amazon GuardDuty y AWS Security Hub CSPM. A diferencia de las políticas, no puedes ver ni editar las implementaciones y las implementaciones no se aplican a las cuentas recién habilitadas. Como alternativa, las funciones de activación automática para las nuevas cuentas de miembros están disponibles en Amazon GuardDuty y AWS Security Hub CSPM.

Catálogo de configuración de Security Hub

El catálogo de configuración de Security Hub ofrece varias opciones para ayudar a configurar las cuentas de su AWS organización de acuerdo con las funciones de seguridad que ofrece Security Hub.

Las siguientes son las opciones disponibles en el catálogo de configuración de Security Hub.

Security Hub (funciones esenciales y adicionales)

Esta es la configuración recomendada para implementar en Security Hub.

Tipo: Política e implementaciones

Descripción: Esta configuración activa las capacidades esenciales de administración de la seguridad, administración de posturas, análisis de amenazas y administración de vulnerabilidades de Security Hub. De forma opcional, habilita capacidades adicionales.

Análisis de amenazas de GuardDuty

Tipo: Despliegue

Descripción: Active determinadas GuardDuty funciones de Amazon para supervisar, analizar y procesar de forma continua las fuentes de AWS datos y los registros de su AWS entorno.

Gestión de la postura desde AWS CSPM de Security Hub

Tipo: Despliegue

Descripción: Esta configuración activa los estándares y controles de Security Hub CSPM, que detectan si sus AWS cuentas y recursos se desvían de las prácticas recomendadas de seguridad.

Gestión de vulnerabilidades desde Amazon Inspector

Tipo: Política

Descripción: Esta configuración activa determinadas funciones de Amazon Inspector, que detectan automáticamente las cargas de trabajo, las instancias, las imágenes de contenedores y otros recursos, y los escanean en busca de vulnerabilidades y exposición a la red.

Habilitar una configuración con un tipo de política

El siguiente procedimiento describe cómo crear una configuración con un tipo de política para las cuentas de su AWS organización. Para crear una política de configuración, primero debes crear la política de administrador delegado en la cuenta de administración de la AWS organización. Para obtener información sobre cómo crear la política del administrador delegado en Security Hub, consulte Creación de la política del administrador delegado en Security Hub.

Para crear una política que habilite y desactive cuentas de miembro

1. Inicia sesión con tu AWS cuenta con tus credenciales de administrador delegado. Abra la consola de Security Hub en https://console.aws.amazon.com/securityhub/v2/home.
2. En el panel de navegación, seleccione Administración y, a continuación, seleccione Configuraciones.
3. Elija un elemento con un tipo de política o política e implementación del catálogo de configuraciones. Para configurar Security Hub por completo, elija Security Hub (funciones esenciales y adicionales).
4. En la página Configurar Security Hub, en la sección Detalles, introduzca un nombre y una descripción para la política.
5. En la sección Capacidades de seguridad, elija una de las siguientes opciones:
   - Habilitar todas las funciones: activa todas las funciones esenciales de Security Hub, el análisis de amenazas y las funciones adicionales.
   - Personalice las capacidades: seleccione las capacidades de las secciones Administración de la seguridad, Análisis de amenazas y Administración de vulnerabilidades. No puede deseleccionar las capacidades que forman parte del plan esencial de Security Hub.
6. En la sección Selección de cuentas, elige una de las siguientes opciones:

- Todas las unidades organizativas y cuentas: aplica la configuración a toda la organización.
- Unidades organizativas y cuentas específicas: usa la barra de búsqueda o el árbol de estructura organizativa para seleccionar las unidades organizativas y las cuentas a las que se aplica la política.
- Sin unidades organizativas ni cuentas: no aplica la configuración a ninguna unidad organizativa o cuenta.

7. En la sección Regiones, elige una de las siguientes opciones:
   - Habilitar todas las regiones: si lo desea, elija si desea habilitar automáticamente las nuevas regiones.
   - Inhabilitar todas las regiones: si lo desea, elija si desea deshabilitar automáticamente las nuevas regiones.
   - Especifique las regiones: elija las regiones que desea habilitar y deshabilitar.
8. (Opcional) Para ver la configuración avanzada, consulte los operadores de herencia en la Guía del AWS Organizations usuario.
9. (Opcional) En el caso de las etiquetas de recursos, añada etiquetas como pares clave-valor para ayudarle a identificar la configuración.
10. Elija Siguiente.
11. Revise los cambios y luego seleccione Aplicar.

    El estado de configuración de su política se muestra en la parte superior de la página de políticas. Cada capacidad proporciona un estado que indica si se configuró correctamente o si tiene errores de implementación. Si hay algún error, elija el enlace del error para ver más detalles. Para ver la política vigente a nivel de cuenta, consulte la pestaña Organización en la página de configuraciones.

Habilitar una configuración con un tipo de implementación

El siguiente procedimiento describe cómo crear una configuración con un tipo de implementación para las cuentas de su AWS organización.

Para crear una implementación que habilite las cuentas de los miembros

1. Inicie sesión con su AWS cuenta con sus credenciales de administrador delegado. Abra la consola de Security Hub en https://console.aws.amazon.com/securityhub/v2/home.

2. En el panel de navegación, seleccione Administración y, a continuación, seleccione Configuraciones.
3. Elija un elemento con un tipo de implementación en el catálogo de configuración.
4. En la sección Capacidades de seguridad, seleccione las capacidades de seguridad que desee activar.
5. En la sección Selección de cuentas, elige una de las siguientes opciones:
   - Todas las unidades organizativas y cuentas: aplica la implementación a toda la organización.
   - Unidades organizativas y cuentas específicas: usa la barra de búsqueda o el árbol de estructura organizativa para seleccionar las unidades organizativas y las cuentas a las que se aplica la implementación.
   - Sin unidades organizativas ni cuentas: no aplica la implementación a ninguna unidad organizativa o cuenta.
6. En la sección Regiones, elige una de las siguientes opciones:
   - Habilitar todas las regiones: si lo desea, elija si desea habilitar automáticamente las nuevas regiones.
   - Inhabilitar todas las regiones: si lo desea, elija si desea deshabilitar automáticamente las nuevas regiones.
   - Especifique las regiones: elija las regiones que desea habilitar y deshabilitar.
7. Elija Configurar.

Edición de una política de configuración

Puede editar las capacidades, las regiones y las cuentas asociadas a una política de configuración. Al abrir una política para editarla, la consola muestra la configuración actual.

> **Note**
>
> Los cambios se aplican solo a las capacidades que seleccione en la política actualizada. Las capacidades no seleccionadas conservan su configuración actual en todas las cuentas y regiones de la política.

Para editar una política de configuración

1. Inicie sesión con su AWS cuenta con sus credenciales de administrador delegado. Abra la consola de Security Hub en https://console.aws.amazon.com/securityhub/v2/home.
2. En el panel de navegación, seleccione Administración y, a continuación, seleccione Configuraciones.
3. En la pestaña Políticas configuradas, elija el botón de opción correspondiente a la política que desea editar y, a continuación, elija Editar.
4. En la sección Capacidad, elija una de las siguientes opciones:
   - Configurar y habilitar todas las capacidades: habilita todas las capacidades de la política.
   - Seleccione las capacidades individuales y elija Habilitar , Deshabilitar o Personalizar para cada una de ellas.
5. En la sección de selección de cuentas, elige una de las siguientes opciones:
   - Todas las unidades organizativas y cuentas: aplica la política a toda la organización.
   - Unidades organizativas y cuentas específicas: usa la barra de búsqueda o el árbol de estructura organizativa para seleccionar las unidades organizativas y las cuentas a las que se aplica la política.
   - Sin unidades organizativas ni cuentas: elimina la política de todos los objetivos.
6. En la sección Regiones, configura a qué regiones se aplica la política. Las opciones dependen de las capacidades que haya seleccionado.

   Si opta por habilitar todas las capacidades:

   - En todas las capacidades seleccionadas: establece la misma configuración regional para todas las capacidades.
   - Por capacidad: le permite elegir las regiones de forma individual para cada capacidad.

   A continuación, elija Habilitar todas las regiones (con la opción de habilitar automáticamente las nuevas regiones) o Habilitar en algunas regiones para seleccionar regiones específicas.

   Si eliges acciones combinadas (habilitar, deshabilitar o personalizar) para las capacidades individuales:

- Si todas las capacidades seleccionadas comparten la misma acción, elija Entre todas las capacidades seleccionadas para establecer las regiones de manera uniforme. Para configurar las regiones para cada capacidad de forma individual, elija Por capacidad.
- Si las capacidades tienen acciones diferentes, debe asignar regiones para cada capacidad de forma individual.
- En el caso de las capacidades con la acción personalizada, elija En todas las capacidades seleccionadas para establecer las regiones de manera uniforme para todas las capacidades. Para configurar las regiones para cada capacidad por separado, elija Por capacidad.

7. Elija Siguiente.
8. Revise los cambios y, a continuación, seleccione Update (Actualizar). La política actualizada configura las cuentas de destino.

Eliminar una política de configuración

Puede eliminar una política de configuración. Cuando eliminas una política, el servicio elimina todas las cuentas y unidades organizativas adjuntas de la política.

Eliminación de una política de configuración

1. Inicia sesión con tu AWS cuenta con tus credenciales de administrador delegado. Abra la consola de Security Hub en https://console.aws.amazon.com/securityhub/v2/home.
2. En el panel de navegación, seleccione Administración y, a continuación, seleccione Configuraciones.
3. En la pestaña Políticas configuradas, seleccione la política que desea eliminar y, a continuación, elija Eliminar.
4. `delete`Introdúzcalo en el cuadro de confirmación y, a continuación, seleccione Eliminar.

Eliminación de la cuenta de administrador delegado en Security Hub

Puede eliminar la cuenta de administrador delegado en la consola de Security Hub en cualquier momento. Sin embargo, esta acción elimina al administrador delegado tanto de Security Hub como de Security Hub CSPM. Recomendamos realizar esta acción únicamente cuando haya confirmado esta operación con la cuenta de seguridad.

> **Note**
>
> Si utiliza una cuenta distinta de la cuenta de administración de la organización como administrador delegado de CSPM de Security Hub, al eliminarla a través de la consola CSPM de Security Hub o de la AWS Organizations API también se eliminará de Security Hub. Del mismo modo, si eliminas al administrador delegado de Security Hub mediante la consola o la AWS Organizations API de Security Hub, también se eliminará del CSPM de Security Hub. Cuando el administrador delegado se elimina del CSPM de Security Hub, Central Configuration se desactiva automáticamente.

Para eliminar la cuenta de administrador delegado

1. Inicie sesión en su AWS cuenta con las credenciales de la cuenta de administración de su organización. Abra la consola de Security Hub en https://console.aws.amazon.com/securityhub/v2/home.
2. En el panel de navegación, seleccione General.
3. En Administrador delegado, seleccione Eliminar administrador delegado. En el cuadro de diálogo de confirmación, escriba eliminar y seleccione Eliminar.

Re-enabling Centro de seguridad

Antes de volver a habilitar Security Hub en cuentas previamente inhabilitadas mediante una política de Security Hub, primero debes desvincular la política de inhabilitación. Si intentas volver a habilitar Security Hub mientras la cuenta o la unidad organizativa aún tiene una política de inhabilitación asociada, la política de inhabilitación anula la de activación y Security Hub permanece deshabilitada.

Para eliminar la política de inhabilitación de Security Hub para una organización o una cuenta

1. Inicia sesión con tu AWS cuenta con las credenciales de la cuenta de administración de tu organización. Abre la AWS Organizations consola en https://console.aws.amazon.com/organizations/v2/home.
2. En el panel de navegación, selecciona AWS cuentas.
3. Si la política actual de inhabilitación de Security Hub se aplica a toda la organización, seleccione Root en la sección Estructura organizativa. Si la política actual de inhabilitación de Security Hub es para cuentas específicas, elige la cuenta específica en la estructura organizativa y, a continuación, sigue los pasos restantes para cada cuenta.

4. En la pestaña Políticas, busca la sección titulada Políticas de Security Hub.
5. Selecciona el botón de radio situado junto a la política que desactiva Security Hub. Elija Desasociar.

Después de separar la política de tu organización o tus cuentas, puedes volver a habilitar Security Hub. Consulta Cómo administrar la configuración de las cuentas de los miembros en una AWS organización para obtener más información sobre cómo volver a habilitar Security Hub.

Recomendaciones de Security Hub

Los siguientes servicios de seguridad AWS envían las conclusiones a Security Hub en formato OCSF. Después de activar Security Hub, actívelos Servicios de AWS para aumentar la seguridad.

CSPM de Security Hub

Cuando habilita el CSPM de Security Hub, obtiene una vista integral del estado de seguridad en AWS. Esto ayuda a evaluar el entorno en función de los estándares de seguridad del sector y las prácticas recomendadas. Si bien puede empezar a usar Security Hub sin habilitar Security Hub CSPM, al habilitar Security Hub CSPM, Security Hub puede correlacionar las señales de seguridad del CSPM de Security Hub para mejorar la gestión de su postura.

Si habilita el CSPM de Security Hub, también le recomendamos que habilite el estándar básico de prácticas recomendadas de seguridad para su cuenta AWS . Este estándar consiste en un conjunto de controles que detectan si tú Cuentas de AWS y tus recursos se desvían de las prácticas recomendadas de seguridad. Cuando habilitas el estándar AWS básico de mejores prácticas de seguridad para tu cuenta, AWS Security Hub CSPM habilita automáticamente todos sus controles, incluidos los controles para los siguientes tipos de recursos:

- Controles de cuenta
- Controles de Amazon DynamoDB
- Controles de Amazon Elastic Compute Cloud
- AWS Identity and Access Management Controles (IAM)
- AWS Lambda controles
- Controles de Amazon Relational Database Service (Amazon RDS)
- Controles de Amazon Simple Storage Service

Puede desactivar cualquiera de los controles de esta lista. Sin embargo, si desactiva alguno de estos controles, no podrá recibir resultados de exposición para los recursos compatibles. Para obtener información sobre los controles que se aplican al estándar AWS Foundational Security Best Practices v1.0.0 (FSBP), consulte el estándar AWS Foundational Security Best Practices v1.0.0 (FSBP).

GuardDuty

Al habilitarlo GuardDuty, puede ver todas las amenazas y los resultados de la cobertura de seguridad en el panel de control de la consola de Security Hub. Si lo habilita GuardDuty, comienza a enviar datos GuardDuty automáticamente a Security Hub en formato OCSF.

Amazon Inspector

Cuando habilita Amazon Inspector, puede ver todas las exposiciones y resultados de cobertura de seguridad en el panel de la consola de Security Hub. Si habilita Amazon Inspector, Amazon Inspector comienza automáticamente a enviar datos a Security Hub en el formato OCSF.

Recomendamos activar el análisis estándar de Amazon EC2 y el análisis estándar de Lambda. Cuando activa el análisis estándar de Amazon EC2, Amazon Inspector analiza las instancias de Amazon EC2 de la cuenta para detectar vulnerabilidades en paquetes y problemas de accesibilidad de red. Cuando activa el análisis estándar de Lambda, Amazon Inspector analiza las funciones de Lambda para detectar vulnerabilidades de software en dependencias de paquetes. Para obtener más información, consulte Activación de un tipo de análisis en la Guía del usuario de Amazon Inspector.

Macie

Cuando habilita Macie, puede detectar exposiciones adicionales en los buckets de Amazon S3. Recomendamos configurar la detección automatizada de información confidencial para que Macie evalúe el inventario de los buckets de Amazon S3 cada día.

Cobertura de cuentas en Security Hub

La página de cobertura de cuentas muestra qué cuentas y regiones de su organización tienen habilitadas Security Hub y sus capacidades de seguridad integradas. Estas capacidades incluyen servicios como Amazon Inspector, Amazon GuardDuty, AWS Security Hub CSPM y Amazon Macie. Utilice esta página para identificar las brechas de cobertura y realizar un seguimiento de la adopción de capacidades en toda su organización.

Página de cobertura de cuentas

En la página de cobertura de la cuenta, puedes ver las métricas de cobertura agregadas. Usa la pestaña Cuentas para obtener detalles a nivel de cuenta y la pestaña Resultados de cobertura para revisar brechas de cobertura específicas.

Para acceder al Security Hub Cobertura de cuenta page

1. Abra la consola de Security Hub en https://console.aws.amazon.com/securityhub/v2/home.
2. En el panel de navegación, en Configuración, selecciona Cobertura de la cuenta.

Sección Descripción general

La sección Descripción general muestra las métricas de cobertura de seguridad agregadas de todas las cuentas monitoreadas. En el caso de las cuentas de administrador delegado, en esta sección se muestran los detalles de activación de Security Hub en toda la organización, lo que proporciona visibilidad de la cobertura de todas las cuentas de los miembros. Esta visualización de alto nivel muestra el porcentaje de cuentas con Security Hub y cada función de seguridad habilitada, lo que ofrece una visión completa de su postura de seguridad. Puede seleccionar el porcentaje de cobertura de Security Hub para ver un desglose de las cuentas habilitadas por región. Puede seleccionar cada porcentaje de capacidad para filtrar los resultados de cobertura por esa capacidad.

Los porcentajes de la sección Descripción general se determinan mediante los siguientes cálculos:

- Activación de Security Hub = (Número de pares de cuentas y regiones en los que Security Hub está activado) ÷ (Total de cuentas de su organización × Regiones en las que Security Hub está disponible)
- Cobertura de servicios = (Número de pares de cuentas habilitadas y regiones configuradas en las que la capacidad está habilitada) ÷ (Número total de pares de cuentas habilitadas y regiones configuradas, en las regiones configuradas en las que la cuenta está habilitada y la capacidad está disponible)

> **Regiones configuradas**
>
> Para la configuración de una región de origen, las regiones configuradas incluyen la región de origen y las regiones vinculadas. Para todas las demás configuraciones, las regiones configuradas se refieren únicamente a la región actual.

Pestaña de cuentas

Esta pestaña solo está disponible en la cuenta de administrador delegado de Security Hub. Utilice la pestaña Cuentas para analizar la cobertura específica de la cuenta. La columna Security Hub muestra el número de regiones en las que Security Hub está habilitado para cada cuenta. Esta columna no se muestra al ver la pestaña en las regiones que se han activado (las regiones que están deshabilitadas de forma predeterminada). Cada capacidad de seguridad muestra un porcentaje de cobertura que, cuando se selecciona, muestra un desglose detallado de las funciones individuales y su porcentaje de cobertura dentro de esa capacidad. Al seleccionar estos porcentajes, Security Hub filtra los resultados para mostrar la cobertura de esa capacidad y cuenta.

Los porcentajes de la pestaña Cuentas se determinan mediante el siguiente cálculo:

Cobertura de la pestaña Cuentas = (número de regiones en las que la función está habilitada) ÷ (Regiones en las que la capacidad está disponible)

Hay varios casos en los que el porcentaje de cobertura puede mostrarse como un 0%:

- Security Hub no está activado en la cuenta y, por lo tanto, no se están recopilando datos de cobertura.
- Security Hub está esperando a que se generen los resultados de la cobertura.

Pestaña de resultados de cobertura

La pestaña de hallazgos de cobertura muestra los hallazgos informativos sobre las capacidades de seguridad que están habilitadas o deshabilitadas en sus cuentas y regiones. Estos resultados ayudan a identificar las áreas en las que se puede mejorar la cobertura de seguridad. Cada resultado muestra el título del hallazgo, la cuenta y la región afectadas y su estado actual. Cada hallazgo también tiene un enlace de configuración que lo lleva al servicio individual donde puede administrar la configuración de esa capacidad, o a la página de configuraciones de Security Hub, donde puede actualizar las configuraciones de los servicios de seguridad.

Puede suprimir las búsquedas de cobertura con el estado No cubierto si esa capacidad de seguridad no es aplicable a la combinación cuenta-región. Security Hub excluye los hallazgos suprimidos del cálculo del porcentaje de cobertura de seguridad.

Para obtener más información sobre los hallazgos de cobertura y cómo suprimirlos, consulte Hallazgos de cobertura en Security Hub.

Widget de cobertura de seguridad

La cobertura de la cuenta también se puede ver a través del widget de cobertura de seguridad en el panel de resumen de Security Hub. Para obtener más información, consulte el widget de cobertura de seguridad.

Plan extendido de Security Hub

Con el plan Security Hub Extended, puede proteger todo el patrimonio de su empresa en la nube, los terminales, la red, la identidad, los datos, el correo electrónico y el navegador. Utilice AWS Security Hub como el centro de una experiencia de operaciones de seguridad integrada. Con el plan Security Hub Extended, puede seleccionar las soluciones de socios que satisfagan sus necesidades de seguridad y suscribirse a precios flexibles de pago por uso sin necesidad de inversiones iniciales ni compromisos a largo plazo. Puede añadir o eliminar soluciones de socios a medida que evolucionen las necesidades de su empresa.

El plan Security Hub Extended está disponible para todos los clientes que hayan habilitado el plan Security Hub Essentials. Los cargos del plan Security Hub Extended aparecen en tu AWS factura mensual AWS si eres el vendedor registrado.

Los precios del plan Security Hub Extended para todas las soluciones están disponibles en la pestaña del plan extendido de la página de detalles de precios de Security Hub.

Permisos para el plan Security Hub Extended

Para suscribirse a un producto asociado del plan Security Hub Extended, necesita los siguientes permisos, además de sus permisos de Security Hub:

- `aws-marketplace:ViewSubscriptions`
- `aws-marketplace:Subscribe`

Para cancelar la suscripción a un producto asociado del plan Security Hub Extended, necesita los siguientes permisos, además de sus permisos de Security Hub:

- `license-manager:ListReceivedLicenses`
- `aws-marketplace:ListAgreementCharges`
- `aws-marketplace:Unsubscribe`

Para obtener más información sobre los permisos de AWS Marketplace, consulte Controlar el acceso a las suscripciones de AWS Marketplace en la Guía del comprador de AWS Marketplace.

Revisar y suscribirse a los socios del plan Extended

Se puede acceder al plan Security Hub Extended a través de la cuenta de administrador delegado de Security Hub o de las cuentas independientes. En la página del plan Security Hub Extended, puede ver los detalles de cada socio, iniciar una suscripción a una solución de socio e iniciar el proceso de incorporación a la solución de cada socio a través de la página de incorporación del socio.

Para acceder al plan Security Hub Extended y suscribirse al producto de un socio

1. Inicie sesión en la consola AWS de administración con las credenciales de su cuenta independiente o de administrador delegado.
2. Abra la consola de Security Hub en https://console.aws.amazon.com/securityhub/v2/home.
3. En el panel de navegación, elija Administración y, a continuación, elija Plan extendido.
4. Para cada solución de socio a la que quiera suscribirse, elija Ver producto.
5. Revisa los detalles de precios del producto y, a continuación, selecciona Suscribirse cuando estés listo para iniciar el proceso de incorporación al producto del socio.
6. Una vez finalizado el proceso de suscripción, selecciona Configurar tu cuenta para que te redirijan a la página de registro del socio.
7. Proporciona la información necesaria para la página de registro del socio y sigue los siguientes pasos, proporcionados por el socio, para completar los pasos de incorporación.

> **Important**
>
> No se te facturará la solución para socios hasta que hayas completado el proceso de incorporación del producto para socios.

Darse de baja de un socio del plan Extended

Si ya no desea utilizar una solución de socio del plan Extended, puede darse de baja de la lista de socios.

Para darte de baja de una solución para socios, sigue las instrucciones sobre cómo cancelar tu suscripción de SaaS en la Guía del comprador de AWS Marketplace.

> **Important**
>
> Además de cancelar la suscripción, sigue todos los pasos de baja adicionales que sean necesarios para la solución para socios, en función de cómo hayas configurado la solución para tu empresa.

Descripción de agregación entre regiones en Security Hub

Cuando habilita la agregación interregional en Security Hub, designa una región de origen. La región de origen recopila los hallazgos, los recursos y las tendencias de una o más regiones vinculadas. A continuación, puede administrar todos los datos de seguridad de una sola región.

Supongamos que establece este de EE. UU.(norte de Virginia) como región de origen y oeste de EE. UU. (Oregón) y oeste de EE. UU. (norte de California) como regiones vinculadas. Al ver la página Resultados en Este de EE. UU. (Norte de Virginia), verá los resultados de las tres regiones. Las actualizaciones de esos resultados también se reflejan en las tres regiones.

Tipos de datos que se agregan

Cuando la agregación entre regiones está habilitada con una o más regiones vinculadas, Security Hub replica los siguientes datos de las regiones vinculadas a la región de origen. Esto ocurre en todas las cuentas que tienen habilitada la agregación entre regiones.

- Hallazgos
- Recursos
- Tendencias

Además de los nuevos datos que se muestran en la lista anterior, Security Hub también replica las actualizaciones de estos datos entre las regiones vinculadas y la región de origen. Las actualizaciones que se producen en una región vinculada se replican en la región de origen. Las actualizaciones que se producen en la región de origen se replican de vuelta en la región vinculada. Si hay actualizaciones contradictorias en la región de origen y en la región vinculada, se utiliza la actualización más reciente.

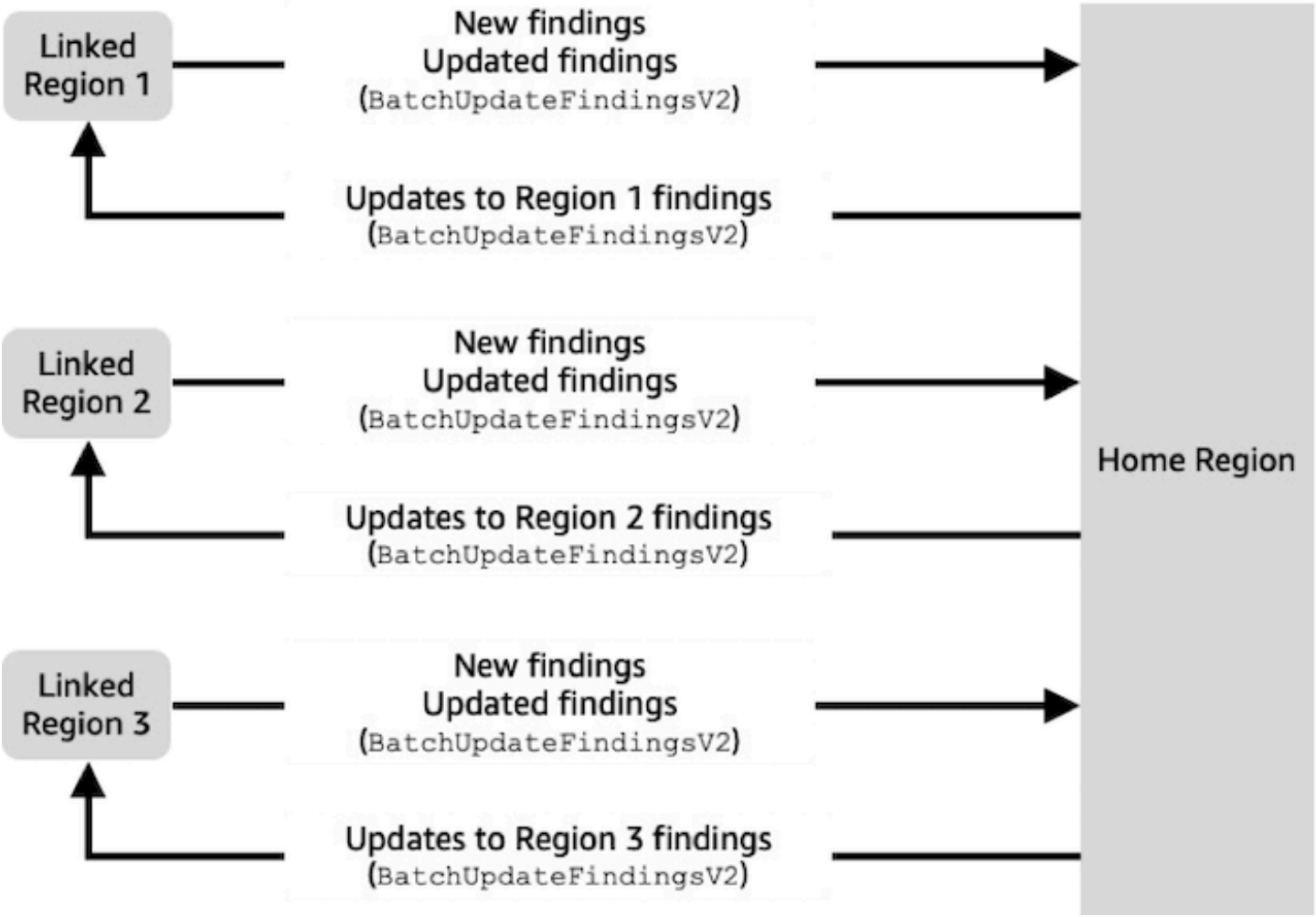
Los hallazgos que existían en una región en el momento en que se convierte en una región vinculada no se replican en la región de origen a menos que se actualice el hallazgo. Una vez que una región

se vincula a una región de origen, hay una diferencia en los resultados entre la región de origen y la región vinculada hasta que los hallazgos de la región vinculada se actualicen o desaparezcan.

Todos los recursos que existían en una región en el momento en que pasa a ser una región vinculada se replican en la región de origen, normalmente entre 24 y 48 horas después de que la región se vincule a la región de origen.

Al eliminar una región vinculada, todos los hallazgos o recursos de esa región permanecen en la región de origen hasta que el hallazgo o el recurso caduquen.

Los datos de tendencias se basan en los hallazgos y los recursos que están presentes en la región a la que se dirige la tendencia. Los datos de tendencias de una región de origen reflejan el estado actual de los hallazgos y los recursos que se han sincronizado con la región de origen.



Cross-Region la agregación no aumenta el costo de Security Hub. No se le cobrará nada cuando Security Hub replique nuevos datos o actualizaciones.

En la región de origen, la página de resumen ofrece una vista de sus hallazgos y recursos activos en todas las regiones vinculadas.

Security Hub solo agrega datos de las regiones en las que haya alguna cuenta que tenga activado Security Hub. Security Hub no se habilita automáticamente para ninguna cuenta en función de la configuración de agregación entre regiones.

Es posible activar la agregación entre regiones sin seleccionar ninguna región vinculada. En este caso, no se replican los datos.

Agregación de cuentas de administrador y de miembros

Las cuentas independientes y las cuentas de administrador pueden configurar la agregación entre regiones. Si un administrador realiza la configuración, la presencia de la cuenta de administrador es esencial para que la agregación entre regiones funcione en las cuentas administradas. Si la cuenta de administrador se elimina o se desvincula de una cuenta de miembro, la agregación interregional de esa cuenta de miembro se detiene. Sin embargo, si la cuenta de miembro tenía su propia configuración de agregación interregional antes de asociarse a un administrador, esa configuración vuelve a tener efecto.

Cuando una cuenta de administrador habilita la agregación entre regiones, Security Hub replica los datos que la cuenta de administrador genera en todas las regiones vinculadas a la región de origen. Además, Security Hub identifica las cuentas de miembros que están asociadas a ese administrador, y cada cuenta de miembro hereda la configuración de agregación entre regiones del administrador. Security Hub replica los datos que genera una cuenta de miembro en todas las regiones vinculadas a la región de origen.

El administrador puede acceder a las conclusiones de seguridad de todas las cuentas de los miembros de las regiones administradas y gestionarlas. Además, el administrador puede ver el inventario de recursos de todas las cuentas de los miembros de las regiones administradas.

Como cuenta de miembro de Security Hub, debe iniciar sesión en la región de origen para ver los datos agregados de su cuenta desde todas las regiones vinculadas. Las cuentas de los miembros no tienen permisos para ver los datos de otras cuentas de miembros y no se les permite llamar a `GetAggregatorV2` las API `CreateAggregatorV2``DeleteAggregatorV2`, y.

Reglas de automatización y agregación interregional

Cuando la agregación entre regiones está habilitada, las reglas de automatización solo se pueden crear en la región de origen definida. Cualquier regla que defina se aplica a todas las regiones

vinculadas, a menos que los criterios de la regla se apliquen a regiones específicas. Debes crear reglas de automatización independientes para cualquier región que no sea una región vinculada.

Todas las reglas que se hayan creado en la región de origen antes de habilitar la agregación entre regiones se aplicarán automáticamente en las regiones vinculadas. Las reglas creadas anteriormente en las regiones vinculadas dejarán de aplicarse una vez que se cree un agregador. Las reglas definidas en las regiones vinculadas volverán a aplicarse una vez que se elimine el agregador o la región deje de estar vinculada.

Habilitación de agregación entre regiones

Debe habilitar la agregación interregional desde la AWS región que desea designar como región de origen.

Para habilitar la agregación entre regiones, debe crear un recurso de Security Hub que se denomina agregador de resultados. El recurso del agregador de resultados especifica su región de origen y las regiones vinculadas (si las hubiera).

No puede usar una AWS región que esté deshabilitada de forma predeterminada como su región de origen. Para ver una lista de las regiones que están deshabilitadas de forma predeterminada, consulta Cómo habilitar una región en la Referencia AWS general.

Cuando activa la agregación entre regiones, puede especificar una o más regiones vinculadas si lo desea. Al habilitar la agregación entre regiones, Security Hub no se habilita en esa región. Para habilitar Security Hub en una región, consulte Crear una política como administrador delegado para administrar las cuentas de los miembros en la guía del usuario de Security Hub.

Para habilitar la agregación interregional (consola)

1. Desde la cuenta de administrador o en una cuenta independiente, abra la consola de AWS Security Hub en https://console.aws.amazon.com/securityhub/v2/home
2. Con el selector de AWS regiones, inicie sesión en la región que desea usar como región de agregación.
3. En el menú de navegación de Security Hub, seleccione Configuración y, a continuación, General.
4. En la sección de Cross-Region agregación, seleccione Configurar.
5. De forma predeterminada, la región de origen aparece como Sin región de agregación.
6. En Región de origen, seleccione la opción para designar la región actual como región de origen.

7. De forma opcional, en Regiones vinculadas, seleccione las regiones desde las que desea agregar datos.
8. Seleccione Save.

Revisión de la configuración de agregación entre regiones

Puede ver la configuración actual de agregación interregional en AWS Security Hub desde cualquier AWS región en la cuenta de administrador o en una cuenta independiente. Las cuentas de los miembros no pueden ver la configuración de agregación interregional. La configuración incluye la región de origen y las regiones vinculadas (si las hay).

Siga los pasos para ver su configuración actual de agregación interregional

Para ver la configuración de agregación entre regiones (consola)

1. Abra la consola AWS de Security Hub en https://console.aws.amazon.com/securityhub/v2/home.
2. En el panel de navegación, elija Configuración y, a continuación, General.
3. Si la agregación entre regiones no está habilitada, la página General muestra la opción para habilitar la agregación entre regiones. Solo las cuentas de administrador y las cuentas independientes pueden habilitar la agregación entre regiones.
4. Si la agregación entre regiones está habilitada, la pestaña Regiones muestra la siguiente información:
   - La región de origen
   - Si desea agregar automáticamente los hallazgos, los recursos y las tendencias de las nuevas regiones compatibles con Security Hub y por las que usted opte
   - La lista de regiones vinculadas (si se selecciona alguna)

Actualización de la configuración de agregación entre regiones

Puede actualizar su configuración actual de agregación interregional en AWS Security Hub cambiando las regiones vinculadas o la región de origen actual.

Los cambios en la agregación interregional no se implementarán en una región que haya optado por participar hasta que habilites la región en tu cuenta. AWS Las regiones que AWS se introdujeron el 20 de marzo de 2019 o después son regiones de participación voluntaria.

Cuando dejas de agregar datos de una región vinculada, AWS Security Hub no elimina ningún dato agregado existente de esa región al que se pueda acceder en la región de origen.

No puede usar los procedimientos de actualización de esta sección para cambiar la región de origen. Para cambiar la región de origen, se debe hacer lo siguiente:

1. Elimine la configuración actual de agregación interregional. Para obtener instrucciones, consulte the section called “Eliminar la agregación”.
2. Cambie a la región que desea que sea la nueva región de origen.
3. Habilitación de agregación entre regiones. Para obtener instrucciones, consulte the section called “Habilitación de agregación”.

Debe actualizar la configuración de agregación entre regiones desde la región de origen actual.

Para cambiar las regiones vinculadas (consola)

1. Desde la cuenta de administrador o en una cuenta independiente, abra la consola AWS de Security Hub en https://console.aws.amazon.com/securityhub/v2/home.
2. Inicie sesión en la región de agregación actual.
3. En el menú de navegación de Security Hub, selecciona Configuración y, a continuación, General.
4. Para la Cross-Region agregación, selecciona Editar.
5. Para la opción Regiones vinculadas, actualice las regiones vinculadas seleccionadas.
6. Seleccione Save.

Eliminar la agregación interregional

Si no desea que AWS Security Hub agregue datos, puede eliminar su agregador de búsquedas. También puedes conservar tu agregador de búsquedas pero no vincular ninguna AWS región a la región de origen actualizando el agregador existente para que no haya ninguna región vinculada seleccionada.

Para cambiar su región de origen, debe eliminar su agregador de resultados actual y crear uno nuevo.

Al eliminar el agregador de resultados, Security Hub deja de agregar datos. No elimina ningún dato agregado existente de la región de origen.

Para eliminar el agregador de resultados (consola)

Puede eliminar su agregador de resultados únicamente desde la región de origen actual.

En las regiones distintas de la región de origen, el panel Agregación de resultados en la consola de Security Hub muestra un mensaje en el que se indica que debe editar la configuración en la región de origen. Seleccione este mensaje para mostrar un enlace para cambiar a la región de origen.

Para detener la agregación entre regiones (consola)

1. Abra la consola AWS de Security Hub en https://console.aws.amazon.com/securityhub/v2/home.
2. Asegúrese de haber iniciado sesión en su región de origen actual.
3. En el menú de navegación de Security Hub, selecciona Configuración y, a continuación, General.
4. En Cross-Region Agregación, selecciona Editar.
5. En Región de agregación, elija Sin región de agregación.
6. Seleccione Save.
7. En el cuadro de diálogo de confirmación, en el campo de confirmación, escriba **`Confirm`**.
8. Elija Confirmar.

Integración de Security Hub con Microsoft Azure

Para supervisar sus recursos de Microsoft Azure, puede integrar Microsoft Azure con AWS Security Hub. Luego, Security Hub habilita automáticamente la administración de posturas y la administración de vulnerabilidades para su entorno de Azure y genera hallazgos y otros datos sobre su entorno. No es necesario que active ningún servicio de seguridad de Azure; toda la funcionalidad corre a cargo de. AWS Más específicamente, el servicio le proporciona lo siguiente:

CIS, Microsoft Azure Foundations, Benchmark v4.0 y Azure Foundational Best Practices

Comprobaciones de cumplimiento automatizadas según el estándar CIS Azure v4.0 y el estándar Azure Foundational Best Practices. Estos estándares abarcan los controles de identidad, redes, almacenamiento, registro y bases de datos.

Administración de vulnerabilidades

Amazon Inspector escanea automáticamente las imágenes de los contenedores de Azure VM, Function Apps y Azure Container Registry (ACR) en busca de vulnerabilidades de software a través del conector vinculado a servicios.

> **Note**
>
> El escaneo de máquinas virtuales requiere que Amazon EC2 Systems Manager esté configurado en la misma región. Para obtener más información sobre la configuración, consulte la documentación de Amazon Inspector sobre la integración con Azure.

Correlación de exposición

Detección automatizada de los recursos de Azure expuestos en función de las combinaciones de accesibilidad de la red, acceso público y errores de configuración.

Alertas de detección de amenazas de Microsoft Defender for Cloud

Si configura la exportación continua de Azure Defender al Event Hub, Security Hub incorpora las alertas de detección de amenazas de Defender for Cloud y las asigna al formato Open Cybersecurity Schema Framework (OCSF). Estas aparecen junto con la gestión de la postura y los resultados de vulnerabilidad en la consola de Security Hub.

Inventario de activos

Un inventario completo de los recursos de Azure descubiertos a través de la integración, visible en la consola de Security Hub junto con sus AWS recursos.

Formato OCSF

Security Hub genera todos los hallazgos en el formato Open Cybersecurity Schema Framework (OCSF), lo que proporciona un esquema coherente AWS para todos los hallazgos de Azure.

Para crear la integración, conecte su entorno de Azure a Security Hub mediante el siguiente proceso:

1. El entorno de Azure se configura con el registro de una aplicación, las credenciales de identidad federadas, las asignaciones de roles de Azure y la infraestructura de Event Hub.
2. Al usar la consola de Security Hub, se crea un conector para la integración. Debe especificar su ID de inquilino de Azure, su ID de cliente de la aplicación, el ámbito de supervisión y la región de Event Hub.

3. Security Hub crea los roles y recursos necesarios vinculados a los servicios en su. Cuenta de AWS
4. AWS Config recopila datos de configuración de recursos de su entorno de Azure.

   AWS Config se usa internamente para recopilar datos de configuración de recursos. A diferencia de AWS la administración de posturas, en la que se debe habilitar explícitamente la grabación AWS Config y pagar por ella, la administración de posturas de Azure AWS Config se gestiona automáticamente. No es necesario habilitar la grabadora AWS Config por separado, configurar una grabadora ni pagar por su AWS Config uso por separado. Estos costos están incluidos en los precios de Security Hub.
5. Security Hub comienza a recibir los datos de configuración de recursos y los eventos del registro de actividad de su entorno de Azure.
6. Security Hub genera información sobre la gestión de la postura y las vulnerabilidades de su entorno de Azure.

Cómo AWS Config se usa

AWS Config se usa internamente para recopilar datos de configuración de recursos y detectar cambios en su entorno de Azure. El conector gestiona esto automáticamente. No es necesario habilitarla AWS Config por separado, configurar una grabadora ni pagar por su AWS Config uso. Estos costos están incluidos en los precios de Security Hub para los recursos de Azure.

Información adicional

Al crear la integración, Security Hub también crea automáticamente las correspondientes integraciones vinculadas a servicios en Security Hub, CSPM y Amazon Inspector. Estas integraciones vinculadas a servicios garantizan que el alcance de las comprobaciones de CSPM y de los análisis de vulnerabilidad del Inspector coincidan con el alcance definido en Security Hub. Si quieres cambiar el alcance, tienes que hacer los cambios en el Security Hub. No puede modificar una integración vinculada a un servicio directamente en Security Hub, CSPM o Inspector.

También puede crear una integración de Azure directamente en Security Hub CSPM y especificar una configuración de ámbito independiente. La integración de CSPM funciona entonces de forma independiente de la integración de Security Hub y puede tener un alcance diferente de la suscripción a Azure y la región de Azure.

Para obtener información sobre cómo estimar y calcular los costos de la integración de Security Hub con Azure, consulte los precios de AWS Security Hub.

Temas

- Requisitos previos para integrar Security Hub con Microsoft Azure
- Configuración de Microsoft Azure para que se integre con Security Hub
- Configuración de Security Hub para que se integre con Microsoft Azure
- Eliminar un conector de Microsoft Azure en Security Hub

Requisitos previos para integrar Security Hub con Microsoft Azure

Antes de integrar Microsoft Azure con AWS Security Hub, complete las siguientes tareas en su entorno AWS y en Azure. Esto ayuda a garantizar que tanto usted como Security Hub dispongan de los recursos y permisos que necesitan para supervisar sus recursos de Azure.

Temas

- Requisitos previos para AWS
- Requisitos previos para Microsoft Azure

Requisitos previos para AWS

Compruebe que tiene lo siguiente en su Cuenta de AWS:

AWS Security Hub activado

Security Hub debe estar habilitado en el Región de AWS lugar Cuenta de AWS y donde desea crear el conector. Debe habilitar Security Hub antes de crear un conector de Azure.

AWS Security Hub (CSPM) activado

El CSPM de Security Hub debe estar habilitado en el mismo y. Cuenta de AWS Región de AWS La integración de Azure se basa en el CSPM de Security Hub para la evaluación de la configuración de los recursos.

Permisos de IAM de consola

El director de IAM que crea el conector debe tener los siguientes permisos:

- `config:GetConnector`
- `config:ListConnectors`
- `config:PutConnector`

La federación de identidades salientes de IAM está habilitada

Debe habilitar la federación de identidades salientes de IAM en su. Cuenta de AWS Esta función permite a AWS los servicios autenticarse ante proveedores de identidad externos (como el Entra ID de Microsoft) utilizando credenciales federadas en lugar de usar secretos de larga data.

Tras habilitar la federación de identidades salientes, anote la URL del emisor del token. Esta URL sigue el formato:

```
https://uuid.tokens.sts.global.api.aws
```

Necesitará esta URL al configurar las credenciales de identidad federada en Azure.

Requisitos previos para Microsoft Azure

Compruebe que dispone de lo siguiente en su entorno de Azure:

Inquilino de Azure

Debe tener un inquilino de Azure en la nube comercial de Azure. Azure Government y Azure China no son compatibles.

Disponibilidad del registro de Microsoft Entra ID

El registro de recursos requiere registros de auditoría e inicio de sesión de Microsoft Graph de tu arrendatario de Microsoft Entra ID. Algunos registros de Microsoft Entra ID requieren la licencia P1 o P2 de Microsoft Entra ID.

Si el inquilino no tiene los registros necesarios, es posible que el registro de recursos indique errores parciales. El registro de la aplicación y las asignaciones de funciones de Azure no proporcionan los datos de registro faltantes.

Función de administrador global

Debe tener la función de administrador global en Microsoft Entra ID para configurar el entorno de Azure. Este rol es necesario para registrar las aplicaciones, conceder el consentimiento del administrador para los permisos de la API de Microsoft Graph, asignar funciones de RBAC en el ámbito del grupo de administración raíz de inquilinos y configurar los ajustes de diagnóstico para los registros de auditoría de Entra ID.

Además de ser administrador global, necesita las siguientes funciones de RBAC de Azure para crear los recursos que requiere la integración:

- Administrador de acceso de usuario (o propietario) en el ámbito raíz (/): para asignar funciones de RBAC en el ámbito del grupo de administración raíz del inquilino.
- Colaborador (o propietario) de políticas de recursos en el ámbito del grupo de administración raíz del inquilino: para crear las definiciones y asignaciones de políticas de Azure que automaticen la configuración de diagnóstico y la corrección.
- Colaborador (o propietario) en el ámbito de la suscripción que aloja el Event Hub: para crear el espacio de nombres del Event Hub y los recursos relacionados.

> **Note**
>
> En muchas organizaciones, el administrador global de Azure y el administrador AWS de seguridad son personas diferentes. La configuración de Azure se puede completar de forma independiente mediante el script de configuración generado.

Tras completar estas tareas, estará listo para configurar su entorno de Azure.

Configuración de Microsoft Azure para que se integre con Security Hub

Tras completar las tareas previas, puede configurar su entorno de Microsoft Azure para que admita la integración con AWS Security Hub. Para ayudarlo a hacerlo, la consola de Security Hub genera un script de configuración personalizado para su configuración.

Para generar el script de configuración

1. Abra la consola AWS de Security Hub en https://console.aws.amazon.com/securityhub/advanced/home? region=us-east-1. .
2. En el panel de navegación, elija Integraciones.
3. Elija Crear conector de Azure.
4. Complete la configuración del conector (ID de inquilino, ámbito y nombre) y, a continuación, copie el script de configuración generado.

Para ejecutar el script, utilice la CLI de Azure y autentíquese con una cuenta de administrador global (`az login`).

Al ejecutar el script, este realiza una serie de tareas. En las siguientes secciones se describe cada tarea que realiza el script. Si su organización restringe la ejecución del script, puede realizar estas

tareas manualmente, utilizando este tema como guía. Después de configurar el entorno de Azure, puede configurar Security Hub para que se integre con Azure.

En los pasos 1 a 7, configure la base compartida que utilizan todas las funciones de Security Hub: el registro de la aplicación, las credenciales federadas, las asignaciones de funciones de Azure, los permisos de Microsoft Graph, Event Hub y la exportación de registros. Los pasos 8 a 10 configuran los recursos adicionales de Azure para capacidades específicas:

- Administración de vulnerabilidades (Amazon Inspector): configura la exportación de eventos del repositorio de Azure Container Registry (ACR) y una identidad gestionada asignada por el sistema en las máquinas virtuales de Azure.
- Detección de amenazas (Microsoft Defender for Cloud): configura Microsoft Defender for Cloud para exportar continuamente las alertas de seguridad al Event Hub.

> **Note**
>
> El registro de una sola aplicación de Azure se comparte entre los servicios AWS de seguridad. Si también usa Security Hub CSPM o Amazon Inspector para Azure, utilizan el mismo registro de aplicaciones. No es necesario crear registros independientes para cada servicio. AWS

Tareas

- Paso 1: Registrar una aplicación de Azure
- Paso 2: Crear una entidad principal de servicio
- Paso 3: Configurar las credenciales de identidad federadas
- Paso 4: Asignar funciones de RBAC
- Paso 5: Configurar los permisos de la API de Microsoft Graph
- Paso 6: configurar Azure Event Hub
- Paso 7: configurar el registro de actividad y exportar el registro de auditoría de Entra ID
- Paso 8: Configurar la exportación de Azure Container Registry
- Paso 9: Habilitar una identidad administrada en las máquinas virtuales de Azure
- Paso 10: Exportar las alertas de Microsoft Defender for Cloud

Paso 1: Registrar una aplicación de Azure

Registra una nueva aplicación en Microsoft Entra ID. Esta aplicación sirve como la identidad que se AWS utiliza para autenticarse en su entorno de Azure mediante credenciales federadas. No se requieren secretos de cliente.

```
$ az ad app create --display-name "AWSSecurityHubIntegration"
```

Anote el ID de la aplicación (cliente) de la salida (el `appId` atributo). Proporcionará este valor al crear el conector en la consola de Security Hub.

Paso 2: Crear una entidad principal de servicio

Cree un principal de servicio para la aplicación registrada. Las asignaciones de roles de Azure se utilizan para conceder permisos al principal de servicio. El principal de servicio realiza acciones en su entorno de Azure.

```
$ az ad sp create --id application-client-id
```

¿Dónde *`application-client-id`* está el ID de la aplicación (cliente) del paso anterior?

Establezca el URI del ID de la aplicación en el registro en`api://`*`application-client-id`*. AWS requiere este identificador para intercambiar tokens federados con la aplicación. Sin este URI, AWS no se puede generar una audiencia de tokens federados válida y ninguna de las funciones puede autenticarse en Azure.

```
$ az ad app update \
  --id application-client-id \
  --identifier-uris "api://application-client-id"
```

Paso 3: Configurar las credenciales de identidad federadas

Configure las credenciales de identidad federadas en la aplicación para AWS permitir la autenticación sin secretos de cliente. Esto establece una confianza OIDC entre Azure y Azure. AWS No se almacenan credenciales ni secretos de larga duración.

La integración de Azure con Security Hub se autentica mediante una función de AWS IAM por capacidad: detección de configuraciones de recursos, administración de vulnerabilidades y detección de amenazas. Agregue una credencial de identidad federada para cada función, de modo que todas

las funciones puedan autenticarse en Azure. AWS crea automáticamente las funciones vinculadas al servicio al crear el conector. La función `Inspector2SSMFederationRole` utilizada para el escaneo de máquinas virtuales no es una función vinculada a un servicio; se crea como parte de la configuración de escaneo de máquinas virtuales de Amazon Inspector, descrita en el paso 9. ???

Funcionalidad	Asunto (ARN del rol de IAM)
Descubrimiento de la configuración de recursos ()AWS Config	`arn:aws:iam::` *`account-id`* `:role/aws-service-role/thirdparty.config.amazonaws.com/AWSServiceRoleForConfigThirdParty`
Gestión de vulnerabilidades (Inspector)	`arn:aws:iam::` *`account-id`* `:role/aws-service-role/thirdparty.inspector2.amazonaws.com/AWSServiceRoleForAmazonInspector2ThirdPa rty`
Administración de vulnerabi lidades: escaneo de máquinas virtuales (Amazon EC2 Systems Manager)	`arn:aws:iam::` *`account-id`* `:role/Inspector2SS MFederationRole-` *`tenant-id`*
Detección de amenazas (Security Hub)	`arn:aws:iam::` *`account-id`* `:role/aws-service-role/securityhubv2.amazonaws.com/AWS ServiceRoleForSecurityHubV2`

Ejecute el siguiente comando una vez para cada tema de la tabla anterior, cambiando los `subject` valores `name` y cada vez. Los `audiences` valores `issuer` y son los mismos para todas las credenciales.

```
$ az ad app federated-credential create \
  --id application-client-id \
  --parameters '{
    "name": "credential-name",
    "issuer": "token-issuer-url",
    "subject": "service-linked-role-arn",
    "audiences": ["api://AzureADTokenExchange"],
    "description": "AWS federation for Security Hub Azure integration"
  }'
```

Valores clave:

- Emisor: la URL de su emisor de tokens de IAM Outbound Identity Federation. Sigue el formato. `https://uuid.tokens.sts.global.api.aws`
- Asunto: un ARN de rol de IAM de la tabla anterior. El rol `tenant-id` de administrador de sistemas de Amazon EC2 es su ID de inquilino de Azure.
- Audiencia: `api://AzureADTokenExchange` (valor estándar para la federación de identidades de cargas de trabajo).
- Nombre: cualquier nombre que sea único en la aplicación.

Paso 4: Asignar funciones de RBAC

Asigne las siguientes funciones integradas al director de servicio:

- Lector: otorga acceso de solo lectura a todos los recursos de Azure para que Security Hub pueda descubrir y evaluar las configuraciones de sus recursos. Asigne este rol en el ámbito raíz ()/.
- Colaborador: otorga el acceso de escritura que Amazon Inspector necesita para escanear las máquinas virtuales, las aplicaciones de funciones y las imágenes de los contenedores de Azure en busca de vulnerabilidades. Asigne este rol al ámbito del grupo de administración raíz del inquilino, que lo propagará a todas las suscripciones del inquilino.
- Receptor de datos de Azure Event Hubs: permite AWS leer los eventos del Event Hub. Asigne este rol al ámbito del grupo de administración raíz del inquilino.

> **Asigne Reader en el ámbito raíz**
>
> Asegúrese de asignar la función de lector al ámbito raíz (/), no al ámbito del grupo de administración raíz del inquilino. Security Hub lee los recursos de asignación de roles de Azure en todos los ámbitos, incluidas las asignaciones asignadas al ámbito raíz del inquilino. Una asignación de lector en el grupo de administración raíz no incluye las asignaciones cuyo ámbito sea/, por lo que, sin ella, esas lecturas fallan y se produce un error de autorización y el conector puede entrar en un estado degradado.

El colaborador otorga acceso de escritura a todo el inquilino

La función de colaborador en el ámbito del grupo de administración raíz del inquilino otorga acceso de escritura con altos privilegios para todo el inquilino a sus recursos de Azure. Security Hub requiere este acceso para que Amazon Inspector pueda analizar sus recursos informáticos en busca de vulnerabilidades. Por ejemplo, Inspector usa los permisos de ejecución de comandos de ejecución de máquinas virtuales que proporciona Contributor. A través de Amazon EC2 Systems Manager Automation, Inspector ejecuta comandos en las máquinas virtuales de Azure para instalar y operar el agente VM Scanner.

```
$ az role assignment create \
  --assignee application-client-id \
  --role "Contributor" \
  --scope "/providers/Microsoft.Management/managementGroups/tenant-id"

$ az role assignment create \
  --assignee application-client-id \
  --role "Azure Event Hubs Data Receiver" \
  --scope "/providers/Microsoft.Management/managementGroups/tenant-id"

$ az role assignment create \
  --assignee application-client-id \
  --role "Reader" \
  --scope "/"
```

Root-scope la tarea requiere un acceso elevado

La asignación de un rol en el ámbito raíz (/) requiere un acceso elevado. Si se produce un error en la asignación de funciones, compruebe que la administración de acceso a los recursos de Azure esté configurada en Sí en Microsoft Entra ID > Propiedades. A continuación, cierra sesión y vuelve a iniciarla para actualizar el token.

Elimine la elevación temporal de la raíz

Al habilitar la administración del acceso para los recursos de Azure, se otorga al administrador que ha iniciado sesión la función de administrador de acceso de usuarios en el ámbito raíz (/), que puede gestionar el acceso en todos los grupos de suscripción

y administración del inquilino. Una vez completada la incorporación, vuelva a configurar la administración del acceso a los recursos de Azure como No en Microsoft Entra ID > Propiedades, guarde y cierre sesión para que esta elevación no permanezca activa.

Paso 5: Configurar los permisos de la API de Microsoft Graph

Conceda los siguientes permisos de la API Graph de Microsoft (tipo de aplicación) a la aplicación y, a continuación, conceda el consentimiento del administrador:

- `Application.Read.All`
- `AuditLog.Read.All`
- `DelegatedPermissionGrant.Read.All`
- `Device.Read.All`
- `Group.Read.All`
- `GroupMember.Read.All`
- `GroupSettings.Read.All`
- `Organization.Read.All`
- `Policy.Read.All`
- `RoleManagement.Read.Directory`
- `User.Read.All`
- `UserAuthenticationMethod.Read.All`

```
$ az ad app permission admin-consent --id application-client-id
```

Paso 6: configurar Azure Event Hub

AWS Config usa un Azure Event Hub para recibir notificaciones casi en tiempo real sobre los cambios en la configuración de los recursos en su entorno de Azure. El script de configuración crea la infraestructura de Event Hub y la etiqueta para su detección. La detección de Event Hub utiliza una resolución basada en etiquetas: Security Hub busca una etiqueta en el espacio de nombres de Event Hub con el formato necesario `AWSConfig-`*`account-id`*`-`*`region`* para identificar la instancia de Event Hub correcta para su integración.

```
$ az group create \
  --name "aws-securityhub-integration" \
  --location event-hub-region

$ az eventhubs namespace create \
  --resource-group "aws-securityhub-integration" \
  --name "aws-securityhub-account-id" \
  --location event-hub-region \
  --sku Standard

$ az eventhubs eventhub create \
  --resource-group "aws-securityhub-integration" \
  --namespace-name "aws-securityhub-account-id" \
  --name "activitylog" \
  --message-retention 3 \
  --partition-count 4

$ az eventhubs eventhub consumer-group create \
  --resource-group "aws-securityhub-integration" \
  --namespace-name "aws-securityhub-account-id" \
  --eventhub-name "activitylog" \
  --name "AWSConfig"
```

Tras crear el Event Hub, etiquete el espacio de nombres para que lo detecte y asigne la función de receptor de datos. Utilícela `az tag update` con `--operation merge` para conservar cualquier otra etiqueta del espacio de nombres (como la etiqueta de detección de amenazas del paso 10):

```
$ az tag update \
  --resource-id namespace-resource-id \
  --operation merge \
  --tags "AWSConfig-account-id-region=activitylog"

$ az role assignment create \
  --assignee application-client-id \
  --role "Azure Event Hubs Data Receiver" \
  --scope namespace-resource-id
```

> **Note**
>
> En el formato de etiquetaAWSConfig-*account-id*-*region*, *account-id* es su Cuenta de AWS identificador de 12 dígitos y *region* es Región de AWS donde está creando el

conector (por ejemplo,`us-east-1`). Estos valores identifican quién Cuenta de AWS y qué región son los propietarios de esta integración de Event Hub.

Configuración clave:

- SKU del espacio de nombres: estándar (obligatorio para los grupos de consumidores).
- Nombre de Event Hub —`activitylog`.
- Grupo de consumidores —`AWSConfig`.
- Etiqueta: `AWSConfig-`*`account-id-region`* con valor`activitylog`. Esta etiqueta permite AWS Config descubrir el Event Hub automáticamente.
- Asignación de funciones: Azure Event Hubs Data Receiver en el espacio de nombres.

Para la detección de amenazas, la configuración también crea un `defender-alerts` Event Hub independiente con un grupo de `AWSSecurityHub` consumidores y agrega una segunda etiqueta de detección en el formato `AWSSecurityHub-`*`account-id-region`* que identifica el hub que Security Hub lee directamente. Para obtener más información, consulta el paso 10.

Paso 7: configurar el registro de actividad y exportar el registro de auditoría de Entra ID

Configure Azure para exportar los registros de actividad y los registros de Entra ID de Microsoft al Event Hub.

Exportación del registro de actividad:

Configure los ajustes de diagnóstico en cada suscripción para exportar los registros de actividad al Event Hub. El script de configuración lo configura automáticamente para todas las suscripciones supervisadas. Los registros de actividad capturan la actividad a nivel de suscripción, incluidas las asignaciones de funciones y los cambios de recursos.

Exportación del registro de Microsoft Entra ID:

Configure los ajustes de diagnóstico en el Entra ID de Microsoft para exportar los registros al mismo Event Hub. Diríjase a Microsoft Entra ID > Supervisión > Configuración de diagnóstico > Añadir configuración de diagnóstico. AuditLogsSignInLogsActívalos y NonInteractiveUserSignInLogs dirígelos a tu Event Hub.

Paso 8: Configurar la exportación de Azure Container Registry

Security Hub escanea las imágenes de los contenedores de Azure Container Registry (ACR) en busca de vulnerabilidades mediante Amazon Inspector. Para ello, Inspector necesita que los eventos del repositorio ACR se exporten a un Event Hub en la misma región de Azure que el registro. Para la configuración de la exportación a ACR, consulte Configurar Amazon Inspector para que se integre con Microsoft Azure en la Guía del usuario de Amazon Inspector.

Paso 9: Habilitar una identidad administrada en las máquinas virtuales de Azure

Security Hub escanea sus máquinas virtuales de Azure a través de Inspector. Cada máquina virtual de Azure de destino debe tener habilitada una identidad gestionada asignada por el sistema. Para agregar esta identidad a sus máquinas virtuales automáticamente, asigne dos políticas de Azure que utilicen el `modify` efecto en el ámbito del grupo de administración raíz del inquilino:

- Para una máquina virtual que no tiene identidad, la política agrega una identidad administrada asignada por el sistema.
- Para una máquina virtual que solo tiene una identidad asignada por el usuario, la política agrega una identidad administrada asignada por el sistema y conserva las identidades asignadas por el usuario existentes.

Una máquina virtual que ya tiene una identidad administrada asignada por el sistema no se modifica. Como las políticas utilizan este `modify` efecto, ajustan la identidad sin tener que volver a implementar la máquina virtual.

Inspector usa Amazon EC2 Systems Manager Automation para implementar y administrar el agente Inspector VM Scanner en sus máquinas virtuales de Azure. Esto requiere una configuración adicional AWS, que incluye un proveedor de identidad OIDC de IAM para Microsoft Entra ID y varias funciones de IAM. Para ver la configuración completa del escaneo de máquinas virtuales, consulte Configurar Amazon Inspector para que se integre con Microsoft Azure en la guía del usuario de Amazon Inspector.

Paso 10: Exportar las alertas de Microsoft Defender for Cloud

Security Hub incorpora las alertas de detección de amenazas de Microsoft Defender for Cloud y las asigna al formato Open Cybersecurity Schema Framework (OCSF). Para enviar estas alertas, crea un centro de `defender-alerts` eventos dedicado y configura Microsoft Defender for Cloud para exportar continuamente las alertas de seguridad a ese centro.

En el espacio de nombres de Event Hub del paso 6, crea el `defender-alerts` Event Hub, un grupo de `AWSSecurityHub` consumidores desde el que pueda leer Security Hub y una regla de autorización de firma de acceso compartido (SAS) en el ámbito del hub con el permiso de envío que Microsoft Defender for Cloud utilice para enviar alertas:

```
$ az eventhubs eventhub create \
  --resource-group "aws-securityhub-integration" \
  --namespace-name "aws-securityhub-account-id" \
  --name "defender-alerts" \
  --message-retention 3 \
  --partition-count 4

$ az eventhubs eventhub consumer-group create \
  --resource-group "aws-securityhub-integration" \
  --namespace-name "aws-securityhub-account-id" \
  --eventhub-name "defender-alerts" \
  --name "AWSSecurityHub"

$ az eventhubs eventhub authorization-rule create \
  --resource-group "aws-securityhub-integration" \
  --namespace-name "aws-securityhub-account-id" \
  --eventhub-name "defender-alerts" \
  --name "DefenderExportSend" \
  --rights Send
```

A continuación, combine una segunda etiqueta de detección en el espacio de nombres para que Security Hub descubra el centro. `defender-alerts` `az tag update--operation mergeUtilícela` con para conservar la etiqueta de `AWSConfig` descubrimiento del paso 6:

```
$ az tag update \
  --resource-id namespace-resource-id \
  --operation merge \
  --tags "AWSSecurityHub-account-id-region=defender-alerts"
```

Por último, configure la exportación continua de Microsoft Defender for Cloud del tipo de datos de las alertas de seguridad al `defender-alerts` Event Hub. En el portal de Azure, vaya a Microsoft Defender for Cloud > Configuración del entorno, seleccione la suscripción, elija Exportación continua > Event Hub, seleccione Alertas de seguridad y elija el `defender-alerts` Event Hub y la regla `DefenderExportSend` SAS.

> **Note**
>
> Si configuras la exportación continua mediante programación (mediante la API de Azure Resource Manager, una plantilla ARM o Azure Policy) en lugar de hacerlo en el portal, autentica la exportación al Event Hub con la cadena de conexión `DefenderExportSend` SAS. Recupérala con `az eventhubs eventhub authorization-rule keys list` la `DefenderExportSend` regla y configúrala como la cadena de conexión de la acción de exportación. Para obtener más información, consulte Configurar la exportación continua en la documentación de Microsoft Azure.

> **Note**
>
> Tras completar estas tareas, espere aproximadamente de 15 a 30 minutos para que la configuración surta efecto. A continuación, comprueba que tu Event Hub reciba mensajes (la IncomingMessages métrica) antes de crear el conector en Security Hub.

Configuración de Security Hub para que se integre con Microsoft Azure

Tras completar las tareas previas y configurar el entorno de Microsoft Azure, puede configurar AWS Security Hub para que se integre con Azure. Para configurar Security Hub para que se integre con Azure, debe crear un conector. Puede crear el conector desde una cuenta de administrador delegado o desde la cuenta de administración. Tras crear el conector, se producen los siguientes eventos:

1. Security Hub valida las credenciales de Azure y la conectividad con su entorno de Azure. Este proceso puede tardar varios minutos.
2. Security Hub crea conectores vinculados a servicios en Security Hub CSPM y Amazon Inspector. Estos conectores garantizan que las comprobaciones de gestión de la postura y el análisis de vulnerabilidades coincidan con el alcance definido en Security Hub.
3. AWS Config comienza a descubrir los recursos de Azure mediante las credenciales de identidad federadas.
4. Security Hub habilita automáticamente el estándar CIS Microsoft Azure Foundations Benchmark v4.0 y el estándar Azure Foundational Best Practices en CSPM para sus recursos de Azure.

5. En el caso de los recursos con eventos de registro de actividad, las conclusiones iniciales comienzan a aparecer en un plazo de 15 a 30 minutos. La evaluación completa de todos los recursos existentes puede tardar hasta 24 horas.

Temas

- Cree un conector de Azure
- Ajustar el alcance de un conector de Azure
- Compruebe el estado de un conector de Azure
- Solucione problemas de un conector de Azure
- Cómo gestiona Security Hub los recursos y la búsqueda de identificadores

Cree un conector de Azure

Para crear un conector de Microsoft Azure para su entorno, complete los pasos siguientes mediante la consola de AWS Security Hub o la API.

1. Abra la consola AWS de Security Hub en https://console.aws.amazon.com/securityhub/advanced/home? region=us-east-1. .
2. En el panel de navegación, elija Integraciones.
3. Elija Crear conector de Azure.
4. En la sección Capacidades de seguridad, elija si desea habilitar la función de escaneo de red. Esta función está habilitada de forma predeterminada en la cuenta en la que se habilita la integración con Azure y se puede desmarcar antes de completar la configuración del conector. Si una política de la organización bloquea esta función para tu cuenta, no aparece como una opción. Para obtener más información, consulte Escaneo de red en Security Hub.
5. Para el ID de inquilino de Azure, introduzca su identificador de inquilino de Microsoft Entra ID. Puede encontrarlo en el portal de Azure, en Microsoft Entra ID > Propiedades > Tenant ID.
6. Para el ID de la aplicación (cliente), introduzca el ID de la aplicación de Azure que registró durante la configuración del entorno de Azure.
7. Configure los ajustes adicionales y el alcance del conector de la siguiente manera:
   - En Nombre, introduzca un nombre único para el conector. El nombre puede contener hasta 50 caracteres alfanuméricos e incluir guiones.

> **Note**
>
> El nombre del conector no se puede cambiar después de la creación.

- En Descripción, si lo desea, introduzca una breve descripción del conector. La descripción puede contener hasta 200 caracteres.

> **Important**
>
> Los nombres y las descripciones se utilizan para identificar el contenido. No incluyas en ellos información sensible, confidencial o de identificación personal (PII).

- En el caso de las suscripciones, elija Todas las suscripciones para supervisar todas las suscripciones actuales y futuras del arrendatario, o Suscripciones específicas para supervisar solo las suscripciones que especifique. Si opta por supervisar solo suscripciones específicas, introduzca el ID de cada una de ellas.
- En el caso de las regiones, elija Todas las regiones para supervisar los recursos en todas las regiones de Azure o Regiones específicas para supervisar solo las regiones que especifique.

> **Note**
>
> Si ya ha creado un conector en Security Hub CSPM o Amazon Inspector para el mismo inquilino de Azure, el alcance del conector en Security Hub debe incluir las mismas suscripciones y regiones que el conector de Security Hub CSPM o Amazon Inspector.

> **Note**
>
> Los controles que evalúan los recursos de Microsoft Entra ID y Microsoft Graph requieren incluir el ámbito regional global en la configuración de la integración. Si seleccionas solo regiones específicas de Azure, estos controles no generan resultados.

8. Revise la configuración del conector.

> **Note**
>
> Si piensa utilizar Amazon Inspector para el escaneo de máquinas virtuales de Azure, debe crear las funciones de IAM necesarias. Para obtener más información, consulte the section called “Funciones de IAM para el escaneo de máquinas virtuales”.

9. Cuando termine de introducir y revisar la configuración, seleccione Crear conector.

Funciones de IAM para el escaneo de máquinas virtuales de Azure mediante Amazon Inspector

Para habilitar el análisis de vulnerabilidades a través de Amazon Inspector, debe crear los siguientes recursos de IAM en su. Cuenta de AWS

Proveedor de identidad OIDC de IAM

Cree un proveedor de identidad OIDC de IAM para con la siguiente configuración: Microsoft Entra ID

- URL del emisor: `https://sts.windows.net/tenant-id/`
- Lista de identificadores de clientes: `api://app-id`, `api://AzureADTokenExchange`
- Huella digital: cadena de 40 caracteres con todos los ceros (`0`repetida 40 veces). AWS STS valida los tokens mediante el punto final del JWKS en lugar del valor de la huella digital.

Inspector2VmScannerRole-***tenant-id***

Lo utiliza el agente Amazon Inspector VM Scanner que se ejecuta en máquinas virtuales de Azure para enviar la telemetría escaneada a Amazon Inspector. Este rol usa la federación de identidades web de OIDC a través del proveedor de identidades. Microsoft Entra ID

Política de confianza:

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Federated": "arn:aws:iam::account-id:oidc-provider/
sts.windows.net/tenant-id/"
```

```
            },
            "Action": "sts:AssumeRoleWithWebIdentity"
        }
    ]
}
```

Etiquetas:

- `inspector-managed` = `true`

Política de permisos (TelemetryPolicy):

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "inspector2-telemetry:*",
            "Resource": "*"
        }
    ]
}
```

Inspector2SSMFederationRole-*tenant-id*

Permite la federación de OIDC a Azure para una autenticación segura entre nubes. Esta función la asumen AND AssumeRole y DispatchRole Amazon EC2 Systems Manager para obtener los tokens de identidad web para las operaciones de Azure.

Política de confianza:

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::account-id:root"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
```

```
                    "aws:PrincipalTag/caller": "SSM"
                },
                "ArnLike": {
                    "aws:PrincipalArn": [
                        "arn:aws:iam::account-id:role/Inspector2SSMAssumeRole-tenant-
id",
                        "arn:aws:iam::account-id:role/Inspector2SSMDispatchRole-tenant-
id"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "ssm.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Política de permisos (FederationPolicy):

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "sts:IdentityTokenAudience": [
                        "api://AzureADTokenExchange"
                    ]
                }
            },
            "Action": [
                "sts:GetWebIdentityToken",
                "sts:TagGetWebIdentityToken"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
```

```
}
```

Etiquetas:

- `caller` = `SSM`
- `inspector-managed` = `true`

Inspector2SSMAssumeRole-*tenant-id*

Ejecuta Amazon EC2 Systems Manager Automation para incorporar las máquinas virtuales de Azure como instancias administradas. Esta función crea y administra las activaciones híbridas, transfiere las funciones a Amazon EC2 Systems Manager y recupera los documentos de automatización.

Política de confianza:

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "ssm.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "account-id"
                }
            }
        }
    ]
}
```

Política de permisos (AssumeRolePolicy):

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
```

```
            "Resource": "arn:aws:iam::account-id:role/
Inspector2SSMFederationRole-tenant-id"
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::account-id:role/
AmazonEC2RunCommandRoleForManagedInstances",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "ssm.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:CreateActivation",
                "ssm:DeleteActivation",
                "ssm:DescribeActivations",
                "ssm:DescribeInstanceInformation",
                "ssm:PutConfigurePackageResult",
                "iam:ListRoleTags"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ssm:AddTagsToResource",
            "Resource": [
                "arn:aws:ssm:*:account-id:activation/*",
                "arn:aws:ssm:*:account-id:managed-instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "ssm:GetDocument",
            "Resource": [
                "arn:aws:ssm:*:*:document/AWS-InstallDistributorPackageOnAzure",
                "arn:aws:ssm:*:*:document/AWS-InstallSsmAgentOnAzure",
                "arn:aws:ssm:*::document/AmazonInspector2-InspectorVmScanner"
            ]
        },
        {
```

```
            "Effect": "Allow",
            "Action": "ssm:GetCloudConnector",
            "Resource": "*"
        }
    ]
}
```

Etiquetas:

- `caller` = `SSM`
- `AzureTenantId` = *`tenant-id`*
- `AzureApplicationId` = *`app-id`*
- `inspector-managed` = `true`

Inspector2SSMDispatchRole-***tenant-id***

Resuelve los objetivos de máquinas virtuales de Azure y distribuye la instalación del agente Amazon Inspector VM Scanner mediante Amazon EC2 Systems Manager Automation. Esta función inicia las ejecuciones de automatización y las transfiere AssumeRole a Amazon EC2 Systems Manager.

Política de confianza:

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "ssm.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "account-id"
                }
            }
        }
    ]
}
```

Política de permisos (DispatchPolicy):

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::account-id:role/Inspector2SSMAssumeRole-tenant-
id",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "ssm.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ssm:StartAutomationExecution",
            "Resource": [
                "arn:aws:ssm:*:*:document/AWS-InstallDistributorPackageOnAzure",
                "arn:aws:ssm:*:account-id:automation-execution/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": "arn:aws:iam::account-id:role/
Inspector2SSMFederationRole-tenant-id"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:DescribeInstanceInformation",
                "ssm:ListCloudConnectors",
                "ssm:GetCloudConnector",
                "iam:ListRoleTags"
            ],
            "Resource": "*"
        }
    ]
}
```

Etiquetas:

- `caller` = `SSM`
- `inspector-managed` = `true`

Requisitos previos para el escaneo de máquinas virtuales

El registro de la aplicación de Azure debe tener el URI de la ID de la aplicación establecido en. `api://app-id`

Cada máquina virtual de Azure que desee escanear debe tener habilitada una identidad administrada asignada por el sistema. Para asignar automáticamente la identidad administrada a las nuevas máquinas virtuales, utilice una DeployIfNotExists política en su entorno de Azure.

Tras crear el conector, Security Hub comienza a supervisar su entorno de Azure. Puede comprobar el estado del conector en la página de integraciones.

Ajustar el alcance de un conector de Azure

Después de crear un conector de Microsoft Azure, puede ajustar el alcance del conector cambiando las suscripciones de Azure o las regiones de Azure que supervisa. Los cambios de alcance suelen tener efecto en un plazo de 15 a 30 minutos en el caso de los recursos con eventos en el registro de actividad. La evaluación completa de las suscripciones de Azure recién agregadas puede tardar hasta 24 horas.

Antes de ajustar el alcance de un conector, tenga en cuenta lo siguiente:

- Cuando cambias el alcance de un conector en Security Hub, los conectores vinculados al servicio asociados en Security Hub CSPM y Amazon Inspector se actualizan automáticamente para que coincidan.
- El alcance de un conector de Security Hub nunca puede ser inferior al de cualquier conector existente gestionado por el cliente en Security Hub CSPM o Amazon Inspector para el mismo inquilino de Azure.
- Si añades una región al alcance del conector, debes volver a ejecutar el script de configuración para aprovisionar la infraestructura de Event Hub en la nueva región. La configuración actual de Event Hub no se ve afectada.

Compruebe el estado de un conector de Azure

Puede comprobar el estado de un conector de Microsoft Azure en cualquier momento para confirmar que Security Hub recibe datos de su entorno de Azure.

Para comprobar el estado de un conector

1. Abra la consola AWS de Security Hub en https://console.aws.amazon.com/securityhub/advanced/home? region=us-east-1. .
2. En el panel de navegación, elige Integraciones y selecciona tu conector de Azure.
3. Compruebe que el estado del conector muestre Activo. Si el conector aparece como Activo, la verificación se ha completado. Si muestra un estado diferente, consultethe section called "Solucionar problemas de un conector".
4. Diríjase a Hallazgos y filtre por `ResourceCloudProviders = Azure` para confirmar que se están generando hallazgos para sus recursos de Azure.
5. Consulte la página de estándares de seguridad para confirmar que el estándar CIS Azure v4.0 muestra los controles en estado APROBADO o FALLIDO (no todos son NO_DATA).

> **Note**
>
> En última instancia, el estado del conector es uniforme. Cuando se produce un problema con los permisos o la configuración, el estado del conector cambia rápidamente a Degradado con un mensaje procesable. Sin embargo, después de solucionar el problema, el estado puede tardar hasta 24 horas en volver a Conectado.
>
> - Un estado degradado después de una corrección reciente no indica necesariamente un problema continuo.
> - Para ver en tiempo real los errores de grabación, comprueba las CloudWatch métricas en el espacio de nombres.

Solucione problemas de un conector de Azure

Si tienes problemas con el conector, consulta los siguientes problemas y soluciones comunes.

El estado del conector no es correcto

Este problema suele producirse si las credenciales federadas no están configuradas correctamente en Azure.

Para solucionar este problema, compruebe que la URL del emisor del token y el ARN del asunto de sus credenciales federadas de Azure coincidan con los suyos. Cuenta de AWS

No se encontró nada después de 30 minutos

Este problema puede producirse si el Event Hub no recibe los registros de actividad.

Para solucionar este problema, compruebe que las opciones de diagnóstico estén configuradas en sus suscripciones de Azure y que el espacio de nombres de Event Hub esté correctamente etiquetado con`AWSConfig-`*`account-id`*`-`*`region`*.

Todos los controles muestran NO_DATA

Este problema puede producirse si el conector está deshabilitado o si AWS Config no puede llegar a su entorno de Azure.

Para solucionar este problema, compruebe que el conector esté habilitado y que el principal del servicio tenga la función de lector en el ámbito del grupo de administración raíz del inquilino.

No se pueden registrar algunos recursos de Azure

El error puede producirse por cualquiera de los siguientes motivos:

- El entorno Azure no cumple los requisitos previos para el registro de recursos.
- El registro de la aplicación no requiere el consentimiento del administrador para los permisos de la API de Microsoft Graph.
- La asignación de funciones de lector no cubre todos los ámbitos requeridos.
- El arrendatario de Microsoft Entra ID no tiene los datos de registro necesarios.

Para corregir el error, haga lo siguiente:

1. Para confirmar que su entorno cumple con todos los requisitos, consulte los requisitos previos para Microsoft Azure.
2. Confirma que el registro de la aplicación cuenta con los permisos necesarios de la API de Microsoft Graph con el consentimiento del administrador.
3. Verifique que el principal del servicio tenga la función de lector en el ámbito del grupo de administración raíz del inquilino.

Los resultados aparecen solo para algunas suscripciones

Este problema puede producirse si la exportación del registro de actividades no está configurada para todas las suscripciones de destino.

Para solucionar este problema, confirme que la configuración de diagnóstico abarque todas las suscripciones incluidas en el conector.

Cómo gestiona Security Hub los recursos y la búsqueda de identificadores

Al habilitar la integración de Azure con AWS Security Hub, los identificadores de búsqueda de recursos y seguridad de otros proveedores de nube se almacenan en AWS Config Security Hub y otros AWS servicios (según sea necesario) como metadatos relacionados con la administración de la configuración de recursos correspondiente y los datos de búsqueda de seguridad recopilados de los otros proveedores de nube. Dichos identificadores no constituyen su contenido. No incluyas en ellos información sensible, confidencial o de identificación personal.

Los siguientes identificadores de su entorno de nube conectado se almacenan y utilizan AWS para proporcionar capacidades de seguridad multinube:

- Identificadores de recursos: ID de inquilino de Azure, ID de suscripción, ubicación (región), ID de recurso (nombres o identificadores de grupos de recursos, proveedor de recursos, tipo de recurso)
- Identificadores de búsqueda de seguridad: los identificadores únicos asignados a cada búsqueda de seguridad generada por el servicio de detección.

Las relaciones entre estos identificadores (incluida la forma en que los recursos se relacionan entre sí y la forma en que los hallazgos se relacionan con los recursos) también se almacenan como metadatos del servicio. AWS utiliza estos identificadores para la correlación de los recursos, la asociación de los hallazgos con los recursos, el registro de las operaciones de los servicios y la deduplicación.

Eliminar un conector de Microsoft Azure en Security Hub

Después de crear un conector de Microsoft Azure en AWS Security Hub, puede eliminarlo en cualquier momento. Si eliminas un conector, Security Hub deja de realizar las comprobaciones de administración de la postura y la supervisión de vulnerabilidades en tu entorno de Azure. Security Hub también deja de generar nuevos hallazgos y otros datos sobre su entorno. Los hallazgos

existentes se conservan durante 90 días. El inventario de recursos permanece igual que cuando se eliminó el conector y se retira después de 90 días.

Al eliminar un conector, Security Hub elimina automáticamente los conectores vinculados a servicios asociados en AWS Security Hub CSPM y Amazon Inspector. Security Hub no elimina el registro de aplicaciones de Azure ni la infraestructura de Event Hub de su entorno de Azure. Debe eliminarlos manualmente, directamente en Microsoft Azure. Para obtener información sobre cómo hacerlo, consulte Eliminar una aplicación en la documentación de Microsoft Azure.

Para eliminar un conector de Azure

1. Abra la consola AWS de Security Hub en https://console.aws.amazon.com/securityhub/advanced/home? region=us-east-1. .
2. En el panel de navegación, elija Integraciones.
3. Seleccione el conector que desea eliminar.
4. Elija Eliminar.
5. Cuando se le solicite, confirme que desea eliminar el conector.

> **Important**
>
> Si eliminas un conector y creas uno nuevo en un plazo de 6 horas, la detección de recursos puede tardar hasta 6 horas. Planifique la eliminación y la recreación del conector en consecuencia.

Trabajando en el panel de resumen de Security Hub

El panel de resumen de la consola de Security Hub muestra una descripción general de sus exposiciones, amenazas, recursos y cobertura de seguridad en todos los widgets de seguridad. Puedes personalizar el panel añadiendo y eliminando widgets y creando y aplicando conjuntos de filtros para recuperar los datos de cada widget.

Consideraciones

Tenga en cuenta lo siguiente antes de interactuar con el panel:

- Las personalizaciones, como los conjuntos de filtros guardados o los cambios en el diseño de los widgets, se guardan automáticamente.

- Los datos se actualizan automáticamente cada vez que abres el panel.
- Si configuras la agregación entre regiones, el panel de control incluye los resultados de todas las regiones vinculadas (al ver el panel de control en tu región de origen).

Ten en cuenta lo siguiente si tu cuenta es una cuenta de administrador delegado para una organización, una cuenta de miembro de una organización o una cuenta independiente.

- Las personalizaciones realizadas por una cuenta de administrador delegado se guardarán independientemente de las personalizaciones realizadas por las cuentas de los miembros. Las personalizaciones pueden incluir conjuntos de filtros guardados o cambios en el diseño de los widgets.
- Si su cuenta es la cuenta de administrador delegado de una organización, los datos incluyen los resultados tanto de su cuenta como de las cuentas de miembro.
- Si tu cuenta es una cuenta de miembro de una organización o una cuenta independiente, los datos solo incluyen los hallazgos de tu cuenta.

Como práctica recomendada, no incluyas información confidencial, sensible o de identificación personal (PII) en los conjuntos de filtros guardados, los widgets personalizados u otros campos de texto de formato libre relacionados.

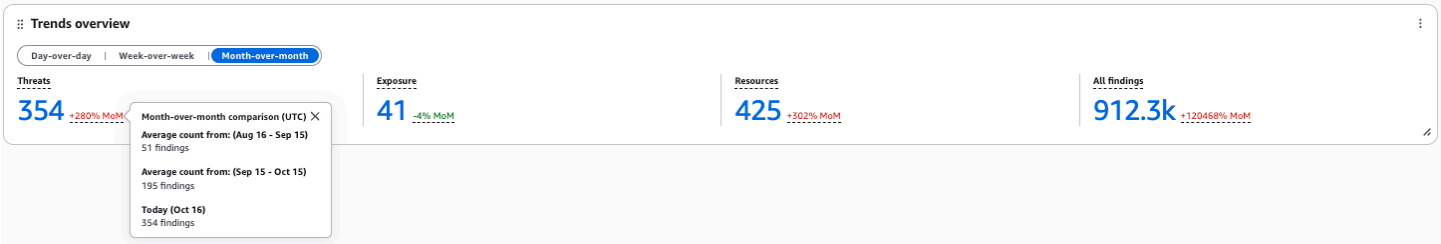
Widgets disponibles

Puedes interactuar con diferentes widgets en las pestañas Ejecutivo y de Clasificación del panel de resumen. La pestaña Ejecutiva incluye widgets que muestran datos sobre tendencias en relación con tus riesgos, amenazas y recursos, y el widget Cobertura de seguridad, que te ayuda a hacer un seguimiento de la cobertura de tu cuenta en las diferentes funciones de seguridad. La pestaña de clasificación incluye widgets que muestran un resumen de tus riesgos, amenazas y recursos. Sin embargo, puedes añadir widgets, eliminar widgets y gestionar la posición de cada widget en ambas pestañas para personalizar tu experiencia.

Widgets de tendencias

Los siguientes widgets muestran datos de tendencias para sus exposiciones, amenazas y recursos, para que pueda analizarlos a lo largo del tiempo.

Widget de resumen de tendencias



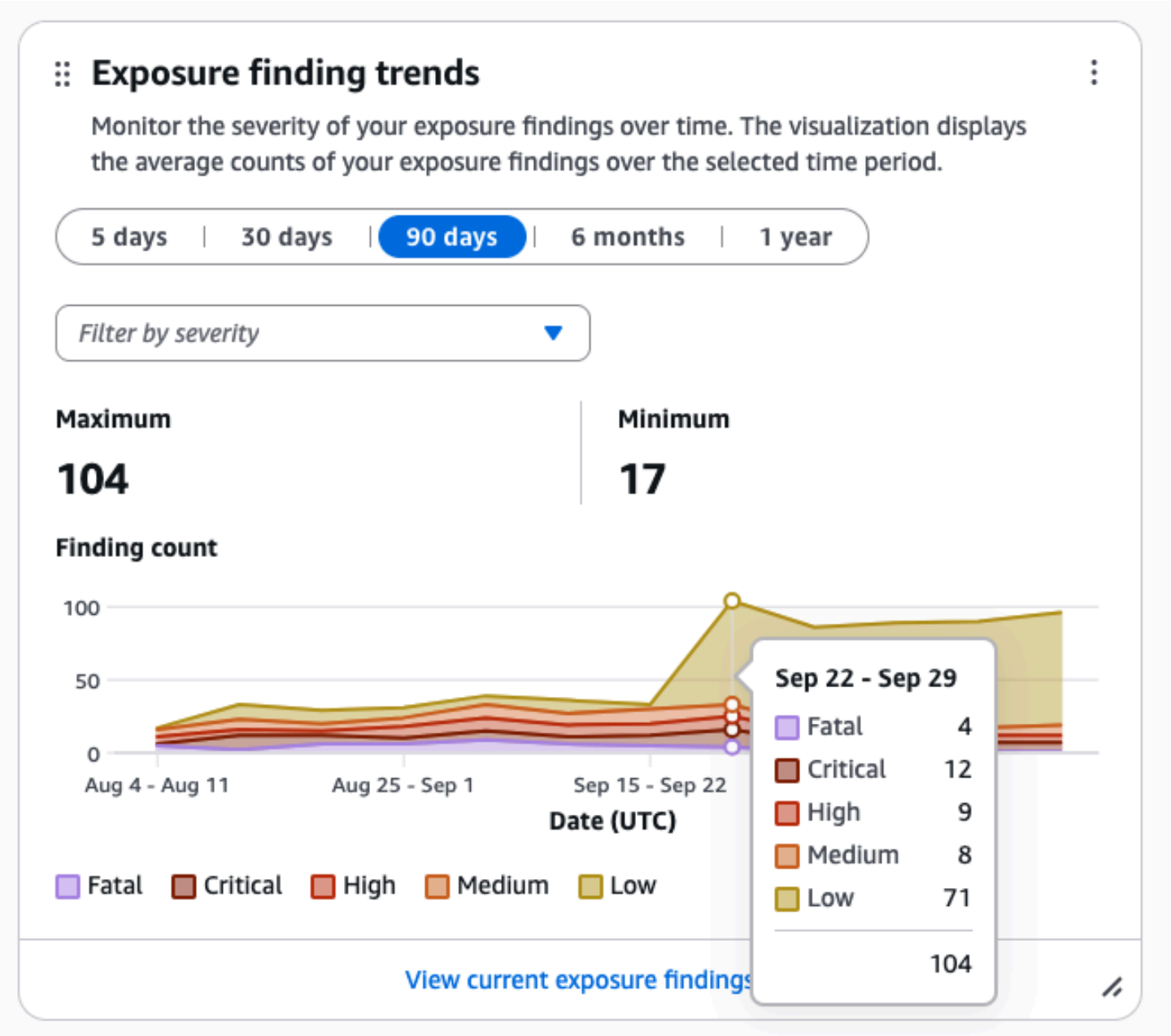
Este widget muestra una descripción general de sus exposiciones, amenazas, recursos y hallazgos en los siguientes períodos de tiempo:

- Month-over-monthrefleja el recuento, período tras período, de los últimos dos meses.
- Week-over-weekrefleja el recuento período tras período de las últimas dos semanas.
- Day-over-dayrefleja el recuento de período tras período de los últimos 2 días.

El número que aparece junto al porcentaje refleja el recuento promedio de un período a otro hasta la fecha. Si eliges este número, accederás a su panel correspondiente en la consola. Si accedes a otro panel que muestra datos de tendencias, el panel solo mostrará los datos de tendencias de los últimos 90 días o del período más adecuado si tu cuenta no contiene hallazgos o recursos con una antigüedad superior a 30 días.

> **Note**
>
> Para recibir datos en este widget, debes habilitar los siguientes servicios de seguridad:
>
> - AWS Security Hub (CSPM): para recibir datos sobre las exposiciones
> - Amazon Inspector: para recibir datos sobre las exposiciones
> - GuardDuty— Para recibir datos sobre amenazas

Widget de tendencias de búsqueda de exposición



Este widget muestra la gravedad de tus hallazgos de exposición en los siguientes períodos de tiempo:

- 5 días
- 30 días
- 90 días
- 6 meses

- 1 año

La visualización muestra el recuento promedio de sus hallazgos durante el período de tiempo seleccionado.

Filtros de gravedad

Puede actualizar el gráfico incluyendo o excluyendo los siguientes filtros de gravedad:

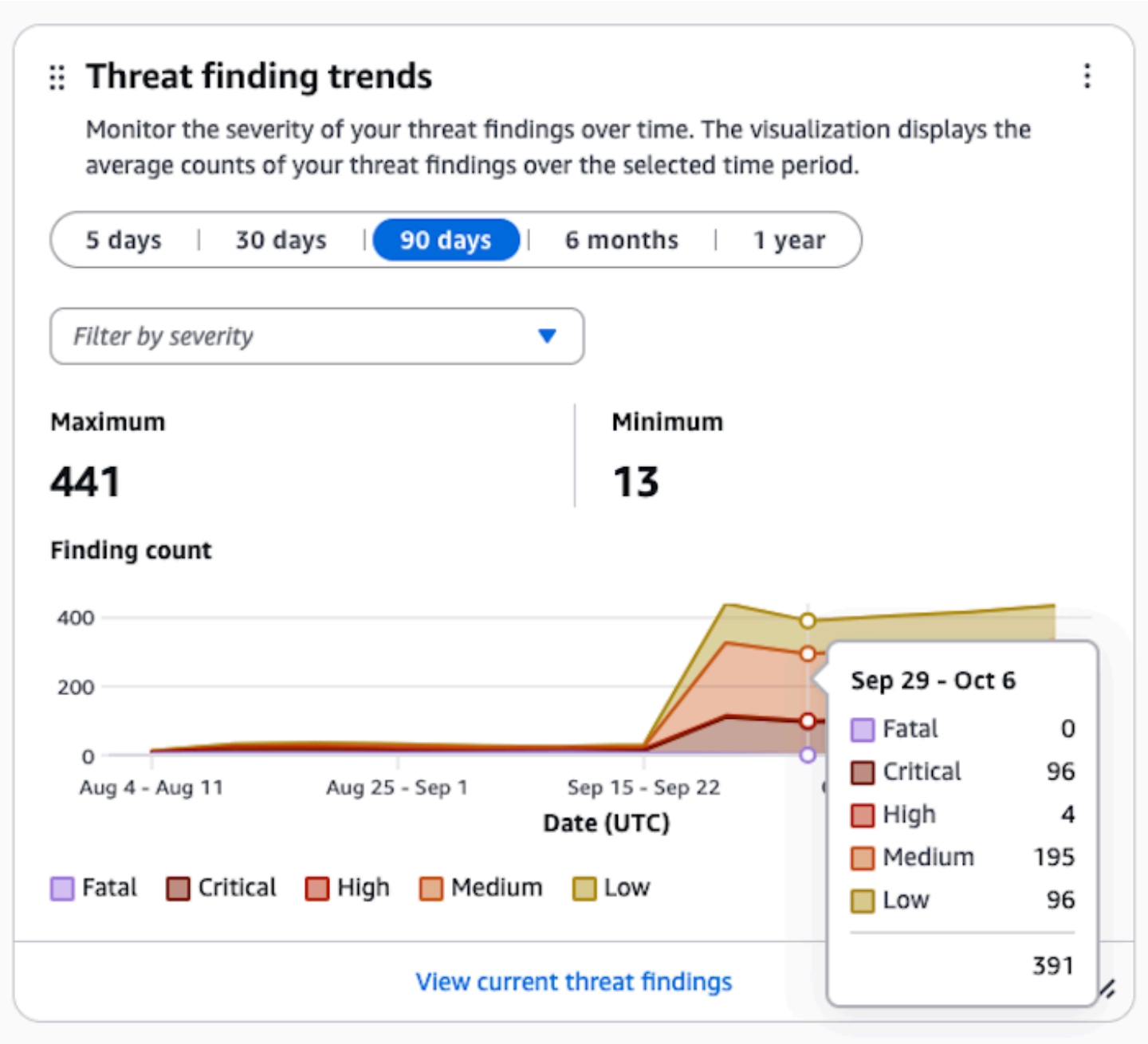
- Mortal
- Critical
- Alta
- Medio
- Baja
- Informativo
- Otros
- Desconocido

Los filtros de gravedad aplicados aparecen en diferentes cuadros en la parte inferior de la visualización. Puedes pasar el ratón por encima de la visualización para revisar el recuento promedio de hallazgos en momentos específicos. También puedes revisar el recuento promedio de hallazgos que coinciden con cada filtro de gravedad aplicado.

Puedes elegir Ver todos los hallazgos de exposición actuales para que te dirijan al panel de exposición. De forma predeterminada, el panel de exposición solo muestra los datos de tendencias de los últimos 90 días. Si su cuenta no contiene datos de exposición con una antigüedad superior a 30 días, el panel muestra los datos de tendencias según el período de tiempo más adecuado.

> **Note**
>
> Para recibir datos en este widget, debes habilitar Amazon Inspector y Security Hub CSPM.

Widget de tendencias de búsqueda de amenazas



Este widget muestra la gravedad de las amenazas detectadas en los siguientes períodos de tiempo:

- 5 días
- 30 días
- 90 días
- 6 meses
- 1 año

La visualización muestra el recuento promedio de sus hallazgos durante el período de tiempo seleccionado.

Filtros de gravedad

Puede actualizar el gráfico incluyendo o excluyendo los siguientes filtros de gravedad:

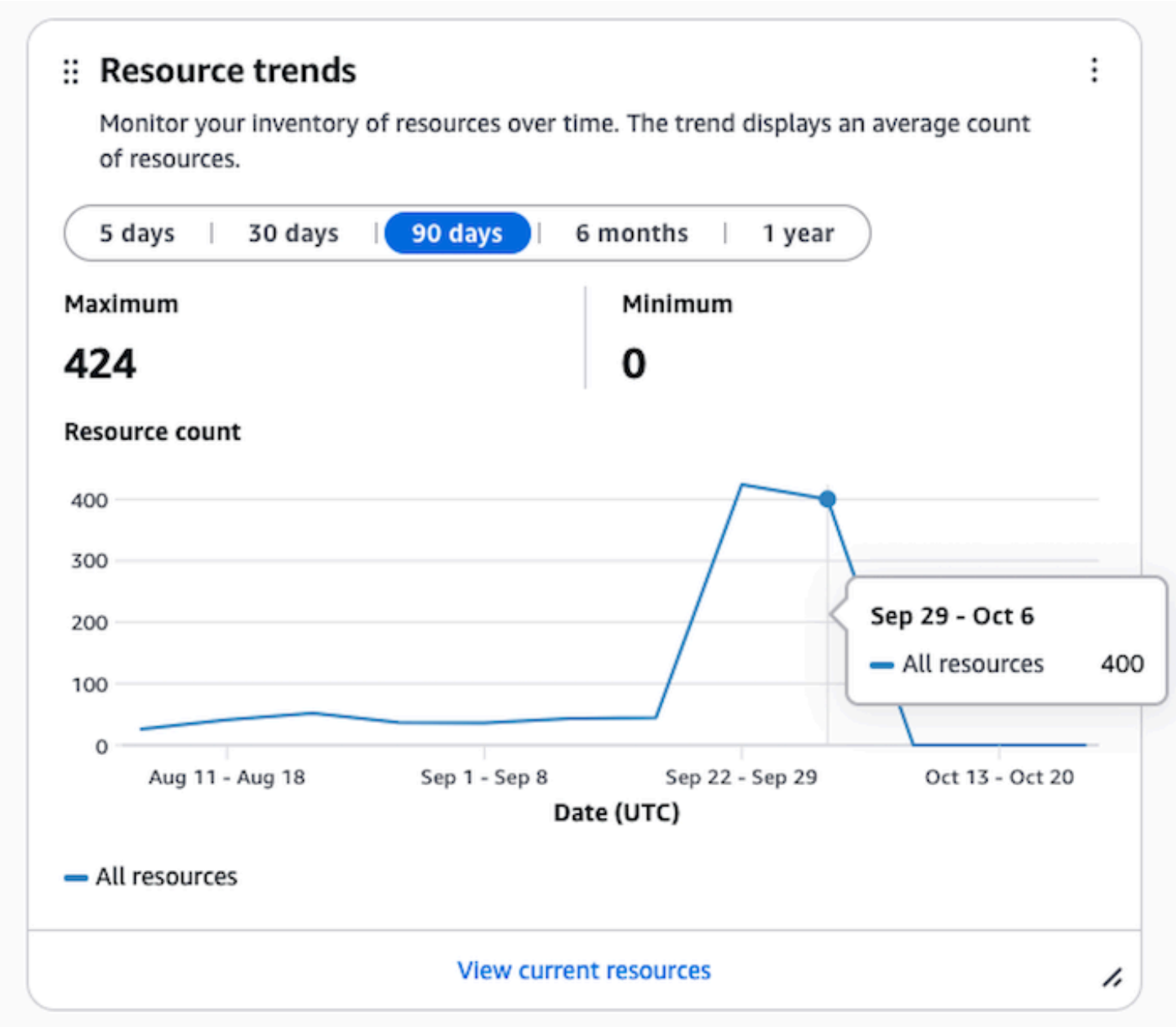
- Mortal
- Critical
- Alta
- Medio
- Baja
- Informativo
- Otros
- Desconocido

Los filtros de gravedad aplicados aparecen en diferentes cuadros en la parte inferior de la visualización. Puedes pasar el ratón por encima de la visualización para revisar el recuento promedio de hallazgos en momentos específicos. También puedes revisar el recuento promedio de hallazgos que coinciden con cada filtro de gravedad aplicado.

Puede elegir Ver todos los hallazgos de amenazas actuales para que se le dirija al panel de exposición. De forma predeterminada, el panel de amenazas solo muestra los datos de tendencias de los últimos 90 días. Si su cuenta no contiene información sobre amenazas detectadas hace más de 30 días, el panel muestra los datos de tendencias según el período de tiempo más adecuado.

> **Note**
>
> Para recibir datos en este widget, debes activarlo. GuardDuty

Widget de tendencias de recursos



Este widget muestra un inventario de tus recursos en los siguientes períodos de tiempo:

- 5 días
- 30 días
- 90 días
- 6 meses
- 1 año

La visualización muestra el recuento promedio de sus recursos durante el período de tiempo seleccionado. Puedes pasar el ratón por encima de la visualización para revisar el recuento promedio de recursos en momentos específicos.

Puedes elegir Ver los recursos actuales para que te dirijan al panel de recursos. De forma predeterminada, el panel de recursos solo muestra los datos de tendencias de los últimos 90 días. Si su cuenta no contiene recursos con una antigüedad superior a 30 días, el panel muestra los datos de tendencias según el período de tiempo más adecuado.

Este widget muestra un inventario de tus recursos en los siguientes períodos de tiempo:

- 5 días
- 30 días
- 90 días
- 6 meses
- 1 año

Retención de datos para conocer las tendencias

Security Hub conserva los datos de tendencias durante un año en todos los Cuentas de AWS lugares en los que Security Hub está activado. Una vez que los datos de tendencias se conservan durante un año, se eliminan de Security Hub.

Los datos de tendencias de las cuentas independientes y de administrador delegado se eliminan cuando se desactiva Security Hub o si se cierran las cuentas.

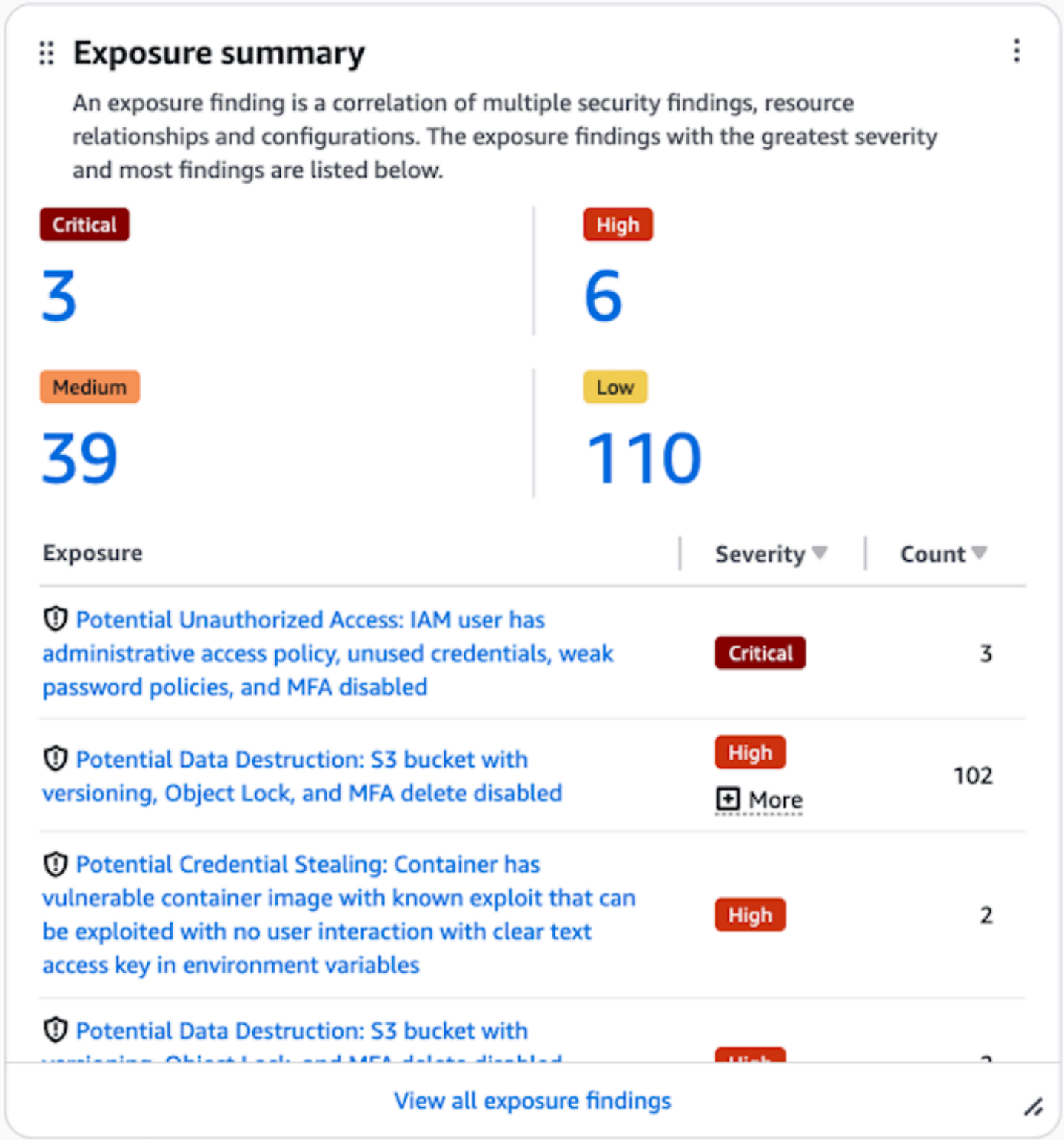
Escenarios de retención de datos de Trends para cuentas de miembros con Security Hub activado:

- Si una cuenta de miembro abandona su organización, Security Hub seguirá almacenando los datos de tendencias, hasta el momento en que la cuenta dejó la organización, durante un año.
- Si Security Hub está inhabilitado para una cuenta de miembro, Security Hub conserva los datos de tendencias, hasta el momento en que se inhabilitó la cuenta, durante un año.
- Si se cancela la cuenta de un miembro, Security Hub desvincula los datos de tendencias de la cuenta cancelada (por ejemplo, borra el ID de la cuenta cancelada) y conserva el resto de los datos de tendencias durante un año.

Widgets de resumen

Los siguientes widgets muestran un resumen de sus exposiciones, amenazas y recursos.

Widget de resumen de exposiciones

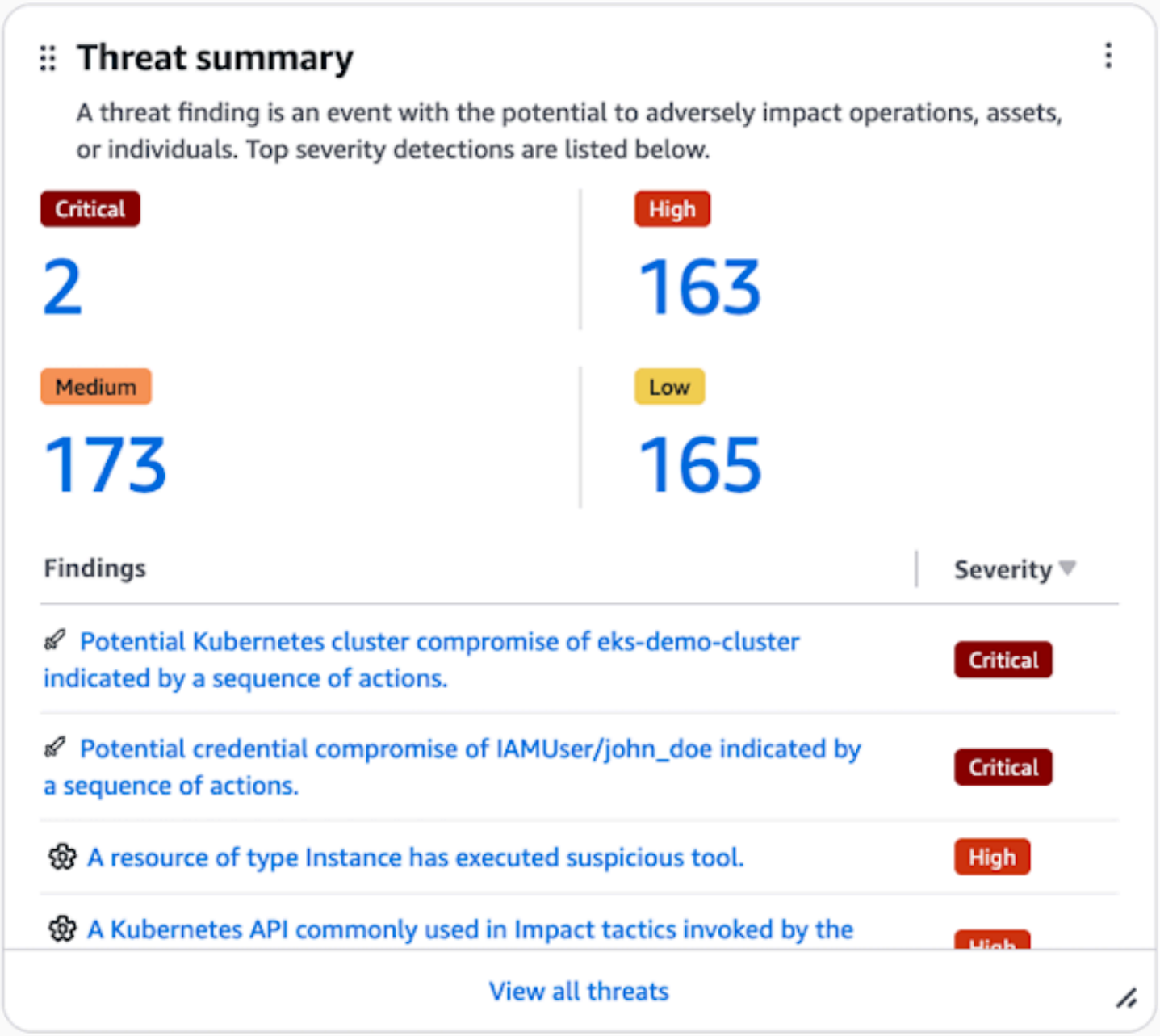


Este widget muestra tus exposiciones por gravedad. La exposición se basa en un análisis de las conclusiones y características de Security Hub y otros servicios de AWS seguridad, como Amazon

Inspector. La lista de exposiciones de este widget se limita a las ocho exposiciones de mayor gravedad. Las exposiciones con mayor gravedad aparecen en primer lugar de la lista. Si dos o más exposiciones tienen la misma gravedad, la lista agrupa automáticamente esas exposiciones detrás de las exposiciones más recientes. Al seleccionar Ver todas las exposiciones, accederá al panel de exposición.

> **Note**
>
> Para recibir datos en este widget, debe habilitar Amazon Inspector y Security Hub CSPM.

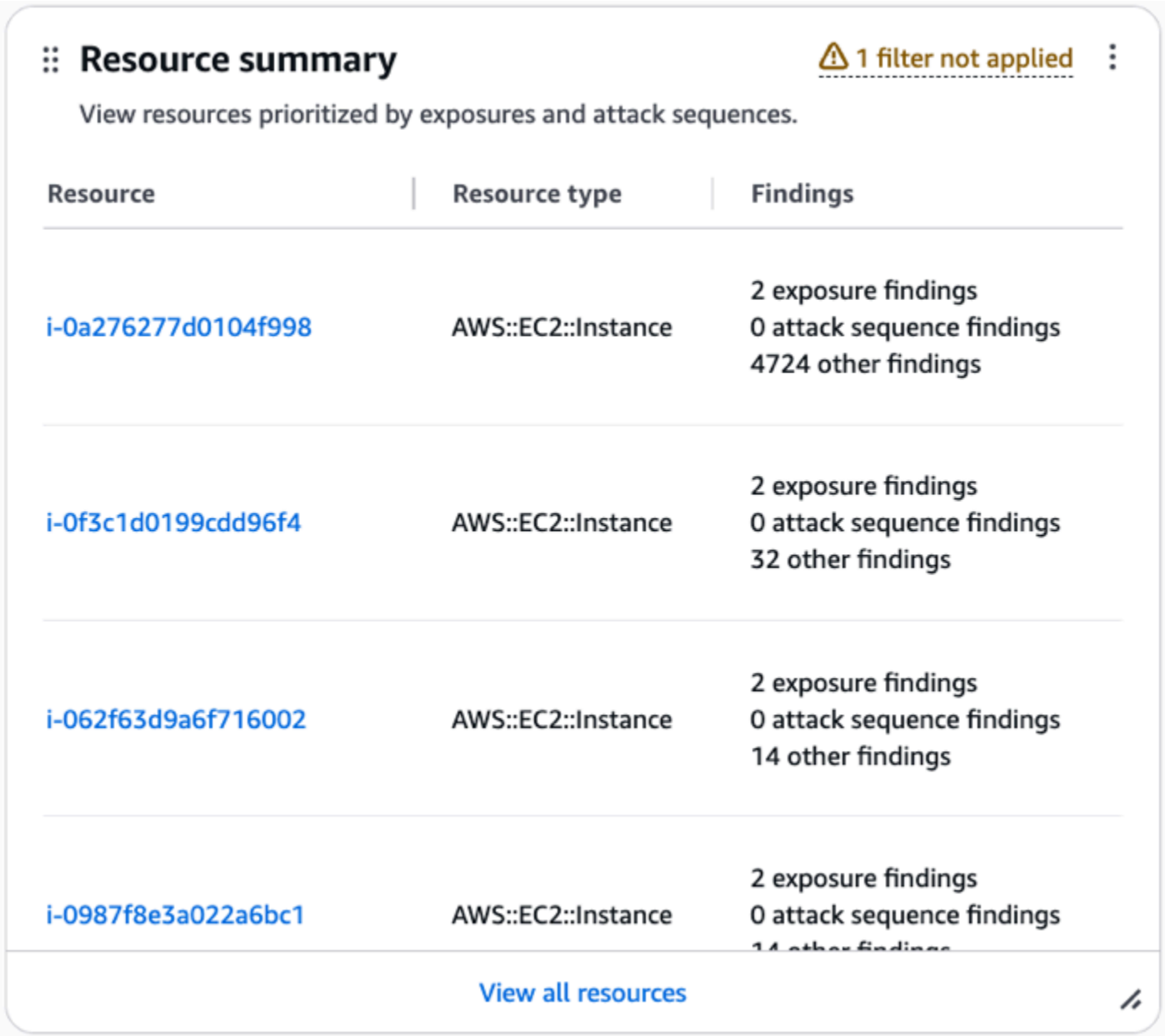
Widget de resumen de amenazas



Este widget muestra las amenazas por gravedad. Una amenaza se refiere a una actividad maliciosa o sospechosa que puede comprometer la seguridad de su entorno. La lista de amenazas en este widget se limita a las ocho amenazas con mayor gravedad. Las amenazas de mayor gravedad aparecen en primer lugar de la lista. Si dos o más amenazas tienen la misma gravedad, la lista las agrupa automáticamente detrás de las amenazas más recientes. Al seleccionar Ver todas las amenazas, accederá al panel de amenazas.

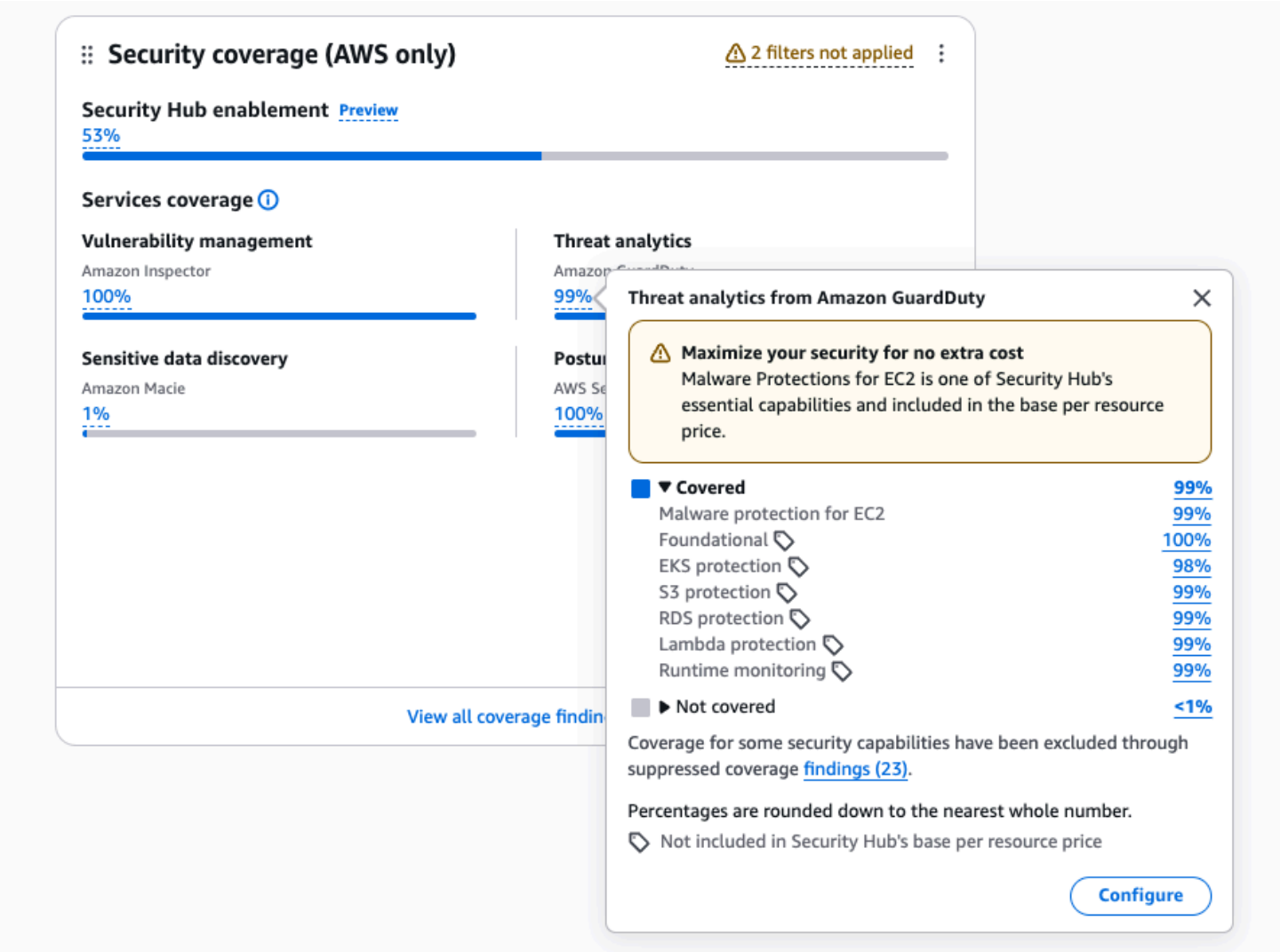
> **Note**
>
> Para recibir datos en este widget, debe habilitarlo GuardDuty.

Widget de resumen de recursos



Este widget muestra los recursos por tipo y los hallazgos asociados a los recursos. Los recursos se priorizan según las exposiciones y las secuencias de ataque. Al seleccionar Ver todos los recursos, accederá al panel de recursos.

Widget de cobertura de seguridad



El widget muestra un resumen de la cobertura de tu cuenta en relación con las siguientes funciones de seguridad:

- Gestión de vulnerabilidades por parte de Amazon Inspector
- Detección de amenazas por parte de Amazon GuardDuty
- Descubrimiento de datos confidenciales por parte de Amazon Macie
- Gestión de posturas mediante AWS Security Hub CSPM

En las cuentas de administrador delegado, el widget también muestra la cobertura de la cuenta para la activación de Security Hub.

Cada elemento de cobertura muestra un porcentaje que representa la activación de esa capacidad en sus cuentas. Al elegir un porcentaje, se muestran detalles sobre la cobertura de esa capacidad. Al elegir el porcentaje de activación de Security Hub, se muestra un panel lateral. El panel muestra cuántas cuentas están habilitadas en cada región de su organización.

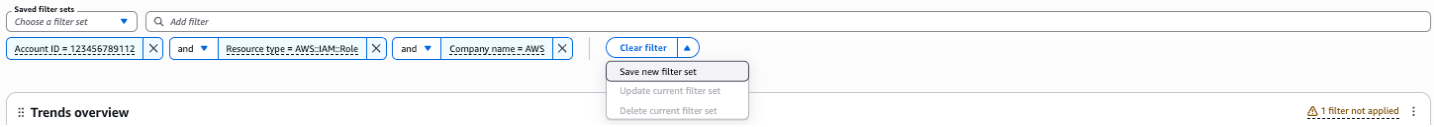
En la sección Cobertura de los servicios, los porcentajes representan la proporción de comprobaciones de cobertura aprobadas para cada función de seguridad. Estas comprobaciones abarcan las cuentas y regiones en las que Security Hub está activado. Al seleccionar un porcentaje de cobertura, aparece una ventana emergente en la que se desglosa cada función como Cubierta (comprobación aprobada) o No cubierta (comprobación fallida). Los porcentajes se redondean hacia abajo al número entero más cercano. Al seleccionar cualquier porcentaje en la ventana emergente, se abre la página de resultados de cobertura con detalles sobre los resultados que componen ese porcentaje. Seleccione Configurar para abrir el servicio individual, donde puede administrar la configuración de esa capacidad, o para abrir la página de configuraciones de Security Hub, donde puede actualizar las configuraciones de los servicios de seguridad.

Si se suprime alguno de sus datos de cobertura en Security Hub, el widget muestra un mensaje en el que se le informa de que se ha excluido la cobertura: Se ha excluido la cobertura de las capacidades de seguridad porque se ha suprimido la cobertura.

Para obtener más información sobre cómo ver y eliminar los datos de cobertura, consulta los resultados de cobertura en Security Hub.

Filtros disponibles

Puede aplicar filtros a los widgets de seguridad mediante la barra de agregar filtros.



Los filtros se organizan en las siguientes categorías:

- Filtros compartidos: se aplican a todos los widgets de seguridad
- Filtros de búsqueda: se aplica a los widgets de seguridad que muestran datos de búsqueda
- Filtros de recursos: se aplican a los widgets de seguridad que muestran datos de recursos

Puedes crear un conjunto de filtros conectando los filtros con los operadores y/ y, a continuación, seleccionando Guardar nuevo conjunto de filtros en el menú desplegable.

Filtros aplicados al widget de tendencias de búsqueda de exposición y al widget de tendencias de búsqueda de amenazas

Actualmente, los filtros compatibles con estos widgets son los siguientes:

- ID de cuenta
- Buscando el nombre de la clase
- Tipo de resultado
- Product name (Nombre del producto)
- Region
- Estado

Filtros aplicados al widget de tendencias de recursos

Actualmente, los filtros compatibles con este widget incluyen los siguientes:

- ID de cuenta
- Region
- Categoría de recurso
- Tipo de recurso

Los filtros no se aplican a los widgets

Si un widget no admite un filtro, el filtro no se aplica al widget. En este caso, el widget muestra un mensaje de advertencia que indica cuántos filtros no se han aplicado y muestra los nombres de los filtros que no admite.

Visualización de detalles sobre los recursos en Security Hub

La página Recursos lleva un registro de los recursos comunes en la cuenta y en la organización. Puede acceder a la página Recursos en la consola de Security Hub al seleccionar Recursos en

el panel de navegación. La ventaja que aporta la página Recursos es que ayuda a supervisar la posición de seguridad, organizar los recursos y revisar información detallada sobre estos. Cuando elige un tipo de recurso, puede revisar todos los recursos asociados a ese tipo. Puede revisar cualquier resultado asociado a un recurso. Los tipos de recursos disponibles en la página de recursos incluyen todos los recursos de sus cuentas cubiertos por los servicios de AWS seguridad que contribuyen a la publicación de sus hallazgos en Security Hub.

> **Note**
>
> El administrador delegado puede ver todos los recursos asociados a las cuentas de miembro. Si has configurado una casa Región de AWS, puedes ver todos los recursos de tu casa Región de AWS desde Linked Regiones de AWS.

Si elige un recurso, puede revisar los detalles de ese recurso. Estos detalles incluyen el nombre del recurso, su ID, ARN, tipo y categoría. Puede revisar el ID de la cuenta asociada al recurso, la fecha de creación (marca de tiempo) y la región en la que se creó el recurso (Región de AWS). También puede revisar detalles de configuración adicionales sobre el recurso. Estos detalles se encuentran en un fragmento JSON que puede copiar.

Si cambia de la pestaña Información general a la pestaña Resultados, puede revisar cualquier resultado asociado al recurso. La pestaña Resultados muestra el nombre de cada resultado, su tipo y su gravedad. Puede agrupar resultados por distintos campos y buscar resultados mediante filtros. Si elige un resultado, puede revisar una vista general del resultado, que incluye información sobre cumplimiento y la forma de remediar los problemas asociados con ese resultado. La pestaña Condiciones muestra cada condición que se haya identificado sobre el recurso. Puede ver las condiciones que contribuyen a generar un resultado de exposición para el recurso. También puede ver condiciones contextuales, que son otros elementos de seguridad identificados para el recurso pero que no contribuyeron directamente a ningún resultado de exposición. Si regresa al recurso, puede seleccionar Abrir recurso para revisarlo en la consola según su tipo de recurso. Por ejemplo, si el recurso es un recurso de IAM, puede abrirlo en la consola de IAM.

La página Recursos ofrece distintas formas de organizar y buscar recursos. Puede agrupar recursos por tipo. Por ejemplo, puedes agrupar los recursos por ID de cuenta, tipo de búsqueda Región de AWS, categoría de recurso, nombre de recurso y tipo de recurso. Los filtros rápidos ayudan a revisar recursos por categoría, cuentas y tipos de resultados.

Security Hub y el marco de esquemas abiertos de ciberseguridad (OCSF)

Security Hub utiliza el marco abierto de esquemas de ciberseguridad (OCSF) como formato estándar para todos los hallazgos de seguridad. En este tema se describe el OCSF y cómo lo implementa Security Hub.

Descripción general de OCSF

Los hallazgos de Security Hub se formatean utilizando OCSF (marco abierto de esquemas de ciberseguridad). OCSF es un proyecto de código abierto que ofrece un marco ampliable para desarrollar esquemas, junto con un esquema de seguridad central independiente del proveedor. Los proveedores y otros productores de datos pueden adoptar y ampliar el esquema para sus dominios específicos. Los productores de datos pueden mapear diferentes esquemas para ayudar a los equipos de seguridad a simplificar la incorporación y la normalización de los datos, de modo que los científicos y analistas de datos puedan trabajar con un lenguaje común para la detección e investigación de amenazas. El objetivo es proporcionar un estándar abierto, que se adopte en cualquier entorno, aplicación o solución y que complemente los estándares y procesos de seguridad existentes.

El marco se compone de tipos de datos, un diccionario de atributos y una taxonomía. Aunque no se limita a la ciberseguridad o a los eventos, el enfoque inicial está en los esquemas de eventos de ciberseguridad. El OCSF es independiente del formato de almacenamiento, los métodos de recopilación de datos y los procesos de ETL.

Security Hub admite actualmente las conclusiones de la versión 1.6 del esquema OCSF.

Recursos relacionados

Para obtener más información sobre OCSF y su implementación, consulte los siguientes recursos:

- Documentación pública sobre OCSF
- Documentación sobre el uso de extensiones OCSF
- Referencia del esquema principal de OCSF
- Registro de extensiones de OCSF

AWS extensión para OCSF

Los esquemas OCSF se pueden ampliar añadiendo nuevos atributos, objetos, categorías, perfiles y clases de eventos. Un esquema es la agregación de las entidades y extensiones principales del esquema.

Las extensiones de OCSF permiten a un proveedor o cliente concreto ampliar un esquema existente añadiendo atributos para ofrecer una personalización específica del dominio, mejorar la interoperabilidad de los datos y añadir un contexto más detallado para el análisis de seguridad.

La AWS extensión para el marco abierto de esquemas de ciberseguridad (OCSF) proporciona definiciones de atributos para los recursos de la nube dentro de los eventos de OCSF. Esta extensión agrega un `cloud_resources` perfil que amplía el `resource_details` objeto OCSF con atributos de recursos específicos de la nube. Con estos atributos, los equipos de seguridad pueden analizar las configuraciones de los recursos, las posibles vulnerabilidades y los metadatos de detección de amenazas.

Objeto **`resource_details`** extendido

La AWS extensión amplía el `resource_details` objeto con los atributos que se mencionan en la lista de referencias de atributos que aparece a continuación. Estos atributos garantizan la identificación y clasificación adecuadas de los recursos de la nube entre los diferentes proveedores dentro de marcos de eventos estandarizados.

AWS Extensión para la referencia de atributos de OCSF

En las secciones Atributos básicos y Objetos específicos del recurso se proporcionan ejemplos de cada uno de los atributos que forman parte de la extensión AWS OCSF de resource_details.

Cada una de las definiciones de atributos contiene un estado de OCSF que describe su relación actual con el esquema OCSF público:

- Existente: este atributo ya estaba en el estándar resource_details del OCSF y ahora forma parte de la extensión. AWS
- Nuevo: el atributo no forma parte de OCSF y se introdujo como parte de la extensión. AWS No existe en el esquema central de OCSF.
- Añadido a resource_details: el atributo está definido en OCSF pero no forma parte de resource_details.

Atributos básicos

Estos son atributos fundamentales que se utilizan para la identificación, la ubicación y los metadatos básicos de los recursos. Consisten en tipos de datos simples, como cadenas, marcas de tiempo y matrices.

Partición en la nube

La partición de nube en la que existe el recurso.

Requisito

Recomendado

Tipo

Cadena

Estado de OCSF

Existentes

Ejemplo

```
{
  "resources": [
    {
      "cloud_partition": "aws"
    }
  ]
}
```

ID de la cuenta de propietario

Un identificador de cuenta de 12 dígitos al que pertenece el recurso.

Requisito

Recomendado

Tipo

Cadena

Estado de OCSF

Existentes

Ejemplo

```
{
  "resources": [
    {
      "owner": {
        "account": {
          "uid": "123456789012"
        }
      }
    }
  ]
}
```

Tipo de recurso

El tipo AWS CloudFormation de recurso que identifica el servicio y el recurso específicos.

Requisito

Obligatorio

Tipo

Cadena

Formato

Debe seguir la convención de nomenclatura de los tipos de AWS CloudFormation recursos: `AWS::<Service>::<ResourceType>`

Estado de OCSF

Existentes

Ejemplo

```
{
  "resources": [
    {
```

```
      "type": "AWS::EC2::Instance"
    }
  ]
}
```

Identificador de recursos

El identificador único del recurso en la nube (por ejemplo, i-1234567890abcdef0).

Requisito

Recomendado

Tipo

Cadena

Formato

Debe ser un identificador de recurso válido. Longitud mínima de 1. Longitud máxima de 768.

Estado de OCSF

Existentes

Ejemplo

```
{
  "resources": [
    {
      "uid": "i-1234567890abcdef0"
    }
  ]
}
```

Identificador de recurso alternativo

El identificador único del recurso en la nube, normalmente el nombre del recurso de Amazon (ARN).

Requisito

Recomendado

Tipo

Cadena

Formato

Debe ser un AWS ARN válido. Los patrones comunes incluyen lo siguiente:

- `"arn:partition:service:region:account-id:resource-id"`
- `"arn:partition:service:region:account-id:resource-type/resource-id"`
- `"arn:partition:service:region:account-id:resource-type:resource-id"`

Nota: Algunos servicios, como S3, utilizan variantes como arn:aws:s3: ::bucket-name (sin región ni identificador de cuenta).

Estado de OCSF

Existentes

Ejemplos

```
{
  "resources": [
    {
      "uid_alt": "arn:aws:ec2:us-east-1:123456789012:instance/i-1234567890abcdef0"
    }
  ]
}
```

```
{
  "resources": [
    {
      "uid_alt": "arn:aws:s3:::my-bucket-name"
    }
  ]
}
```

Nombre del recurso

El nombre único del recurso en la nube.

Requisito

Recomendado

Tipo

Cadena

Formato

User-created nombres cuyos valores dependerán del entorno.

estado de OCSF

Existentes

Ejemplo

```
{
  "resources": [
    {
      "name": "My-Server-1"
    }
  ]
}
```

Región de nube

La AWS región en la que se encuentra el recurso.

Requisito

Recomendado

Tipo

Cadena

Formato

Identificador de región de nube válido (por ejemplo, us-east-1, eu-west-1, ap-southeast-2)

Estado de OCSF

Existentes

Ejemplo

```
{
```

```
  "resources": [
    {
      "region": "us-west-2"
    }
  ]
}
```

Hora de creación del recurso

La hora en que se creó el recurso.

Requisito

Recomendado

Tipo

Timestamp

Formato

Marca de tiempo de Unix en milisegundos desde la época (1 de enero de 1970, 00:00:00 UTC)

Estado de OCSF

Existentes

Ejemplo

```
{
  "resources": [
    {
      "created_time": 1762019193000
    }
  ]
}
```

Tags

Key-value pares para la organización y los metadatos de los recursos.

Requisito

Recomendado

Tipo

Matriz de objetos clave:valor

Formato

Un objeto genérico que permite definir un par clave:valor.

Estado de OCSF

Existentes

Ejemplo

```
{
  "resources": [
    {
      "tags": [
        {
          "name": "Environment",
          "value": "Production"
        },
        {
          "name": "Owner",
          "value": "SecurityTeam"
        }
      ]
    }
  ]
}
```

Dirección IP

La dirección IP asociada a la instancia en formato IPv4 o IPv6.

Requisito

Opcional

Tipo

Cadena

Formato

Dirección IPv4 o IPv6 válida

Estado de OCSF

Existentes

Ejemplo

```
{
  "resources": [
    {
      "ip": "10.0.1.25"
    }
  ]
}
```

Direcciones IP

Un conjunto de direcciones IP (IPv4 o IPv6) asociadas al dispositivo. Estas pueden incluir direcciones IP públicas y privadas.

Requisito

Opcional

Tipo

Matriz de direcciones IP

Estado de OCSF

New

Ejemplo

```
{
  "resources": [
    {
      "ip_addresses": ["10.0.1.25", "52.12.34.56"]
    }
  ]
}
```

IDENTIFICADOR DE VPC

El ID de VPC en el que se encuentra el recurso.

Requisito

Opcional

Tipo

Cadena

Formato

Identificador de VPC (por ejemplo, vpc-12345678900)

Estado de OCSF

Añadido a `resource_details`

Ejemplo

```
{
  "resources": [
    {
      "vpc_uid": "vpc-0a1b2c3d4e5f6g7h8"
    }
  ]
}
```

Ejemplo de objeto de recurso con atributos básicos

```
{
  "resources": [
    {
      "cloud_partition": "aws",
      "owner": {
        "account": {
          "uid": "123456789012"
        }
      },
      "region": "us-east-1",
      "type": "AWS::EC2::NetworkInterface",
      "uid": "eni-03e6c892dd45e836c",
```

```
      "uid_alt": "arn:aws:ec2:us-east-1:123456789012:network-interface/
eni-03e6c892dd45e836c",
      "zone": "us-east-1f",
      "vpc_uid": "vpc-0ef6045717b0362f6"
    }
  ]
}
```

Objetos específicos de un recurso

Se trata de objetos anidados complejos que proporcionan información detallada sobre tipos de recursos y servicios específicos. Cada objeto contiene varios campos y subobjetos con una configuración y unos metadatos específicos del servicio.

Dispositivo

Atributos de instancia en la nube mejorados para los recursos informáticos, incluidos los detalles de cifrado, la información de la imagen, el perfil de la instancia y la hora de lanzamiento.

Requisito

Opcional

Tipo

Objeto

Estado de OCSF

Añadido a. `resource_details` Consulte la definición del objeto del dispositivo OCSF.

AWS La extensión agrega los siguientes atributos a este objeto:

- `encryption_details`- Los detalles de cifrado del recurso
- `image`- Información de imagen
- `instance_profile`- El perfil de la instancia de IAM que se va a asociar a la instancia
- `launch_time`- La hora en que se lanzó la instancia
- `uid_alt`- Nombre de recurso de Amazon (ARN) del recurso

Ejemplo

```
{
  "device": {
    "image": {
      "uid": "ami-99999999",
      "name": "LoadTestAMI-Current"
    },
    "instance_profile": {
      "uid": "LoadTestingInstanceProfileId",
      "uid_alt": "arn:aws:iam::012345678999:instance-profile/generated"
    },
    "launch_time": 1762019193000,
    "launch_time_dt": "2025-08-02T02:05:06Z",
    "model": "m3.xlarge",
    "network_interfaces": [
      {
        "ip": "198.51.100.0",
        "security_groups": [
          {
            "name": "LoadTestingSecurityGroupName",
            "uid": "LoadTestingSecurityId"
          }
        ],
        "uid": "eni-abcdef12"
      }
    ],
    "type": "Virtual",
    "type_id": 6,
    "uid": "i-99999999"
  }
}
```

Interfaz de red

Detalles y configuración de la interfaz de red, incluidos los archivos adjuntos y los grupos de seguridad.

Requisito

Opcional

Tipo

Objeto

Estado de OCSF

Añadido a. `resource_details` Consulte la definición del objeto de la interfaz de red OCSF.

AWS La extensión agrega los siguientes atributos a este objeto:

- `attachments`- Información sobre los archivos adjuntos de la interfaz de red
- `security_groups`- Conjunto de identificadores únicos de grupos de seguridad
- `uid_alt`- Nombre de recurso de Amazon (ARN) del recurso

Ejemplo

```
{
  "network_interface": {
    "uid": "eni-0a1b2c3d4e5f6g7h8",
    "uid_alt": "arn:aws:ec2:us-east-1:123456789012:network-interface/
eni-0a1b2c3d4e5f6g7h8",
    "name": "prod-web-server-eni",
    "attachments": [
      {
        "uid": "eni-attach-0abcd1234efgh5678",
        "instance_uid": "i-0123456789abcdef0",
        "name": "/dev/eth0",
        "state": "attached",
        "attach_time": 1762019193000
      }
    ],
    "security_groups": [
      {
        "uid": "sg-0a1b2c3d4e5f6g7h8",
        "name": "web-server-sg"
      },
      {
        "uid": "sg-9i8h7g6f5e4d3c2b1",
        "name": "ssh-access-sg"
      }
    ]
  }
}
```

Dispositivo de almacenamiento

Detalles del dispositivo de almacenamiento, incluidos los datos adjuntos, el cifrado y las instantáneas.

Requisito

Opcional

Tipo

Objeto

Estado de OCSF

New

El objeto de dispositivo de almacenamiento incluye los siguientes atributos:

- `name`- El nombre del dispositivo de almacenamiento
- `uid`- El identificador único del dispositivo de almacenamiento
- `attachments`- Los archivos adjuntos del dispositivo de almacenamiento
- `encryption_details`- La clave de cifrado del dispositivo de almacenamiento
- `is_encrypted`- Si el dispositivo de almacenamiento está cifrado (obligatorio)
- `snapshot_id`- El identificador de instantáneas del dispositivo de almacenamiento
- `uid_alt`- El nombre del recurso de Amazon (ARN) del recurso

Ejemplo

```
{
  "storage_device": {
    "is_encrypted": false,
    "name": "LocalVolumeDeviceName1",
    "snapshot_id": "snap-12345678901234567",
    "uid": "vol-09d5050dea915943d",
    "uid_alt": "arn:aws:ec2:us-west-2:123456789000:volume/vol-09d5050dea915943d"
  }
}
```

Base de datos

Los atributos de la instancia de base de datos incluyen el tipo de motor, el punto final y la información del usuario.

Requisito

Opcional

Tipo

Objeto

Estado de OCSF

Añadido a. `resource_details` Consulte la definición del objeto de la base de datos OCSF.

AWS La extensión agrega los siguientes atributos a este objeto:

- `cluster_uid`- El identificador del clúster de la base de datos
- `db_endpoint`- El punto final de la base de datos
- `encryption_details`- Los detalles de cifrado de la base de datos
- `engine`- El nombre del motor de la base de datos (por ejemplo, mysql)
- `is_encrypted`- Si la base de datos está cifrada
- `is_iam_authentication`- Si la autenticación de IAM está habilitada
- `is_public`- Si la base de datos es de acceso público
- `port`- El número de puerto de la base de datos
- `security_groups`- Matriz de grupos de seguridad de VPC asociados a la instancia de base de datos
- `snapshot_details`- Los detalles de la instantánea de la base de datos
- `status`- El estado de la base de datos (por ejemplo, disponible)
- `subnet_group`- Un grupo de subredes de base de datos es un conjunto de subredes de una VPC
- `uid_alt`- Nombre de recurso de Amazon (ARN) del recurso
- `user`- El usuario de la base de datos
- `version`- La versión de la base de datos

Ejemplo

```
{
  "database": {
    "cluster_uid": "SampleDBClusterId",
    "engine": "mysql",
    "is_iam_authentication": true,
    "is_public": false,
    "type": "Relational",
    "type_id": 1,
    "uid": "SampleDBId",
    "version": "13.6"
  }
}
```

Grupo de bases de datos

Los atributos de la instancia de base de datos incluyen el tipo de motor, el punto final y la información del usuario.

Requisito

Opcional

Tipo

Objeto

Estado de OCSF

New

El objeto de base de datos incluye los siguientes atributos:

- `uid`- El identificador único del clúster de bases de datos
- `uid_alt`- El nombre del recurso de Amazon (ARN) del recurso
- `name`- El nombre del clúster de bases de datos
- `status`- El estado del clúster de bases de datos
- `engine`- El motor asociado al clúster
- `version`- La versión del clúster de bases de datos
- `cluster_members`- Lista de instancias de bases de datos que forman parte del clúster
- `security_groups`- Matriz de grupos de seguridad asociados al clúster

- `is_encrypted`- Si el clúster de la base de datos está cifrado
- `is_iam_authentication`- Si la autenticación de IAM está habilitada
- `encryption_details`- Los detalles de cifrado del clúster de bases de datos
- `subnet_group`- El grupo de subredes asociado al clúster
- `port`- El número de puerto del clúster de bases de datos
- `zones`- Lista de zonas de disponibilidad
- `db_endpoint`- El punto final del clúster de bases de datos
- `snapshot_details`- Detalles de la instantánea de la base de datos

Ejemplo

```
{
  "db_cluster": {
    "uid": "production-aurora-cluster",
    "uid_alt": "arn:aws:rds:us-east-1:123456789012:cluster:production-aurora-cluster",
    "name": "production-aurora-cluster",
    "status": "available",
    "engine": "aurora-mysql",
    "version": "8.0.mysql_aurora.3.04.0",
    "cluster_members": [
      "instance-1",
      "instance-2"
    ],
    "security_groups": [
      {
        "uid": "sg-0a1b2c3d4e5f6g7h8",
        "name": "db-security-group"
      }
    ],
    "is_encrypted": true,
    "is_iam_authentication": true,
    "encryption_details": {
      "key_uid": "arn:aws:kms:us-
east-1:123456789012:key/12345678-1234-1234-1234-123456789012"
    },
    "subnet_group": {
      "uid": "production-db-subnet-group"
    },
    "port": 3306,
    "zones": [
```

```
      "us-east-1a",
      "us-east-1b",
      "us-east-1c"
    ],
    "db_endpoint": {
      "name": "production-aurora-cluster.cluster-abc123xyz.us-
east-1.rds.amazonaws.com",
      "port": 3306
    }
  }
}
```

Función de nube

Los atributos de las funciones en la nube para las funciones sin servidor incluyen la configuración del controlador, las capas y el tiempo de ejecución.

Requisito

Opcional

Tipo

Objeto

Estado de OCSF

New

El objeto de función en la nube incluye los siguientes atributos:

- `name`- El nombre de la función de nube
- `uid`- El identificador único de la función en la nube
- `uid_alt`- El nombre del recurso de Amazon (ARN) del recurso
- `encryption_details`- Los detalles de cifrado de la función en la nube
- `handler`- El método del código de función que procesa los eventos
- `layers`- La lista de capas de funciones de la nube que contienen código o datos complementarios
- `runtime`- El entorno específico del lenguaje de las funciones en la nube
- `security_groups`- Conjunto de grupos de seguridad asociados a la función de nube
- `subnet_info_list`- Detalles sobre las subredes asociadas a la función de nube

- `user`- Detalles sobre la entidad de IAM que concede el permiso de acceso a los servicios a cloud_function
- `version`- La versión de la función en la nube
- `vpc_uid`- El identificador único de la VPC si la función en la nube está en una VPC

Ejemplo

```
{
  "cloud_function": {
    "name": "my-lambda-function",
    "uid": "my-lambda-function",
    "uid_alt": "arn:aws:lambda:us-east-1:123456789012:function:my-lambda-function",
    "handler": "index.handler",
    "runtime": "python3.11",
    "version": "$LATEST",
    "layers": [
      {
        "name": "my-layer",
        "uid_alt": "arn:aws:lambda:us-east-1:123456789012:layer:my-layer:1",
        "version": "1"
      }
    ],
    "security_groups": [
      {
        "name": "lambda-security-group",
        "uid": "sg-0123456789abcdef0"
      }
    ],
    "subnet_info_list": [
      {
        "uid": "subnet-0a1b2c3d4e5f6g7h8"
      }
    ],
    "vpc_uid": "vpc-0ef6045717b0362f6"
  }
}
```

Cubeta de datos

Atributos de almacenamiento de datos o depósito de datos de S3.

Requisito

Opcional

Tipo

Objeto

Estado de OCSF

Añadido a. `resource_details` Consulte la definición del objeto OCSF Databucket.

Nota: La extensión agrega este objeto a resource_details. AWS El objeto Databucket principal de OCSF se usa sin atributos adicionales.

Ejemplo

```
{
  "databucket": {
    "type": "S3",
    "type_id": 1,
    "uid": "my-bucket-name"
  }
}
```

Image

Información de imagen para los recursos informáticos, incluidos los detalles de uso y plataforma.

Requisito

Opcional

Tipo

Objeto

Estado de OCSF

Añadido a. `resource_details` Consulte la definición del objeto de imagen de OCSF.

AWS La extensión agrega los siguientes atributos a este objeto:

- `platform`- La plataforma del sistema operativo de la imagen
- `in_use_count`- Recuento de recursos que utilizan esta imagen

Ejemplo

```
{
  "image": {
    "uid": "ami-0abcdef1234567890",
    "uid_alt": "arn:aws:ec2:us-east-1:123456789012:image/ami-0abcdef1234567890",
    "name": "my-custom-ami",
    "platform": "AMAZON_LINUX_2",
    "in_use_count": 2
  }
}
```

Información de subred

Detalles sobre la subred en la que se encuentra el recurso.

Requisito

Opcional

Tipo

Objeto

Estado de OCSF

New

El objeto de información de subred incluye los siguientes atributos:

- `uid`- El identificador único de la subred
- `uid_alt`- El nombre del recurso de Amazon (ARN) del recurso
- `name`- El nombre de la subred
- `zone`- La zona de disponibilidad
- `ip_count`- El número de direcciones IP de la subred
- `cidr_block`- El bloque CIDR de la subred

- `is_default`- Si esta es la subred predeterminada
- `is_public`- Si la subred es de acceso público
- `state`- El estado de la subred
- `vpc_uid`- El ID de VPC donde se encuentra la subred

Ejemplo

```
{
  "subnet_info": {
    "uid": "subnet-0a1b2c3d4e5f6g7h8",
    "uid_alt": "arn:aws:ec2:us-east-1:123456789012:subnet/subnet-0a1b2c3d4e5f6g7h8",
    "name": "production-web-subnet-1a",
    "zone": "us-east-1a",
    "ip_count": 251,
    "cidr_block": "10.0.1.0/24",
    "is_default": false,
    "is_public": true,
    "state": "available",
    "vpc_uid": "vpc-0123456789abcdef0"
  }
}
```

Usuario

Los atributos del usuario de IAM incluyen políticas y perfiles de instancia.

Requisito

Opcional

Tipo

Objeto

Estado de OCSF

Añadido a. `resource_details` Consulte la definición del objeto de usuario de OCSF.

El objeto de usuario incluye los siguientes atributos:

- `instance_profiles`- Lista de perfiles de instancia adjuntos a una instancia en la nube

- `policies`- Políticas que asignan permisos a usuarios, grupos, roles y recursos

Ejemplo

```
{
  "user": {
    "type_id": 1,
    "uid": "AIDACKCEVSQ6C2EXAMPLE",
    "uid_alt": "arn:aws:iam::123456789012:user/developers/john.doe",
    "name": "john.doe",
    "type": "User",
    "groups": [
      {
        "name": "Developers"
      },
      {
        "name": "ReadOnlyAccess"
      }
    ],
    "policies": [
      {
        "name": "AmazonS3ReadOnlyAccess"
      },
      {
        "name": "AmazonEC2ReadOnlyAccess"
      }
    ]
  }
}
```

Resultados de cobertura en Security Hub

Los resultados de cobertura de Security Hub permiten saber qué funciones de AWS seguridad están habilitadas y dónde pueden existir brechas de cobertura en una cuenta independiente o en las cuentas de los miembros de una organización. Actualmente, las conclusiones sobre la cobertura permiten informar sobre qué servicios y funciones están habilitados para Amazon GuardDuty, Amazon Inspector, Amazon Macie y AWS Security Hub CSPM. Estos resultados aparecen en el widget de cobertura de seguridad del panel de Security Hub, con la posibilidad de profundizar en vistas más detalladas según cada capacidad de seguridad.

Limitaciones

- En el caso de las cuentas de miembros, la información de cobertura se agrega de forma transversal Regiones de AWS, pero solo para esa cuenta de miembro.
- La información de cobertura no se muestra para las cuentas que no estén integradas en Security Hub.

Hallazgos de cobertura para AWS CSPM de Security Hub

Los resultados de la cobertura del CSPM de Security Hub evalúan si una cuenta cuenta cuenta con un estándar de seguridad cualificado para la gestión de posturas. La habilitación de cualquier estándar CSPM de Security Hub cumplirá los requisitos, con la excepción de las normas de etiquetado de recursos AWS Control Tower .

La detección de los estándares habilitados de forma predeterminada al habilitar el CSPM de Security Hub puede tardar hasta 24 horas.

Hallazgos de cobertura para Amazon GuardDuty

GuardDuty los resultados de cobertura evalúan si GuardDuty está habilitada y qué GuardDuty funciones están habilitadas en Cuenta de AWS:

- GuardDuty Protección contra malware para Amazon EC2: analiza las instancias de Amazon EC2 en busca de malware potencial.
- GuardDuty Protección de Amazon EKS: supervisa los registros de auditoría de Kubernetes para detectar amenazas en los clústeres de Amazon EKS.
- GuardDuty Protección Lambda: analiza las invocaciones de funciones de Lambda para detectar posibles amenazas.
- GuardDuty Protección de Amazon S3: analiza los eventos de datos para detectar posibles amenazas para los buckets de Amazon S3.
- GuardDuty Protección de Amazon RDS: monitorea las amenazas a las bases de datos de Amazon RDS.
- GuardDuty Supervisión del tiempo de ejecución: proporciona una supervisión en tiempo real del comportamiento del tiempo de ejecución en las instancias de Amazon EC2.
- GuardDuty Cobertura básica: GuardDuty funciones básicas que se activan automáticamente cuando GuardDuty están habilitadas.

> **Note**
>
> En el caso de GuardDuty la cobertura básica, los resultados de cobertura que indican que la función está desactivada significan que no GuardDuty está habilitada en la cuenta en la que se encontró la cobertura.

Las actualizaciones de la GuardDuty cobertura pueden tardar hasta 24 horas en reflejarse en todas las cuentas de los miembros de una organización.

Resultados de cobertura para Amazon Inspector

Los resultados de cobertura de Amazon Inspector evalúan si Amazon Inspector está habilitado y qué características están activadas en una cuenta:

- Escaneo con Inspector EC2: analiza las instancias de Amazon EC2 en busca de vulnerabilidades.
- Escaneo con Inspector ECR: escanea las imágenes de los contenedores de Amazon ECR en busca de vulnerabilidades.
- Escaneo estándar de Inspector Lambda: analiza las funciones de Lambda en busca de vulnerabilidades.
- Escaneo de código con Inspector Lambda: analiza las funciones del código Lambda en busca de vulnerabilidades en el código.

Resultados de cobertura de Amazon Macie

Los resultados de cobertura de Macie evalúan si Macie está habilitado en las Cuentas de AWS:

- Cobertura de descubrimiento automático de información confidencial de Macie: evalúa de forma continua los datos en Amazon S3 para identificar información confidencial.

Las actualizaciones de los resultados de cobertura del descubrimiento automático de información confidencial de Amazon Macie pueden tardar hasta 24 horas en reflejarse en todas las cuentas de miembro de una organización.

Supresión de los hallazgos de cobertura

De forma predeterminada, los resultados de la cobertura de seguridad evalúan qué funciones de Amazon GuardDuty, Amazon Inspector, Amazon Macie y AWS Security Hub CSPM están habilitadas para una cuenta y una región. Si determinadas funciones de seguridad no le son aplicables o representan un riesgo aceptado, puede utilizar la función de supresión para eliminar los resultados de cobertura de forma similar a todos los demás resultados. Cuando se suprime una búsqueda de cobertura, no se incluye en los cálculos de cobertura del widget de cobertura de seguridad. El widget muestra el siguiente mensaje: Se ha excluido la cobertura de las funciones de seguridad porque se ha detectado una cobertura suprimida. El mensaje incluye un recuento de los hallazgos suprimidos.

Para suprimir un hallazgo de cobertura en Security Hub

1. Cuando veas el widget de cobertura de seguridad, elige el enlace relativo al porcentaje de cobertura.
2. En la ventana emergente de cobertura, selecciona Ver los resultados de cobertura. Cada hallazgo con el estado de Nuevo describe una brecha de cobertura observada.
3. Seleccione la casilla de verificación situada junto a cada hallazgo que desee suprimir.
4. En la parte superior de la página, selecciona Estado de actualización y, a continuación, selecciona Suprimido.
5. En el cuadro de diálogo Definir estado como Suprimido, si lo desea, introduzca una nota que detalle el motivo del cambio de estado. Luego, elija Establecer estado.

Inventario de IA en Security Hub

El inventario de IA de AWS Security Hub proporciona una vista unificada de los recursos de inteligencia artificial (IA) y aprendizaje automático (ML) en todo el AWS entorno. Utilice el inventario de IA para identificar las cargas de trabajo de IA no autorizadas, comprender dónde se está ejecutando la IA y cómo se descubrió, y priorizar los recursos que requieren una revisión de seguridad más detenida. Security Hub organiza los recursos de IA en dos tipos de descubrimiento:

- Gestionado: recursos de IA que se AWS proporcionan como un servicio gestionado. Security Hub descubre estos recursos a partir de los elementos de AWS Config configuración. Los tipos de recursos gestionados incluyen un subconjunto compatible de Amazon Bedrock, Amazon Bedrock AgentCore y Amazon. SageMaker

- Self-hosted— Recursos de IA que no se proporcionan como un servicio gestionado. Algunos ejemplos son los modelos de código abierto, los agentes y los servidores de inferencia que se ejecutan en su propia computadora. Security Hub detecta estos recursos a partir de señales que contribuyen a las instancias de Amazon Elastic Compute Cloud (Amazon EC2) y a las imágenes de Amazon Elastic Container Registry (Amazon ECR). Las señales incluyen los hallazgos de la lista de materiales (SBOM) del software Amazon Inspector y la actividad del GuardDuty DNS de Amazon.

Las cuentas de administrador pueden ver los recursos de IA de todas las cuentas habilitadas de su organización. Las cuentas de los miembros solo pueden ver los recursos de IA de su propia cuenta.

Requisitos previos para el descubrimiento de IA autohospedado

El descubrimiento de los recursos de IA gestionados no requiere ninguna configuración adicional más allá de la activación de Security Hub. Para descubrir los recursos de IA autohospedados, también debes habilitar los Servicios de AWS que proporcionan las señales que contribuyen a ello:

- Amazon Inspector: permite que Amazon Inspector (con los elementos esenciales de Security Hub) genere SBOM. Security Hub utiliza estos SBOM para detectar modelos autohospedados, puntos finales de inferencia y agentes. Para las instancias Amazon EC2, habilite el escaneo basado en agentes con el modo de escaneo mejorado, el escaneo sin agente o el escaneo híbrido. Agent-based el escaneo sin el modo de escaneo mejorado no produce el inventario exhaustivo de software que requiere la detección de recursos de IA. Para las imágenes de Amazon ECR, Amazon Inspector proporciona SBOM mediante el escaneo de imágenes de contenedores.
- Amazon GuardDuty: habilítelo GuardDuty para que Security Hub pueda utilizar la actividad del DNS para detectar puntos de enlace de IA externos a los que llaman sus instancias de Amazon EC2.

Tipos de recursos de IA compatibles

Cuando esté disponible de forma general, Security Hub admite los siguientes tipos de recursos de IA autohospedados. Security Hub utiliza un sistema de detección basado en la confianza para los recursos de IA autohospedados. Cada detección está anclada a una señal principal, como un componente de la SBOM. A continuación, Security Hub correlaciona las señales adicionales para establecer la confianza antes de que un recurso aparezca en su inventario. Security Hub muestra solo los recursos que cumplen con el umbral de confianza, lo que ayuda a minimizar los falsos positivos. Cada recurso usa a `ResourceType` con el `SelfHosted::AI::` prefijo.

- Modelos (`SelfHosted::AI::Model`) — Modelos Hugging Face y Ollama. Security Hub detecta los modelos solo en los directorios de caché de modelos predeterminados (como las cachés Hugging Face y Ollama) y en las rutas personalizadas que usted configure para el escaneo de Amazon Inspector.
- Puntos finales de inferencia (`SelfHosted::AI::InferenceEndpoint`): software de servidor de modelos compatible, como VLLM, Ollama TorchServe, Triton, Text Generation Inference (TGI), SGlang, llama.cpp, LocalAI, BentoML, Xinference, Ray Serve y GPT4all.
- Agentes `SelfHosted::AI::Agent` () OpenClaw : agentes.
- Puntos de enlace externos (`SelfHosted::AI::ExternalEndpoint`): dominios de servicios de IA externos a los que llaman sus instancias de Amazon EC2. Security Hub mantiene una lista de dominios de servicios de IA conocidos, como OpenAI, Anthropic, Cohere, Mistral y otros proveedores de IA importantes, y detecta cuándo tus instancias les realizan solicitudes de DNS. Los puntos de enlace externos se detectan únicamente a partir de la actividad del GuardDuty DNS en Amazon EC2.

Los recursos de IA gestionados son un subconjunto compatible de los tipos de elementos de SageMaker configuración de Amazon Bedrock, Amazon Bedrock AgentCore y Amazon, cada uno con la `AI/ML` categoría de recursos.

Cómo encontrar recursos de IA en la página de recursos

En la página de recursos se enumeran todos los recursos de su entorno. En el caso de los recursos de IA, puede utilizar las siguientes funciones para identificar las cargas de trabajo de IA y los hosts que las ejecutan:

- AI/ML Los recursos gestionados muestran un icono de IA junto al recurso. Selecciona el icono para ver una descripción.
- Los recursos de alojamiento que ejecutan recursos de IA autohospedados, como las instancias de Amazon EC2, muestran una insignia de recuento de IA autohospedada. Los anfitriones que no tienen recursos de IA autohospedados no muestran ningún distintivo.
- Usa el botón de filtro rápido para mostrar solo los hosts que contienen recursos de IA autohospedados.
- Para obtener información detallada sobre un anfitrión, selecciónelo para abrir su panel de detalles, elija la pestaña de activos de IA y, a continuación, elija Ver todo para ver los recursos de IA autohospedados detectados en ese host.

Uso de la página de inventario de IA

La página de inventario de IA se centra en los recursos de IA de su organización. Todos los recursos de esta página pertenecen a la categoría `AI/ML` de recursos. Esta página muestra los recursos de AWS IA gestionados y los recursos de IA autohospedados en su entorno. En las siguientes secciones se describen los componentes principales de la página.

Barra de resumen

La barra de resumen muestra el número total de activos de IA y un desglose por tipo de descubrimiento, ya sea autohospedado o gestionado. También muestra un desglose por subcategoría, como modelo o agente. Elija el valor de una estadística para mostrar los detalles de respaldo en la tabla.

Agrupación, filtrado y búsqueda

La tabla de inventario de IA agrupa los recursos por tipo de recurso de forma predeterminada. Puede modificar la agrupación o eliminarla para obtener una vista plana de todos los recursos. Los campos de agrupación disponibles incluyen el identificador canónico, el tipo de recurso del host, el tipo de descubrimiento, el identificador de cuenta y el tipo de recurso.

El ID canónico identifica qué es un recurso, independientemente de dónde se ejecute. Por ejemplo, dos instancias de Amazon EC2 que ejecutan el mismo modelo de Hugging Face comparten el mismo ID canónico, de modo que puede encontrar todas las implementaciones de un modelo específico en su organización.

> **Note**
>
> Las agrupaciones canónicas de ID y tipo de recurso de host se aplican únicamente a los recursos autohospedados. Al agrupar por estos campos, los recursos de IA gestionados no aparecen en los resultados porque no tienen estos atributos. Usa el tipo de descubrimiento o las agrupaciones de tipos de recursos para ver juntos los recursos gestionados y los autohospedados.

Los filtros rápidos permiten filtrar por subcategoría de recursos o tipo de descubrimiento. Los filtros de propiedades admiten campos adicionales, como el tipo de recurso del host y el identificador canónico de los recursos autohospedados.

Detalles de los recursos y señales que contribuyen

Elija una fila de recursos para abrir el panel de detalles. En el caso de los recursos gestionados, el panel muestra la configuración del recurso en formato JSON. En el caso de los recursos autohospedados, el panel muestra las señales de contribución que Security Hub utilizó para detectar el recurso. Estas señales incluyen la fuente de detección y los detalles de las señales individuales, como los componentes de la SBOM y el software de inferencia compatible con un modelo, o el dominio DNS de un punto final externo.

Pasando al recurso del host

En el caso de un recurso de IA autohospedado, el panel de detalles muestra el recurso anfitrión en el que Security Hub detectó el recurso. Para ver todos los recursos de IA autohospedados en el mismo host, filtra la tabla por el recurso del host. Con esta vista, puede desglosar desde un recurso autohospedado individual hasta su anfitrión y revisar los recursos de IA adyacentes en ese host.

Consideraciones

En términos de disponibilidad general, el inventario de IA presenta las siguientes limitaciones:

- Self-hosted Los recursos de IA no incluyen resultados en esta versión. Security Hub muestra únicamente los recuentos de búsquedas de los recursos de IA gestionados.
- Self-hosted La detección de IA solo se admite en las instancias de Amazon EC2 y en las imágenes de Amazon ECR. AWS Lambda no se admiten funciones ni otros tipos de procesamiento.
- En esta versión, Security Hub no atribuye las imágenes de Amazon ECR a un host principal, por lo que los recuentos de IA del host no las incluyen.
- Security Hub detecta puntos de conexión externos a partir de la actividad de GuardDuty DNS únicamente en Amazon EC2. En esta versión, Security Hub no atribuye las llamadas de AWS Fargate, AWS Lambda Amazon, SageMaker Amazon EKS ni de ningún otro sistema informático gestionado por servicios.

Acceder al inventario de IA con la API

Puede recuperar los datos del inventario de IA mediante programación con la GetResourcesV2 y GetResourcesStatisticsV2las operaciones.

En el AI/ML caso de los recursos, la `GetResourcesV2` respuesta incluye los campos `ResourceSubCategory` y`DiscoveryType`. El `DiscoveryType` campo indica si un recurso

es `Managed` o`SelfHosted`. En el caso de los recursos de IA autohospedados y sus recursos anfitriones, la respuesta también incluye `ResourceInfo` una `AIDetails` estructura.

Self-hosted Los recursos de IA utilizan a `ResourceType` con el `SelfHosted::AI::` prefijo. Entre los tipos admitidos se incluyen los siguientes:

- `SelfHosted::AI::Model`
- `SelfHosted::AI::Agent`
- `SelfHosted::AI::InferenceEndpoint`
- `SelfHosted::AI::ExternalEndpoint`

La `AIDetails` estructura vincula un recurso de IA autohospedado a su anfitrión mediante los `HostResourceType` campos `HostResourceGuid` y. El `CanonicalId` campo identifica qué es un recurso, independientemente de dónde esté desplegado, para que puedas agregar recursos idénticos en varios hosts. El ID canónico usa un `type/identifier` formato:

- Para los modelos ML: `model/<purl>` (por ejemplo,) `model/pkg:huggingface/meta-llama/llama-3-8b`
- Para los puntos finales y los agentes de inferencia: un formato `type/asset-identifier-name`
- Para los puntos finales externos: el dominio normalizado (por ejemplo,) `api.*.openai.com`

En un recurso de host, como una instancia de Amazon EC2, `SelfHostedAI*ResourceCount` los campos y el `SelfHostedTotalAIResourceCount` campo contienen los recuentos de los recursos de IA autohospedados detectados en el host.

> **Note**
>
> Cuando utilice `GetResourcesV2` y filtre por`ResourceSubCategory`, también debe incluir un `ResourceCategory` filtro. Establezca la comparación en `EQUALS` y el valor en`AI/ML`. Este requisito también se aplica al agrupar por `ResourceSubCategoryResourceInfo.AIDetails.HostResourceType`, o `ResourceInfo.AIDetails.CanonicalId` en`GetResourcesStatisticsV2`. De lo contrario, la operación devuelve un`ValidationException`.
> El siguiente ejemplo muestra una combinación de filtros válida:
>
> ```
> {
> ```

```
    "Filters": {
        "CompositeFilters": [
            {
                "Operator": "AND",
                "StringFilters": [
                    {
                        "FieldName": "ResourceCategory",
                        "Filter": {
                            "Comparison": "EQUALS",
                            "Value": "AI/ML"
                        }
                    },
                    {
                        "FieldName": "ResourceSubCategory",
                        "Filter": {
                            "Comparison": "EQUALS",
                            "Value": "Model"
                        }
                    }
                ]
            }
        ]
    }
}
```

Resultados de exposición en Security Hub

Un resultado de exposición en Security Hub representa la correlación de varias señales de seguridad que identifican los posibles riesgos de seguridad en su AWS entorno. Los resultados de la exposición le ayudan a comprender y priorizar los riesgos de seguridad. Analizan automáticamente las combinaciones de vulnerabilidades, configuraciones, amenazas y relaciones de recursos. Un resultado de exposición incluye condiciones y señales. Una señal puede incluir uno o varios tipos de condiciones de exposición. Security Hub genera una detección de exposición cuando las señales de Security Hub CSPM, Amazon Inspector GuardDuty, Macie u otros AWS servicios indican la presencia de una exposición. Un recurso puede ser el recurso principal en, como máximo, un hallazgo de exposición. Si un recurso no tiene ningún rasgo de exposición o tiene rasgos insuficientes, Security Hub no genera un hallazgo de exposición para ese recurso.

Cómo funcionan los resultados de exposición

Security Hub genera los hallazgos de exposición de la siguiente manera:

Analizar las señales de varios servicios AWS de seguridad

Security Hub recopila y analiza de forma continua las señales de seguridad de varios servicios AWS de seguridad. Incluye las conclusiones de Amazon Inspector GuardDuty para la detección de amenazas, para la evaluación de vulnerabilidades, Security Hub CSPM para las comprobaciones de configuración y Macie para la exposición de datos confidenciales. Estas señales se procesan mediante motores de correlación avanzados para identificar los posibles riesgos de seguridad.

Evaluación de las configuraciones y relaciones de los recursos

El sistema realiza una evaluación detallada de las configuraciones de los recursos comparándolas con las mejores prácticas de seguridad. Examina la configuración específica del servicio, los requisitos de cumplimiento y los controles de seguridad. Este análisis ayuda a identificar errores de configuración que podrían provocar vulnerabilidades de seguridad si se combinan con otros factores.

Evaluar la accesibilidad de la red

Un componente crucial de los resultados de la exposición es la evaluación de la accesibilidad de la red. El sistema evalúa tanto la exposición a Internet como las rutas de acceso a la red interna. Analiza las configuraciones de los grupos de seguridad y la configuración de las ACL de red para determinar los posibles vectores de ataque. Este análisis ayuda a identificar los recursos que podrían estar expuestos inadvertidamente a un acceso no autorizado.

Correlacionar los problemas de seguridad relacionados

El motor de correlación mapea las relaciones entre AWS los recursos, analiza cómo interactúan e identifica las posibles implicaciones de seguridad. Examina los permisos, las funciones y los patrones de acceso a los recursos de IAM para comprender el contexto de seguridad más amplio. Este proceso ayuda a identificar los riesgos de seguridad que pueden existir debido a la combinación de configuraciones individuales aparentemente inocentes.

Componentes de un hallazgo de exposición

Cada resultado de exposición incluye:

Título y descripción del posible riesgo de seguridad

Cada resultado de exposición incluye un título claro y descriptivo que refleja de forma inmediata la naturaleza del riesgo de seguridad. La descripción proporciona información detallada sobre el posible impacto en la seguridad, los recursos afectados y el contexto más amplio de la exposición. Esta información ayuda a los equipos de seguridad a comprender y evaluar rápidamente el riesgo.

Clasificación de gravedad (crítica, alta, media, baja)

- La gravedad crítica indica que se requiere atención inmediata debido a la alta probabilidad de explotación y al importante impacto potencial. Estos hallazgos suelen representar vulnerabilidades que se pueden descubrir y explotar fácilmente.
- La alta gravedad sugiere que se necesita una atención prioritaria, con una probabilidad de explotación de moderada a alta y un impacto potencial sustancial. Estos hallazgos pueden ser relativamente fáciles de explotar, pero pueden requerir condiciones específicas.
- La gravedad media indica que se requiere una atención programada, con una menor probabilidad de explotación y un impacto potencial moderado. Estos hallazgos suelen requerir métodos de explotación más complejos.
- La baja gravedad sugiere que se necesita una atención rutinaria, con un potencial de explotación limitado y un impacto menor. Estos hallazgos suelen ser difíciles de explotar y presentan un riesgo mínimo.

Rasgos que contribuyeron a la exposición

Los rasgos que contribuyen a la exposición representan los factores principales que condujeron al hallazgo de la exposición. Estos incluyen las vulnerabilidades de seguridad directas, los problemas de configuración, las condiciones de exposición de la red y la configuración de los permisos de los recursos. Cada característica proporciona detalles específicos sobre cómo contribuye al riesgo de seguridad general.

Visualización de la posible ruta de ataque y el radio de la explosión

La visualización de la ruta potencial del ataque y el radio de la explosión proporciona un diagrama interactivo que muestra cómo los posibles atacantes podrían aprovechar la exposición identificada. Mapea las relaciones entre los recursos, las rutas de red y las rutas de escalamiento de privilegios con los recursos posteriores a los que un atacante podría acceder si se aprovecha la exposición.

Guía de remediación detallada

Cada resultado de exposición incluye una guía de remediación detallada con medidas específicas y viables para abordar los riesgos identificados. Esta guía incluye recomendaciones de mejores prácticas, pasos para corregir la configuración y elementos de acción priorizados. La guía se adapta al escenario de exposición específico y tiene en cuenta los AWS servicios involucrados.

Detalles de configuración de los recursos

La configuración del recurso en el momento en que se creó la búsqueda, así como la configuración actual del recurso en el panel de inventario de recursos de Security Hub.

Características contextuales que proporcionan un contexto de seguridad adicional

Los rasgos contextuales son marcadores de seguridad adicionales que Security Hub identificó pero que no se utilizaron para determinar la exposición.

La información de acceso no utilizada de IAM Access Analyzer puede aparecer como rasgos contextuales en los hallazgos de exposición. Cuando una función de IAM asociada a un recurso tiene permisos no utilizados, Security Hub incluye esta información como un rasgo contextual en la vista detallada de la exposición. Por ejemplo, si una instancia de Amazon EC2 tiene una vulnerabilidad de software y su rol de IAM adjunto tiene 47 permisos no utilizados en 5 servicios, el resultado de la exposición muestra los permisos no utilizados como contexto adicional. Esto le ayuda a comprender el posible radio de explosión: un recurso vulnerable con una función de IAM con privilegios excesivos presenta un riesgo mayor que uno con permisos con privilegios mínimos, ya que un recurso comprometido podría utilizar esos permisos no utilizados para aumentar el acceso.

Los siguientes tipos de recursos pueden mostrar características contextuales del acceso no utilizado en sus resultados de exposición:

- Instancias de Amazon Elastic Compute Cloud
- AWS Lambda funciones
- Servicios de Amazon Elastic Container Service
- Clústeres de Amazon Elastic Kubernetes Service
- Usuarios de IAM (directamente)

Clasificación de gravedad

Los hallazgos de exposición se clasifican en función de:

- Facilidad de descubrimiento
- Facilidad de explotación
- Probabilidad de explotación
- Sensibilización pública
- Impacto potencial

Para obtener más información, consulte la clasificación de gravedad de los hallazgos de exposición.

Beneficios de los hallazgos relacionados con la exposición

- Reducción del análisis manual mediante la correlación automatizada: los resultados de la exposición reducen significativamente el tiempo y el esfuerzo necesarios para analizar la seguridad mediante la correlación automatizada y la priorización inteligente de los riesgos. Security Hub monitorea su AWS entorno de forma continua, identificando y correlacionando automáticamente los riesgos de seguridad que podrían pasarse por alto mediante una revisión manual.
- Visión priorizada de los riesgos de seguridad: Security Hub emplea sofisticados algoritmos de evaluación de riesgos para priorizar las exposiciones en función de la gravedad, el impacto, la importancia de los recursos y la probabilidad de explotación. Esto ayuda a los equipos de seguridad a centrar sus esfuerzos primero en los riesgos más importantes, lo que mejora la eficiencia de las operaciones de seguridad.

Fuentes de exposición: hallazgos

Los hallazgos sobre la exposición incorporan datos de:

- GuardDuty La integración con Amazon proporciona capacidades de detección continua de amenazas dentro de los hallazgos de exposición. Supervisa las actividades maliciosas, las posibles amenazas a las cuentas y las anomalías de comportamiento. El sistema incorpora estos hallazgos de amenazas en un análisis de exposición más amplio, lo que ayuda a identificar cuándo las amenazas se combinan con otros problemas de seguridad para crear riesgos importantes.
- Amazon Inspector aporta datos cruciales de evaluación de vulnerabilidades a los resultados de la exposición. Proporciona información detallada sobre la accesibilidad de la red, las vulnerabilidades del software y las infracciones de las mejores prácticas de seguridad. Esta integración ayuda a comprender cómo se pueden aprovechar las vulnerabilidades a través de las rutas de ataque identificadas.

- AWS Security Hub CSPM garantiza que el cumplimiento de la configuración y los estándares de seguridad se tengan en cuenta al analizar la exposición. Evalúa los recursos comparándolos con los controles de seguridad establecidos y las mejores prácticas, y proporciona una base para comprender los riesgos basados en la configuración.
- Amazon Macie mejora los resultados de exposición con funciones de detección y clasificación de datos confidenciales. Identifica dónde existen datos confidenciales en su AWS entorno y evalúa los posibles riesgos de privacidad, lo que ayuda a comprender el posible impacto de las exposiciones identificadas.

Prácticas recomendadas

- Revise periódicamente los resultados de la exposición: la gestión eficaz de la exposición requiere procesos de revisión estructurados. Las organizaciones deben realizar revisiones diarias de las exposiciones críticas, evaluaciones semanales del estado general de exposición, análisis mensuales de las tendencias y evaluaciones trimestrales de la postura de seguridad. Este enfoque escalonado garantiza una atención adecuada tanto a los riesgos inmediatos como a las tendencias de seguridad a largo plazo.
- Priorice las exposiciones críticas y de alta gravedad: la gestión exitosa de la exposición depende de una priorización eficaz de los riesgos. Las organizaciones deben centrarse primero en las exposiciones críticas y, al mismo tiempo, tener en cuenta la importancia de los recursos y el impacto empresarial. Este enfoque basado en el riesgo ayuda a garantizar que los esfuerzos de seguridad se alineen con las prioridades empresariales y a maximizar la reducción de riesgos.
- Implemente los pasos de remediación recomendados: la remediación de la exposición debe seguir un enfoque sistemático. Las organizaciones deben implementar cuidadosamente las medidas correctivas recomendadas, mantener una documentación detallada de los cambios, realizar pruebas exhaustivas de las modificaciones y validar la eficacia de las correcciones implementadas. Este enfoque metódico ayuda a garantizar una mitigación exitosa de los riesgos y, al mismo tiempo, evita las consecuencias imprevistas.
- Configure reglas de respuesta automatizadas: maximizar el valor de los hallazgos de exposición requiere una automatización eficaz. Las organizaciones deben implementar reglas de respuesta automatizada, configurar las notificaciones adecuadas, establecer flujos de trabajo eficientes y mantener registros de auditoría exhaustivos. Esta automatización ayuda a garantizar una respuesta coherente y oportuna a las exposiciones identificadas, al tiempo que reduce el esfuerzo manual.

Tipos de recursos compatibles con los resultados de exposición en Security Hub

AWS Security Hub genera los resultados de exposición para los siguientes tipos de AWS recursos:

- `AWS::DynamoDB::Table`
- `AWS::EC2::Instance`
- `AWS::ECS::Service`
- `AWS::EKS::Cluster`
- `AWS::IAM::User`
- `AWS::Lambda::Function`
- `AWS::RDS::DBInstance`
- `AWS::S3::Bucket`
- `AWS::SageMaker::NotebookInstance`

Si tiene un conector de Azure, Security Hub también genera datos de exposición para los siguientes tipos de recursos de Azure:

- `microsoft.app/containerapps`
- `microsoft.compute/virtualmachines`
- `microsoft.containerservice/managedclusters`
- `microsoft.documentdb/databaseaccounts`
- `microsoft.graph/user`
- `microsoft.sql/servers/databases`
- `microsoft.storage/storageaccounts/blobservices/containers`
- `microsoft.web/sites`

Security Hub genera una búsqueda de exposición por recurso principal. Si un recurso no tiene ningún rasgo de exposición o tiene rasgos insuficientes, Security Hub no genera un hallazgo de exposición para ese recurso.

Tipos de condiciones admitidas en Security Hub

AWS Security Hub genera un resultado de exposición cuando los hallazgos del control de CSPM de AWS Security Hub y los hallazgos generados por otros proveedores compatibles Servicios de AWS, como Amazon Inspector, contienen características de exposición para un recurso. La siguiente tabla proporciona información sobre los tipos de condiciones compatibles.

Tipo de condición	Description (Descripción)	origen	Recursos afectados
Asumibilidad	Indica un recurso con permisos concedidos AWS Identity and Access Management	Configuración de recursos desde AWS Config	AWS recursos con AWS Identity and Access Management roles asociados
Impact	Indica el radio potencial de explosión si el recurso se ve compromet ido, en función de los permisos efectivos de AWS Identity and Access Management los responsab les asociados, incluida la capacidad de crear y modificar recursos	Análisis de los permisos efectivos de los principal es asociados AWS Identity and Access Management	AWS recursos con identidad es asociadas AWS Identity and Access Management
Configuración incorrecta	Indica un recurso mal configurado	AWS Los resultados del control de CSPM de Security Hub, los hallazgos de GuardDuty amenazas en Amazon y la informaci ón sobre la confirmación de	Todos los tipos de recursos

Tipo de condición	Description (Descripción)	origen	Recursos afectados
		los recursos en. AWS Config	
Alcance	Indica las rutas de red abiertas a un recurso	AWS Hallazgos sobre el control de CSPM de Security Hub, sobre GuardDuty amenazas en Amazon y sobre la accesibil idad de la red de Amazon Inspector.	Instancias de Amazon EC2, clústeres de Amazon EKS, funciones de Lambda y cubos de Amazon S3
Información confidencial	Indica que un recurso contiene datos confidenciales	Hallazgos de datos confidenc iales de Macie	Buckets de Amazon S3
Vularidad	Indica que un recurso tiene una debilidad que podría ser explotada por una fuente de amenazas.	Hallazgos de vulnerabilidad de paquetes de Amazon Inspector y hallazgos de malware de GuardDuty Amazon EC2.	Instancias de Amazon EC2, servicios de Amazon ECS, clústeres de Amazon EKS y funciones de Lambda.

Cada condición se puede asociar con varios títulos que proporcionan detalles sobre la exposición que afecta al recurso. Por ejemplo, podría ver un título Explotación disponible para la condición Vulnerabilidad en los detalles de un resultado de exposición de EC2.

Impacto y permisos efectivos

El rasgo de impacto describe el radio de explosión potencial de una exposición, es decir, los recursos intermedios que un atacante podría alcanzar y comprometer si el recurso principal detectado por la exposición se ve comprometido. Para determinar el impacto, Security Hub analiza los permisos efectivos de las personas principales AWS Identity and Access Management (IAM) asociadas al recurso.

Los permisos efectivos son los permisos que realmente tiene un principal después de que Security Hub evalúe sus políticas basadas en la identidad junto con las políticas basadas en los recursos de los recursos a los que puede acceder. Como los permisos efectivos tienen en cuenta tanto lo que se concede a un principal como lo que permiten los recursos de destino, reflejan con mayor precisión las acciones que puede realizar un principal que las políticas basadas en la identidad por sí solas.

Con permisos efectivos, Security Hub rastrea las rutas de escalamiento de privilegios desde el recurso principal a otros recursos de su entorno. Cada ruta es una cadena de recursos conectados por los permisos que permiten a un atacante pasar de un recurso a otro. Cuando Security Hub identifica una ruta concreta hacia un recurso existente, muestra esa ruta como parte de la característica Impact. Impact también tiene en cuenta los permisos Servicios de AWS que van más allá de estas rutas, como la capacidad de invocar para crear o modificar otros recursos. Puedes revisar estas rutas en el gráfico de posibles rutas de ataque y reducir el radio de la explosión eliminando los permisos innecesarios. Para obtener más información, consulte Visualización de exposiciones en Security Hub mediante el gráfico de ruta potencial de ataque.

Generación de resultados de exposición

Security Hub genera los hallazgos de exposición casi en tiempo real. A medida que se recopilan nuevos hallazgos de seguridad y se actualizan los existentes, Security Hub genera o actualiza los hallazgos de exposición casi en tiempo real. Security Hub genera una búsqueda de exposición por cada ID de recurso.

Security Hub no publica los resultados de exposición de los tipos de recursos que no estén respaldados por los hallazgos de exposición. Cuando un recurso presenta una cantidad y combinación significativas de condiciones, Security Hub genera un resultado de exposición. La cantidad y combinación de condiciones también determinan el nivel de gravedad del resultado de exposición.

Ejemplo de resultado de exposición

AWS Security Hub normaliza los resultados de exposición en el marco del esquema abierto de ciberseguridad (OCSF).

Ejemplo de resultado de exposición

En el siguiente ejemplo de resultado de exposición, el parámetro `related_events` contiene información exclusiva de ese resultado de exposición, como los resultados contribuyentes. Los resultados contribuyentes son las condiciones y señales asociadas con un resultado de exposición. Un único resultado contribuyente puede incluir una o varias condiciones. El parámetro `observables` identifica el recurso asociado con el resultado contribuyente. Este puede ser distinto del parámetro `resources`, que identifica el recurso asociado con el resultado de exposición.

```
{
    "activity_id": 1,
    "activity_name": "Create",
    "category_name": "Findings",
    "category_uid": 2,
    "class_name": "Detection Finding",
    "class_uid": 2004,
    "cloud": {
        "account": {
            "uid": "123456789012",
            "name": "production-application"
        },
        "cloud_partition": "aws",
        "provider": "AWS",
        "region": "us-east-1"
    },
    "finding_info": {
        "analytic": {
            "name": "Exposure",
            "type": "Rule",
            "type_id": 1,
            "uid": "0.0.1"
        },
        "created_time_dt": "2024-11-15T21:39:26.337224100Z",
        "desc": "Publicly invocable Lambda function executed outside of VPC has
 vulnerability with known exploit that can be exploited from remote network",
        "finding.info.modified_time_dt": "2024-11-15T21:39:26.337224100Z",
        "related_events_count": 3,
        "related_events": [
```

```
            {
                "tags": [
                    {
                        "name": "Vulnerability",
                        "values": [
                            "Attack Vector Network",
                            "EPSS Level >= High",
                            "EPSS Level >= Medium",
                            "Exploit Available",
                            "No Privileges Required",
                            "No User Interaction Required",
                            "Vulnerable"
                        ]
                    }
                ],
                "product": {
                    "uid": "arn:aws:securityhub:us-east-1::productv2/aws/inspector"
                },
                "observables": [
                    {
                        "type": "Resource UID",
                        "type_id": 10,
                        "value": "arn:aws:lambda:us-east-1:123456789012:application-
function"
                    }
                ],
                "type": "Finding",
                "title": "CVE-2023-33246 - org.apache.rocketmq:rocketmq-controller",
                "uid": "arn:aws:inspector2:us-
east-1:123456789012:finding/1234567890abcdef0"
            },
            {
                "tags": [
                    {
                        "name": "Reachability",
                        "values": [
                            "Publicly Invocable"
                        ]
                    }
                ],
                "product": {
                    "uid": "arn:aws:securityhub:us-east-1::productv2/aws/securityhub"
                },
                "observables": [
```

```
                    {
                        "type": "Resource UID",
                        "type_id": 10,
                        "value": "arn:aws:lambda:us-east-1:123456789012:application-
function"
                    }
                ],
                "type": "Finding",
                "title":  "Lambda function policies should prohibit public access",
                "uid": "arn:aws:securityhub:us-east-1:123456789012:security-control/
Lambda.1/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa"
            },
            {
                "tags": [
                    {
                        "name": "Misconfiguration",
                        "values": [
                            "Deployed outside VPC"
                        ]
                    }
                ],
                "product": {
                    "uid": "arn:aws:securityhub:us-east-1::productv2/aws/securityhub"
                },
                "observables": [
                    {
                        "type": "Resource UID",
                        "type_id": 10,
                        "value": "arn:aws:lambda:us-east-1:123456789012:application-
function"
                    }
                ],
                "type": "Finding",
                "title": "Lambda functions should be in a VPC",
                "uid": "arn:aws:securityhub:us-east-1:123456789012:security-control/
Lambda.3/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
            }
        ],
        "title": "Publicly invocable Lambda function executed outside of VPC has
 vulnerability with known exploit that can be exploited from remote network",
        "types": [
            "Exposure/Potential Impact/Resource Hijacking"
        ],
```

```
        "uid": "arn:aws:securityhub:us-
east-1:123456789012:risk:1234f781c7ae7507f01e2fb460f15ca8fe7f9c95e257698a092cb74a4ea84a42"
    },
    "metadata": {
        "product": {
            "name": "Security Hub Exposure Analysis",
            "uid": "arn:aws:securityhub:us-east-1::productv2/aws/securityhub-risk",
            "vendor_name": "Amazon"
        },
        "processed_time_dt": "2024-11-15T21:39:58.819Z",
        "profiles": [
            "cloud",
            "datetime"
        ],
        "version": "1.4.0-dev"
    },
    "resources": [
        {
            "cloud_partition": "aws",
            "region": "us-east-1",
            "tags": [
                {
                    "name": "aws:cloudformation:stack-name",
                    "value": "LambdaProdStack"
                },
                {
                    "name": "aws:cloudformation:stack-id",
                    "value": "arn:aws:cloudformation:us-east-1:123456789012:stack/
LambdaProdStack/a1b2c3d4-5678-90ab-cdef-EXAMPLE22222"
                },
                {
                    "name": "aws:cloudformation:logical-id",
                    "value": "lambdar3function94D10D40"
                }
            ],
            "type": "AwsLambdaFunction",
            "uid": "arn:aws:lambda:us-east-1:123456789012:application-function"
        }
    ],
    "severity": "Critical",
    "severity_id": 5,
    "impact": "High",
    "impact_id": 3,
    "likelihood": "Very High",
```

```
    "likelihood_id": 5,
    "status": "New",
    "status_id": 1,
    "time": 1731706766337,
    "time_dt": "2024-11-15T21:39:26.337224100Z",
    "type_name": "Detection Finding: Create",
    "type_uid": 200401,
    "vendor_attributes": {
        "severity_id": 5,
        "severity": "Critical"
    }
}
```

Cómo determinar el nivel de gravedad de un resultado de exposición

AWS Security Hub asigna a cada exposición una gravedad predeterminada de`CRITICAL`,, `HIGHMEDIUM`, o`LOW`. Los hallazgos de exposición con una gravedad de no `INFORMATIONAL` se publican. Security Hub determina la gravedad de una exposición al combinar dos dimensiones, la probabilidad y el impacto, en una matriz de riesgos. La probabilidad refleja la facilidad con la que se puede aprovechar la exposición, y el impacto refleja la magnitud del daño si se explota.

En los casos en que no se puede determinar el impacto de un recurso, la gravedad se basa únicamente en la probabilidad.

Matriz de riesgos

La siguiente tabla muestra cómo la probabilidad y el impacto se combinan para determinar la gravedad final de una declaración de exposición. La probabilidad establece una gravedad de referencia y el impacto la ajusta: un impacto alto aumenta la gravedad en un nivel (con un límite máximo`CRITICAL`), un impacto medio no cambia la gravedad y un impacto bajo la reduce en `INFORMATIONAL` un nivel (con un límite mínimo). El impacto solo ajusta la gravedad que establece la probabilidad. El impacto por sí solo no genera un hallazgo de exposición.

Matriz de riesgos de gravedad

Probabilidad ↓ /Impacto →	Bajo	Medio	Alto
Muy alta	ALTO	CRÍTICO	CRÍTICO
Alta	MEDIO	ALTO	CRÍTICO

Probabilidad ↓ /Impacto →	Bajo	Medio	Alto
Moderado	BAJA	MEDIO	ALTO
Baja	INFORMATIVO	BAJA	MEDIO

> **Note**
>
> La baja probabilidad combinada con un bajo impacto da como resultado una gravedad de`INFORMATIONAL`. Security Hub no publica los resultados de exposición con esta gravedad, por lo que no aparecen en la página de exposiciones ni en GetFindingsV2 los resultados.

Probabilidad

La probabilidad mide la facilidad con la que se puede aprovechar una exposición, en función de las características que contribuyen a ello y que están presentes en el recurso, como la suposición, la mala configuración, la accesibilidad, los datos confidenciales y la vulnerabilidad. Security Hub utiliza varias características para evaluar la probabilidad, entre las que se incluyen las siguientes:

- Conocimiento público: grado en que la exposición deja de ser teórica y cuenta con métodos de explotación públicos o automatizados.
- Facilidad de detección: indica si existen herramientas automatizadas, como un análisis de puertos o una búsqueda en Internet, que permiten detectar el recurso en riesgo.
- Facilidad de explotación: mide qué tan fácilmente un actor malicioso puede explotar la exposición. Por ejemplo, si existen rutas de red abiertas o metadatos mal configurados, un actor malicioso puede explotar la exposición con mayor facilidad.
- Probabilidad de explotación: mide la probabilidad de que la exposición sea explotada en los próximos 30 días. Este factor corresponde al sistema de puntuación de predicción de exploits (EPSS).

Impact

El impacto mide la magnitud del daño causado al medio ambiente si se aprovecha la exposición. Por ejemplo, una exposición puede generar pérdida de trazabilidad, pérdida de disponibilidad, pérdida de confidencialidad por exposición de datos o pérdida de integridad por corrupción de datos.

Para evaluar el impacto, Security Hub analiza los permisos efectivos de las AWS Identity and Access Management personas principales asociadas al recurso para determinar las acciones que Servicios de AWS un atacante podría invocar. También identifica los recursos existentes que un atacante podría alcanzar y comprometer mediante la escalada de privilegios. Para obtener más información, consulte Impacto y permisos efectivos.

Cómo revisar los resultados de exposición

Puede revisar todos los resultados de exposición en la consola de Security Hub y mediante la API GetFindingsV2. La página Exposiciones en la consola de Security Hub muestra todos los resultados de exposición activos. Los resultados de exposición aparecen en orden descendente según la gravedad. Puede filtrar los resultados de exposición. Para ello, agregue y quite filtros con la barra de búsqueda Agregar filtro. Puede agrupar los resultados de exposición con el menú desplegable Agrupar por. También puede filtrar los resultados de exposición con el menú Filtros rápidos.

Detalles de los resultados de exposición

Puede consultar numerosos detalles sobre un resultado de exposición. Estos detalles se organizan en pestañas dentro de la consola de Security Hub. La pestaña Descripción general presenta los detalles clave del resultado de exposición. La pestaña Condiciones enumera las condiciones y señales asociadas con un resultado de exposición. La pestaña Recursos presenta detalles sobre el recurso y las etiquetas del recurso asociadas con un resultado de exposición. A continuación, se presentan las descripciones de los elementos incluidos dentro de los detalles de los resultados de exposición:

- Título del resultado: el título del resultado de exposición.
- Nivel de gravedad: el nivel de gravedad del resultado de exposición. Security Hub usa la cantidad y la combinación de condiciones de un recurso para determinar el nivel de gravedad de un resultado de exposición. El nivel de gravedad puede ser `CRITICAL`, `HIGH`, `MEDIUM` o `LOW`. Security Hub no publica los resultados de exposición con una gravedad de`INFORMATIONAL`. Es posible actualizar la `Severity` desde la consola de Security Hub o mediante la operación de la API BatchUpdateFindingsV2.
- Descripción: la descripción del resultado de exposición.

- Tipo: el nombre del tipo de resultado de exposición. Por ejemplo, el nombre puede presentarse como `Exposure/Potential Impact/Resource Hijacking`.
- Cuenta: el identificador de la Cuenta de AWS donde se generó el resultado de exposición.
- Antigüedad: indica el tiempo que el resultado de exposición ha permanecido activo.
- Hora de creación: la marca de tiempo que indica el momento en que se creó el resultado de exposición.
- Hora de modificación: la marca de tiempo que indica el momento en que se actualizó por última vez el resultado de exposición.
- Región: el Región de AWS lugar donde se generó el hallazgo de exposición.
- Nombre del producto: el nombre del producto que generó el resultado de exposición. Esto siempre corresponde a Detección de exposición de Security Hub.
- Nombre de la empresa: el nombre de la empresa que generó el resultado de exposición. Siempre se tratará de AWS.
- Nombre de la actividad: el nombre de la actividad realizada más recientemente sobre el resultado de exposición.
- Estado: el estado del resultado de exposición.
- Identificador del resultado: un identificador único asociado con el resultado de exposición.
- Ruta potencial de ataque (solo en consola): una visualización interactiva que muestra cómo posibles atacantes pueden obtener acceso y control sobre recursos asociados con un resultado de exposición. Para obtener más información, consulte Visualización de exposiciones en Security Hub mediante el gráfico de ruta potencial de ataque.
- Condiciones: identifica los tipos de condiciones y los títulos de condiciones asociados con el resultado de exposición. En la consola de Security Hub, es posible revisar condiciones por tipo de condición o por señal. Esto permite analizar los resultados contribuyentes dentro del contexto de la exposición relacionada.
- Corrección: enlaces a la documentación de corrección específica para las condiciones identificadas en la exposición.
- Recursos: identifica el recurso asociado con el resultado de exposición.

Cómo revisar los detalles de los resultados de exposición

Este tema describe la manera de revisar los detalles de los resultados de exposición en la consola de AWS Security Hub y mediante la API.

Revisión de detalles de un resultado de exposición en la consola de Security Hub.

Para consultar los detalles de un resultado de exposición en la consola de Security Hub

1. Inicie sesión con sus credenciales y abra la consola de Security Hub en https://console.aws.amazon.com/securityhub/v2/home.
2. En el panel de navegación, elija Exposiciones.
3. Elija el resultado de exposición cuyo detalle desea consultar.

Revisión de detalles de un resultado de exposición con la API

Es posible revisar los resultados de exposición mediante la API GetFindingsV2 o a través de la AWS CLI. Es posible filtrar todos los resultados de exposición con el campo `metadata.product.feature.uid` con el valor `security-hub/Exposure`. Para obtener más información, consulte GetFindingsV2.

Comando de ejemplo:

A continuación, se AWS CLI muestra un ejemplo en el que se recuperan los 10 datos de exposición generados más recientemente en su cuenta. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
aws securityhub get-findings-v2 \
--max-results '10' \
--filter '{"CompositeFilters": [{"StringFilters":
 [{"FieldName":"metadata.product.feature.uid","Filter": {"Value":"security-hub/
Exposure","Comparison":"EQUALS"}} ]}]}'
```

Visualización de exposiciones en Security Hub mediante el gráfico de ruta potencial de ataque

El gráfico de ruta potencial de ataque es una visualización interactiva que muestra cómo posibles atacantes pueden obtener acceso y control sobre los recursos asociados con un resultado de exposición. Solo puede acceder a este gráfico en la consola de Security Hub desde la página de exposiciones. Al consultar los detalles de la detección de una exposición, la pestaña Descripción general incluye una sección denominada Ruta potencial de ataque y radio de explosión.

El gráfico de la ruta de ataque muestra el recurso principal en el que se generó la exposición, la ruta de la red (si corresponde) y los recursos posteriores a los que podría acceder un atacante

si aumentara los permisos. Cuando Security Hub identifica rutas concretas de escalamiento de privilegios desde el recurso principal a otros recursos de su entorno, las muestra en el gráfico como la parte del radio de explosión. Cada nodo representa un recurso y las conexiones entre los nodos muestran los permisos que permiten a un atacante pasar de un recurso a otro.

En esta sección de la pestaña Descripción general, seleccione y arrastre los recursos de AWS dentro del gráfico de ruta potencial de ataque. Concéntrese en áreas específicas del gráfico mediante los íconos de acercar y alejar. Amplíe el gráfico de ruta potencial de ataque dentro y fuera del modo de pantalla completa mediante el ícono de pantalla completa. La leyenda codifica el recurso principal, el recurso involucrado, los recursos del radio de explosión y el recuento de rasgos contribuyentes por color, y muestra las categorías de rasgos y el número de rasgos en el gráfico de rutas de ataque. Para ver los detalles de un recurso, seleccione un recurso y elija Ver detalles del recurso. También es posible copiar el identificador y el número de Cuenta de AWS asociados con un recurso. Los resultados de exposición con una condición de alcance muestran la ruta de red pública y la ruta de red colapsada en el gráfico de ruta de ataque. Es posible consultar este detalle. Para ello, seleccione el nodo de ruta de red colapsada.

Para ver los recursos posteriores y las rutas de escalamiento de privilegios que los conectan, selecciona la pestaña Evaluación de impacto. Cada ruta muestra la cadena de recursos que un atacante podría atravesar y los permisos específicos de cada paso. Para obtener más información sobre las características de impacto y los permisos efectivos, consulteImpacto y permisos efectivos.

Corrección de resultados de exposición

En los temas de esta sección se describen los pasos para corregir los hallazgos de exposición en diferentes Servicios de AWS regiones.

El campo `Remediation` del formato OCSF contiene dos campos: `remediation` y `references`.

```
"Remediation": {
    "Recommendation": {
        "remediation":{"desc":"String",
        "references":["string array"]}
    }
},
```

> **Note**
>
> La guía de remediación que se proporciona en las siguientes secciones puede requerir consultas adicionales en otros AWS recursos.

Remediación de exposiciones en tablas de DynamoDB

AWS Security Hub puede generar resultados de exposición para las tablas de DynamoDB.

En la consola de Security Hub, la tabla de DynamoDB involucrada en un resultado de exposición y su información de identificación aparecen en la sección Recursos de los detalles del resultado. Mediante programación, puede recuperar los detalles de los recursos con el GetFindingsV2 funcionamiento de la API CSPM de Security Hub.

Después de identificar el recurso involucrado en un resultado de exposición, puede eliminar el recurso si no lo necesita. Eliminar un recurso no esencial puede reducir su perfil de exposición y sus costos. AWS Si el recurso es esencial, siga estos pasos de remediación recomendados para ayudar a mitigar el riesgo. Los temas de remediación se dividen según el tipo de condición.

Un único resultado de exposición puede incluir problemas identificados en varios temas de remediación. También es posible abordar un resultado de exposición y disminuir su nivel de gravedad con solo tratar uno de los temas de remediación. El enfoque de remediación adecuado depende de los requisitos y cargas de trabajo de la organización.

> **Note**
>
> La guía de remediación que se proporciona en este tema puede requerir consultas adicionales en otros AWS recursos.

Contenido

- Condiciones de configuración incorrecta en DynamoDB
  - La tabla de DynamoDB tiene la función de recuperación a un punto en el tiempo desactivada
  - La tabla de DynamoDB no está cubierta por un plan de copias de seguridad
  - La tabla de DynamoDB tiene la protección contra eliminación desactivada

Condiciones de configuración incorrecta en DynamoDB

La siguiente información describe las condiciones de configuración incorrecta y los pasos de remediación para tablas de DynamoDB.

La tabla de DynamoDB tiene la función de recuperación a un punto en el tiempo desactivada

Solución: habilite la recuperación puntual de DynamoDB

La recuperación a un punto en el tiempo de DynamoDB proporciona copias de seguridad automáticas y continuas de los datos de la tabla de DynamoDB. Para obtener información sobre cómo restaurar una tabla de DynamoDB a un punto en el tiempo, consulte Restaurar una tabla de DynamoDB a un punto en el tiempo en la guía para desarrolladores de Amazon DynamoDB.

La tabla de DynamoDB no está cubierta por un plan de copias de seguridad

AWS La copia de seguridad proporciona un servicio centralizado para configurar, gestionar y automatizar las copias de seguridad en todos los servicios, incluido DynamoDB. AWS Sin un plan de copias de seguridad, la tabla carece de copias de seguridad programadas y automatizadas con periodos de retención personalizables, lo que genera riesgos de seguridad significativos. Un atacante podría corromper o eliminar maliciosamente los datos de la tabla. Sin las copias de seguridad adecuadas, es posible que no tenga ninguna opción de recuperación más allá de la ventana de Point-in-Time recuperación (si está habilitada), lo que podría provocar una pérdida permanente de datos. Siguiendo las prácticas recomendadas de protección de datos, cubra sus tablas de DynamoDB con un plan de respaldo.

Solución: cree un plan de respaldo

Antes de crear un plan de copias de seguridad, determine una frecuencia de copia de seguridad adecuada y los periodos de retención de los datos. Para obtener información sobre cómo crear un plan de respaldo, consulte Asignar recursos a un plan de respaldo en la Guía para desarrolladores de AWS copias de seguridad.

La tabla de DynamoDB tiene la protección contra eliminación desactivada

La protección contra eliminación evita el borrado accidental de tablas de DynamoDB. Cuando la protección contra eliminación está desactivada, las tablas de DynamoDB son vulnerables a eliminaciones no intencionadas mediante acciones en la consola, llamadas a la API, comandos de la CLI o procesos automatizados. Esto puede exponer su AWS entorno a la pérdida de datos, ya que una entidad no autorizada con acceso a su AWS entorno podría eliminar las tablas de forma

intencionada, lo que provocaría una interrupción del servicio y una pérdida permanente de datos. Si sigue las prácticas recomendadas de protección de datos, habilite la protección de datos para las tablas de DynamoDB.

Solución: habilite la protección contra eliminaciones

Si administra varias tablas, considere la posibilidad de utilizarlas CloudFormation para actualizar las propiedades de las tablas de forma masiva. Puede modificar CloudFormation las plantillas para incluir `DeletionProtectionEnabled` propiedades y actualizar las pilas. Después de completar la remediación, verifique que la protección contra eliminación esté habilitada en el menú desplegable Información adicional en la pestaña Configuración.

Remediación de exposiciones para instancias de EC2

AWS Security Hub puede generar hallazgos de exposición para las instancias de Amazon Elastic Compute Cloud (EC2).

En la consola de Security Hub, la instancia de EC2 implicada en un resultado de exposición y su información de identificación aparecen en la sección Recursos de los detalles del resultado. Mediante programación, puede recuperar los detalles de los recursos con la GetFindingsV2 operación de la API CSPM de Security Hub.

Después de identificar el recurso involucrado en un resultado de exposición, puede eliminar el recurso si no lo necesita. Eliminar un recurso no esencial puede reducir su perfil de exposición y sus costos. AWS Si el recurso es esencial, siga estos pasos de remediación recomendados para ayudar a mitigar el riesgo. Los temas de remediación se dividen según el tipo de condición.

Un único resultado de exposición puede incluir problemas identificados en varios temas de remediación. También es posible abordar un resultado de exposición y disminuir su nivel de gravedad con solo tratar uno de los temas de remediación. El enfoque de remediación adecuado depende de los requisitos y cargas de trabajo de la organización.

> **Note**
>
> La guía de remediación que se proporciona en este tema puede requerir consultas adicionales en otros AWS recursos.

Contenido

- Condiciones de configuración incorrecta para instancias de EC2
  - La instancia de EC2 permite el acceso a IMDS mediante la versión 1.
  - La instancia de Amazon EC2 tiene un grupo de seguridad o ACL de red que permite el acceso SSH o RDP.
  - La instancia de Amazon EC2 tiene un grupo de seguridad abierto
- Condiciones de accesibilidad para instancias de EC2
  - Se puede acceder a la instancia de EC2 a través de Internet
- Condiciones de vulnerabilidad para instancias de EC2
  - La instancia de EC2 presenta vulnerabilidades de software explotables a través de la red con una probabilidad alta de explotación
  - La instancia de Amazon EC2 presenta vulnerabilidades de software.
  - La instancia EC2 tiene un sistema operativo End-Of-Life
  - La instancia EC2 contiene paquetes de software malintencionado
  - La instancia EC2 contiene archivos malintencionados
- Características de impacto de las instancias EC2
  - Tiene el control total de la ruta de ejecución privilegiada
  - Tiene una ruta directa de escalamiento de políticas
  - Tiene una ruta de secuestro de políticas de confianza
  - Tiene una ruta de ransomware de datos
  - Ha eliminado la ruta de restricción
  - Tiene el rol de pase, crea la ruta de ejecutor.
  - Tiene una ruta de ejecución existente (rol de intercambio).
  - Tiene una ruta de escalamiento de la cadena de funciones
  - Tiene una ruta de ejecución privilegiada para inyectar código
  - Ha deshabilitado la ruta del registro de auditoría
  - Tiene acceso a la ruta de ejecución existente
  - Tiene una ruta de acuñación de credenciales
  - Tiene una ruta de acceso a los datos del rol de pase
  - Ha pasado el rol, la tarea, el secuestro, la ruta
  - Tiene una ruta de acceso a los datos de un solo salto
  - Tiene una ruta de avance de la capacidad

Condiciones de configuración incorrecta para instancias de EC2

Aquí se describen las condiciones de configuración incorrecta para instancias de EC2 y los pasos de remediación sugeridos.

La instancia de EC2 permite el acceso a IMDS mediante la versión 1.

Los metadatos de instancia son datos sobre la instancia de Amazon EC2 que las aplicaciones pueden usar para configurar o administrar la instancia en ejecución. El servicio de metadatos de instancia (IMDS) es un componente de la instancia que utiliza el código de instancia para acceder de forma segura a los metadatos de la instancia. Si IMDS no está debidamente asegurado, se puede convertir en un posible vector de ataque, ya que proporciona acceso a credenciales temporales y otros datos confidenciales de configuración. IMDSv2 ofrece una protección más sólida contra la explotación mediante autenticación orientada a sesiones, que requiere un token de sesión para las solicitudes de metadatos y limita la duración de la sesión. Siguiendo los principios de seguridad estándar, configure las instancias de Amazon EC2 para que usen IMDSv2 e inhabilite IMDSv1.

Corrección

Tome una o más de las siguientes medidas para hacer frente a esta exposición:

Prueba de la compatibilidad de aplicaciones

Antes de implementar IMDSv2, pruebe la instancia para asegurarse de que sea compatible con IMDSv2. Es posible que algunas aplicaciones o scripts requieran IMDSv1 para la funcionalidad principal y requieran una configuración adicional. Para obtener más información sobre herramientas y rutas recomendadas para probar la compatibilidad de aplicaciones, consulte Transición al uso de la versión 2 del servicio de metadatos de instancias (IMDS) en la Guía del usuario de Amazon Elastic Compute Cloud.

Actualización de la instancia para usar IMDSv2

Modifique las instancias existentes para usar IMDSv2. Para obtener más información, consulte Modificación de las opciones de metadatos de instancia para instancias existentes en la Guía del usuario de Amazon Elastic Compute Cloud.

Aplicación de actualizaciones a instancias en un grupo de escalado automático

Si la instancia forma parte de un grupo de escalado automático, actualice la plantilla de lanzamiento o configuración de lanzamiento con una nueva configuración y vuelva a cargar la instancia.

La instancia de Amazon EC2 tiene un grupo de seguridad o ACL de red que permite el acceso SSH o RDP.

Los protocolos de acceso remoto como SSH y RDP permiten que los usuarios se conecten y administren instancias de Amazon EC2 desde ubicaciones externas. Cuando los grupos de seguridad permiten acceso sin restricciones a estos protocolos desde Internet, aumentan la superficie de las instancias de Amazon EC2 expuesta a ataques al permitir acceso desde Internet a la instancia. Siguiendo los principios de seguridad estándar, limite el acceso remoto a rangos o direcciones IP específicos y confiables.

Solución: modifique las reglas del grupo de seguridad

Restrinja el acceso a las instancias de Amazon EC2 únicamente a direcciones IP específicas y de confianza. Limite el acceso mediante SSH y RDP a direcciones IP específicas de confianza o utilice la notación CIDR para especificar los intervalos de IP (por ejemplo, 192.168.1). 0/24). Para modificar las reglas del grupo de seguridad, consulte Configuración de reglas de grupos de seguridad en la Guía del usuario de Amazon Elastic Compute Cloud.

La instancia de Amazon EC2 tiene un grupo de seguridad abierto

Los grupos de seguridad actúan como firewalls virtuales para controlar el tráfico entrante y saliente de las instancias de Amazon EC2. Los grupos de seguridad abiertos, que permiten acceso sin restricciones desde cualquier dirección IP, pueden exponer las instancias a accesos no autorizados. Siguiendo los principios de seguridad estándar, restrinja el acceso de los grupos de seguridad a direcciones IP y puertos específicos.

Corrección

Tome una o más de las siguientes medidas para hacer frente a esta exposición:

Revisión de las reglas del grupo de seguridad y evaluación de la configuración actual

Evalúe qué puertos están abiertos y accesibles desde rangos amplios de direcciones IP, como `(0.0.0.0/0 or ::/0)`. Para obtener instrucciones sobre cómo ver los detalles de los grupos de seguridad, consulte DescribeSecurityGroups la referencia del Asistente de portabilidad para la API de.NET.

Modificación de reglas del grupo de seguridad

Modifique las reglas del grupo de seguridad para restringir el acceso únicamente a direcciones IP o rangos específicos y de confianza. Al actualizar las reglas del grupo de seguridad, considere

separar los requisitos de acceso para distintos segmentos de red mediante la creación de reglas para cada rango de IP de origen requerido o la restricción del acceso únicamente a puertos específicos. Para modificar las reglas del grupo de seguridad, consulte Configuración de reglas de grupos de seguridad en la Guía del usuario de Amazon EC2.

Condiciones de accesibilidad para instancias de EC2

Estas son las condiciones de accesibilidad para instancias de EC2 y los pasos de remediación sugeridos.

Se puede acceder a la instancia de EC2 a través de Internet

Las instancias de Amazon EC2 con puertos a los que se puede acceder desde Internet pueden exponer su instancia. La accesibilidad puede producirse a través de una puerta de enlace de Internet (incluidas las instancias que utilizan los balanceadores de carga de aplicaciones o los balanceadores de carga clásicos), una conexión de interconexión de VPC o una puerta de enlace virtual de VPN. Siguiendo los principios de seguridad estándar, implementa controles de acceso a la red con los privilegios mínimos restringiendo el tráfico entrante solo a las fuentes y los puertos necesarios.

Corrección

Tome una o más de las siguientes medidas para abordar esta exposición:

Modificación o eliminación de reglas de grupos de seguridad

En la pestaña Recursos, abra el recurso del grupo de seguridad de Amazon EC2. Revise si la instancia requiere acceso a Internet para funcionar. Modifique o elimine reglas de grupos de seguridad entrantes que permiten acceso sin restricciones (`0.0.0.0/0` o `::/0`). Implemente reglas más restrictivas basadas en intervalos de direcciones IP específicos o en grupos de seguridad. Si se requiere un acceso público limitado, limite el acceso únicamente a los puertos y protocolos específicos necesarios para la función de la instancia. Para obtener instrucciones sobre cómo administrar las reglas de grupos de seguridad, consulte Configuración de reglas de grupos de seguridad en la Guía del usuario de Amazon EC2.

Actualización de las ACL de red

Revise y modifique las listas de control de acceso de red (ACL) asociadas a la subred de la instancia. Verifique que la configuración de la ACL esté alineada con los cambios del grupo de seguridad y no permita involuntariamente el acceso público. Para obtener instrucciones sobre cómo modificar las ACL de red, consulte Uso de las ACL de red en la Guía del usuario de Amazon VPC.

Métodos de acceso alternativos

Considere las siguientes opciones para métodos de acceso alternativos:

- Utilice la puerta de enlace NAT para la conectividad saliente a Internet: en el caso de subredes privadas que requieren acceso a Internet (por ejemplo, para descargar actualizaciones), considere la posibilidad de utilizar una puerta de enlace NAT en lugar de asignar una dirección IP pública. Una puerta de enlace de NAT permite que las instancias en subredes privadas inicien conexiones salientes a Internet y evita las conexiones entrantes desde Internet.
- Uso del Administrador de sesiones de Systems Manager Session Manager: el Administrador de sesiones proporciona acceso seguro con intérprete de comandos a las instancias de Amazon EC2 sin necesidad de habilitar puertos entrantes, administrar claves SSH o mantener hosts bastión.
- Usa WAF y Elastic Load Balancing o Application Load Balancer. Para las instancias que ejecutan aplicaciones web, considera la posibilidad de usar un LB combinado con un firewall de aplicaciones AWS web (WAF). Los equilibradores de carga se pueden configurar para permitir que las instancias se ejecuten en subredes privadas mientras el equilibrador de carga se ejecuta en una subred pública y gestiona el tráfico de Internet. Agregar un WAF al equilibrador de carga proporciona protección adicional contra atques web que aprovechan las vulnerabilidades y bots.

Condiciones de vulnerabilidad para instancias de EC2

Estas son las condiciones de vulnerabilidad para instancias de EC2 y los pasos de remediación sugeridos.

La instancia de EC2 presenta vulnerabilidades de software explotables a través de la red con una probabilidad alta de explotación

Los paquetes de software instalados en instancias de EC2 pueden estar expuestos a vulnerabilidades y exposiciones comunes (CVE). Los CVE críticos representan importantes riesgos de seguridad para su entorno. AWS Entidades principales no autorizadas pueden aprovechar estas vulnerabilidades sin parches de revisión para comprometer la confidencialidad, integridad o disponibilidad de los datos, o para acceder a otros sistemas. Las vulnerabilidades críticas con alta probabilidad de explotación representan amenazas de seguridad inmediatas, ya que el código de explotación puede estar disponible públicamente y ser utilizado activamente por atacantes o por herramientas automatizadas de detección. Corrija estas vulnerabilidades para proteger su instancia.

Solución: actualice las instancias afectadas

Consulte la sección Referencias en la pestaña Vulnerabilidad de la condición. La documentación del proveedor puede incluir instrucciones específicas de remediación. Aplique la remediación correspondiente según estas pautas generales:

Use el Administrador de parches de Systems Manager para aplicar parches tanto al sistema operativo como a las aplicaciones. El Administrador de parches ayuda a seleccionar e implementar parches de sistema operativo y de software de manera automática en grandes grupos de instancias. Si no tiene configurado el administrador de parches, actualice manualmente el sistema operativo en cada instancia afectada.

Actualice las aplicaciones afectadas a sus versiones seguras más recientes según los procedimientos recomendados por el proveedor. Para administrar las actualizaciones de aplicaciones en varias instancias, considere usar Systems Manager State Manager para mantener el software en un estado coherente. Si las actualizaciones no están disponibles, considera eliminar o deshabilitar la aplicación vulnerable hasta que se publique un parche o adoptar otras medidas paliativas, como restringir el acceso de red a la aplicación o deshabilitar las funciones vulnerables.

Siga las recomendaciones de remediación específicas incluidas en el resultado de Amazon Inspector. Esto podría implicar cambiar las reglas de grupos de seguridad, modificar las configuraciones de la instancia o ajustar la configuración de la aplicación.

Comprueba si la instancia forma parte de Auto Scaling Group. AMI-replacement Los parches se realizan en infraestructuras inmutables actualizando el ID de AMI que está configurado para implementar nuevas instancias de Amazon EC2 en un grupo de Auto Scaling. Si utiliza una custom/golden AMI, cree una instancia con la nueva AMI y, a continuación, personalice la instancia y cree una nueva AMI dorada. Para obtener más información, consulte la aplicación de parches a las actualizaciones de la AMI (uso de AMI parcheadas para los grupos de Auto Scaling).

Consideraciones futuras

Para evitar incidentes futuros, considere implementar un programa de administración de vulnerabilidades. Amazon Inspector se puede configurar para buscar de manera automática vulnerabilidades y exposiciones comunes (CVE) en las instancias. Amazon Inspector también se puede integrar con el CSPM de Security Hub para realizar remediaciones automáticas. Considere implementar un programa regular de aplicación de parches con las Ventanas de mantenimiento de Systems Manager para minimizar la interrupción en las instancias.

La instancia de Amazon EC2 presenta vulnerabilidades de software.

Los paquetes de software que se instalan en las instancias de Amazon EC2 pueden estar expuestos a vulnerabilidades y exposiciones comunes (CVE). Los CVE no críticos representan debilidades de seguridad con menor gravedad o capacidad de explotación en comparación con los CVE críticos. Aunque estas vulnerabilidades representan un riesgo menos inmediato, los atacantes aún pueden aprovechar estas vulnerabilidades sin parches para comprometer la confidencialidad, integridad o disponibilidad de los datos, o para acceder a otros sistemas. Siguiendo las prácticas recomendadas de seguridad, corrija estas vulnerabilidades para proteger su instancia de los ataques.

Solución: actualice las instancias afectadas

Utilice el administrador de parches de AWS Systems Manager para aplicar parches a los sistemas operativos. El Administrador de parches ayuda a seleccionar e implementar parches de sistema operativo y de software de manera automática en grandes grupos de instancias. Si no tiene configurado el administrador de parches, actualice manualmente el sistema operativo en cada instancia afectada.

Actualice las aplicaciones afectadas a sus versiones seguras más recientes según los procedimientos recomendados por el proveedor. Para gestionar las actualizaciones de las aplicaciones en varias instancias, considera la posibilidad de utilizar AWS Systems Manager State Manager para mantener el software en un estado uniforme. Si las actualizaciones no están disponibles, considere la posibilidad de eliminar o deshabilitar la aplicación vulnerable hasta que se publique un parche u otras medidas de mitigación, como restringir el acceso de red a la aplicación o deshabilitar las funciones vulnerables.

Siga las recomendaciones de remediación específicas incluidas en el resultado de Amazon Inspector. Esto podría implicar cambiar las reglas de grupos de seguridad, modificar las configuraciones de la instancia o ajustar la configuración de la aplicación.

Comprueba si la instancia forma parte de Auto Scaling Group. AMI-replacement Los parches se realizan en infraestructuras inmutables actualizando el ID de AMI que está configurado para implementar nuevas instancias de Amazon EC2 en un grupo de Auto Scaling. Si utiliza una custom/golden AMI, cree una instancia con la nueva AMI y, a continuación, personalice la instancia y cree una nueva AMI dorada. Para obtener más información, consulte la aplicación de parches a las actualizaciones de la AMI (uso de AMI parcheadas para los grupos de Auto Scaling).

Consideraciones futuras

Para evitar incidentes futuros, considere implementar un programa de administración de vulnerabilidades. Amazon Inspector se puede configurar para buscar de manera automática vulnerabilidades y exposiciones comunes (CVE) en las instancias. Amazon Inspector también se puede integrar con el CSPM de Security Hub para realizar remediaciones automáticas. Considere implementar un programa regular de aplicación de parches con las Ventanas de mantenimiento de Systems Manager para minimizar la interrupción en las instancias.

La instancia EC2 tiene un sistema operativo End-Of-Life

La instancia EC2 ejecuta un sistema operativo al final de su ciclo de vida útil que el desarrollador original ya no ofrece soporte ni mantenimiento. Esto expone a la instancia a vulnerabilidades de seguridad y posibles ataques. Cuando los sistemas operativos llegan al final de su vida útil, los proveedores suelen dejar de publicar nuevos avisos de seguridad. Los avisos de seguridad existentes también pueden eliminarse de los feeds de los proveedores. En consecuencia, Amazon Inspector podría dejar de generar resultados para las CVE conocidas, lo que crearía más brechas en la cobertura de seguridad.

Consulte los sistemas operativos descatalogados en la guía del usuario de Amazon Inspector para obtener información sobre los sistemas operativos que han llegado al final de su vida útil y que Amazon Inspector puede detectar.

Solución: actualice a una versión de sistema operativo compatible

Actualice a una versión compatible del sistema operativo. En el hallazgo de exposición, abra el recurso para acceder al recurso afectado. Antes de actualizar la versión del sistema operativo de la instancia, cree una instantánea o una copia de seguridad de la AMI en caso de que necesite revertirla. A continuación, consulta las versiones disponibles en la sección Sistemas operativos compatibles de la Guía del usuario de Amazon Inspector para ver una lista de las versiones de sistemas operativos compatibles actualmente.

La instancia EC2 contiene paquetes de software malintencionado

Los paquetes malintencionados son componentes de software que contienen código dañino diseñado para comprometer la confidencialidad, la integridad y la disponibilidad de sus sistemas y datos. Los paquetes malintencionados representan una amenaza activa y crítica para su instancia, ya que los atacantes pueden ejecutar código malintencionado automáticamente sin aprovechar una vulnerabilidad. Siguiendo las prácticas recomendadas de seguridad, elimina los paquetes maliciosos para proteger tu instancia de posibles ataques.

Solución: elimina los paquetes malintencionados

Revise los detalles del paquete malicioso en la sección Referencias de la pestaña Vulnerabilidad de la característica para comprender la amenaza. Elimine los paquetes maliciosos identificados mediante el administrador de paquetes adecuado. Consulte la herramienta de administración de paquetes en la Guía del usuario de Amazon Linux 2023 para ver un ejemplo. Tras eliminar los paquetes malintencionados, considere la posibilidad de realizar un análisis para asegurarse de que se hayan eliminado todos los paquetes que el código malintencionado haya podido instalar. Para obtener más información, consulte Iniciar el análisis de On-demand malware GuardDuty en.

La instancia EC2 contiene archivos malintencionados

Los archivos malintencionados contienen código dañino diseñado para comprometer la confidencialidad, la integridad y la disponibilidad de sus sistemas y datos. Los archivos malintencionados representan una amenaza activa y crítica para su instancia, ya que los atacantes pueden ejecutar código malintencionado automáticamente sin aprovechar una vulnerabilidad. Siguiendo las prácticas recomendadas de seguridad, elimina los archivos malintencionados para proteger tu instancia de posibles ataques.

Solución: elimina los archivos malintencionados

Para identificar el volumen específico de Amazon Elastic Block Store (Amazon EBS) que contiene archivos malintencionados, consulte la sección Recursos donde encontrará información sobre el hallazgo de la característica. Una vez que haya identificado el volumen con el archivo malicioso, cree una instantánea del volumen antes de realizar cambios y, a continuación, elimine los archivos maliciosos identificados. Tras eliminar los archivos malintencionados, considere la posibilidad de realizar un análisis para asegurarse de que se han eliminado todos los archivos que pudiera haber instalado el archivo malintencionado. Para obtener más información, consulte Iniciar el análisis de On-demand malware GuardDuty en.

Características de impacto de las instancias EC2

Los rasgos de impacto describen el radio de explosión potencial de una exposición. Security Hub analiza los permisos efectivos del AWS Identity and Access Management principal asociado a la instancia EC2 para determinar los recursos posteriores a los que podría acceder un atacante si la instancia se viera comprometida. Cada rasgo de impacto identifica un patrón de escalamiento de privilegios específico. Para reducir tu radio de ataque, revisa las rutas de permisos descritas en cada rasgo y elimina cualquier privilegio innecesario.

Siguiendo los principios de seguridad estándar, otorga el mínimo privilegio proporcionando solo los permisos necesarios para realizar una tarea. Sustituya las políticas generales por políticas más específicas que concedan solo las acciones y los recursos específicos que se necesitan. Para

identificar los permisos no utilizados que desee eliminar, utilice IAM Access Analyzer para generar recomendaciones basadas en el historial de acceso. Para obtener más información, consulte las conclusiones sobre el acceso externo y no utilizado y sobre la aplicación de permisos con privilegios mínimos en la guía del usuario de IAM.

Tiene el control total de la ruta de ejecución privilegiada

El director asociado puede transferir una función e inyectar código en un recurso informático que ya tenga permisos elevados. Esto permite al principal obtener el control total sobre el ejecutor y realizar cualquier acción que permita la función del ejecutor.

Tiene una ruta directa de escalamiento de políticas

El director asociado puede modificar directamente las políticas de IAM para concederse permisos adicionales, aumentando así sus propios privilegios sin necesidad de recursos intermedios.

Tiene una ruta de secuestro de políticas de confianza

El director asociado puede modificar la política de confianza de una función de IAM para poder asumir esa función y obtener los permisos correspondientes.

Tiene una ruta de ransomware de datos

El director asociado puede cifrar o eliminar datos de una forma que podría utilizarse para el ransomware, por ejemplo, cifrando objetos de Amazon S3 con una AWS KMS clave gestionada por el cliente y, a continuación, modificando la política de claves.

Ha eliminado la ruta de restricción

El principal asociado puede eliminar las restricciones de seguridad, como los límites de permisos, las políticas de control de servicios o las declaraciones de denegación de políticas basadas en recursos, ampliando así lo que pueden hacer otros directores o el propio recurso.

Tiene el rol de pase, crea la ruta de ejecutor.

El principal asociado puede crear un nuevo recurso informático (como una función de Lambda o una instancia de Amazon EC2) y asignarle un rol privilegiado, lo que permite blanquear de manera efectiva sus propios permisos a través del nuevo recurso.

Tiene una ruta de ejecución existente (rol de intercambio).

El director asociado puede cambiar la función de IAM asociada a un recurso informático existente y sustituirla por una función más privilegiada para escalar el acceso.

Tiene una ruta de escalamiento de la cadena de funciones

El director asociado puede asumir una secuencia de funciones, en la que cada función de la cadena tiene permisos cada vez más amplios y, en última instancia, alcanza una función altamente privilegiada.

Tiene una ruta de ejecución privilegiada para inyectar código

El principal asociado puede inyectar código en un recurso informático en ejecución que tenga permisos elevados y ejecutar operaciones arbitrarias bajo la función privilegiada de ese recurso.

Ha deshabilitado la ruta del registro de auditoría

El director asociado puede deshabilitar los servicios de registro o supervisión, por ejemplo CloudTrail, cubrir eficazmente sus huellas durante una escalada o después de ella.

Tiene acceso a la ruta de ejecución existente

El principal asociado puede invocar un recurso informático existente o conectarse a él y usar su rol adjunto para realizar acciones privilegiadas.

Tiene una ruta de acuñación de credenciales

El director asociado puede crear nuevas credenciales a largo plazo (como claves de acceso o perfiles de inicio de sesión) para otros principales, estableciendo rutas de acceso persistentes que sobrevivan a la rotación de contraseñas o al vencimiento de la sesión.

Tiene una ruta de acceso a los datos del rol de pase

El principal asociado puede crear un recurso de servicio y asignarle una función de acceso a datos confidenciales y obtener acceso indirecto a esos datos a través del nuevo recurso.

Ha pasado el rol, la tarea, el secuestro, la ruta

El director asociado puede transferir un rol a una tarea programada o basada en eventos (como una función de Lambda activada por un evento), lo que le permite ejecutar código arbitrario con los permisos de ese rol.

Tiene una ruta de acceso a los datos de un solo salto

El director asociado puede acceder directamente a los recursos de datos confidenciales (como los cubos de Amazon S3 o las tablas de DynamoDB) mediante sus permisos actuales, sin necesidad de pasos de escalamiento intermedios.

Tiene una ruta de avance de la capacidad

El principal asociado tiene una ruta de escalamiento de privilegios que mejora sus capacidades generales más allá de lo que sugerirían los permisos que le han sido asignados directamente. Esta es una clasificación general para las rutas que no coinciden con un patrón más específico.

Remediación de exposiciones para los servicios de Amazon ECS

AWS Security Hub puede generar hallazgos de exposición para los servicios de Amazon Elastic Container Service (Amazon ECS).

El servicio de Amazon ECS involucrado en un resultado de exposición y su información identificatoria se incluyen en la sección Recurso de los detalles del resultado. Puede recuperar estos detalles de los recursos en la consola de Security Hub o mediante programación utilizando la API GetFindingsV2 CSPM de Security Hub.

Después de identificar el recurso involucrado en un resultado de exposición, puede eliminar el recurso si no lo necesita. Eliminar un recurso no esencial puede reducir su perfil de exposición y sus costos. AWS Si el recurso es esencial, siga estos pasos de remediación recomendados para ayudar a mitigar el riesgo. Los temas de remediación se dividen según el tipo de condición.

Un único resultado de exposición puede incluir problemas identificados en varios temas de remediación. También es posible abordar un resultado de exposición y disminuir su nivel de gravedad con solo tratar uno de los temas de remediación. El enfoque de remediación adecuado depende de los requisitos y cargas de trabajo de la organización.

> **Note**
>
> La guía de remediación que se proporciona en este tema puede requerir consultas adicionales en otros AWS recursos.

Contenido

- Condiciones de configuración incorrecta para servicios de Amazon ECS
  - El servicio de Amazon ECS usa una definición de tarea que permite que los contenedores accedan a los sistemas de archivos raíz
  - El servicio de Amazon ECS usa una definición de tarea configurada para compartir el espacio de nombres de procesos del host.

- El servicio de Amazon ECS usa una definición de tarea configurada con credenciales en texto plano en las variables de entorno.
- El servicio de Amazon ECS tiene un grupo de seguridad abierto
- El servicio Amazon ECS tiene direcciones IP públicas
- El servicio de Amazon ECS utiliza una definición de tarea configurada con el modo de redes del host habilitado.

- Características de accesibilidad de los servicios de Amazon ECS
  - Se puede acceder al servicio Amazon ECS a través de Internet
- Condiciones de vulnerabilidad para los servicios de Amazon ECS
  - El servicio de Amazon ECS tiene un contenedor con vulnerabilidades de software explotables a través de la red y con una alta probabilidad de explotación
  - El servicio de Amazon ECS tiene un contenedor con vulnerabilidades de software
  - El servicio Amazon ECS tiene un contenedor con un sistema End-Of-Life operativo
  - El servicio Amazon ECS tiene un contenedor con paquetes de software malintencionado
- Características de impacto de los servicios de Amazon ECS
  - Tiene el control total de la ruta de ejecución privilegiada
  - Tiene una ruta directa de escalamiento de políticas
  - Tiene una ruta de secuestro de políticas de confianza
  - Tiene una ruta de ransomware de datos
  - Ha eliminado la ruta de restricción
  - Tiene el rol de pase, crea la ruta de ejecutor.
  - Tiene una ruta de ejecución existente (rol de intercambio).
  - Tiene una ruta de escalamiento de la cadena de funciones
  - Tiene una ruta de ejecución privilegiada para inyectar código
  - Ha deshabilitado la ruta del registro de auditoría
  - Tiene acceso a la ruta de ejecución existente
  - Tiene una ruta de acuñación de credenciales
  - Tiene una ruta de acceso a los datos con rol de pasante
  - Tiene una ruta de secuestro de tareas de rol aprobado
  - Tiene una ruta de acceso a los datos de un solo salto

  - Tiene una ruta de avance de la capacidad

Condiciones de configuración incorrecta para servicios de Amazon ECS

Estas son las condiciones de configuración incorrecta para servicios de Amazon ECS y los pasos de remediación sugeridos.

El servicio de Amazon ECS usa una definición de tarea que permite que los contenedores accedan a los sistemas de archivos raíz

Los contenedores de Amazon ECS con acceso al sistema de archivos raíz del host pueden leer, modificar o ejecutar archivos críticos en el sistema del host. Esta configuración aumenta el riesgo de que un contenedor comprometido se pueda usar para acceder a recursos o modificarlos fuera del alcance previsto, lo que podría exponer información confidencial en el sistema de archivos del host. De acuerdo con los principios de seguridad estándar, conceda el mínimo de privilegios, lo que significa que solo concederá los permisos necesarios para realizar una tarea.

Solución: revise y modifique los contenedores con acceso al sistema de archivos del host

En el resultado de exposición, identifique el ARN de la definición de tarea. Abra la definición de tarea en la consola de Amazon ECS. Busque la sección volúmenes en la definición de tarea que define las asignaciones de rutas del host.

Revise la definición de tarea para determinar si el acceso al sistema de archivos del host es necesario para la funcionalidad del contenedor. Si no se requiere acceso al sistema de archivos del host, cree una nueva revisión de la definición de tarea y elimine cualquier definición de volumen que use rutas del host. Si se requiere acceso al sistema de archivos del host, considere configurar el contenedor para que use un sistema de archivos de solo lectura y evitar modificaciones no autorizadas.

El servicio de Amazon ECS usa una definición de tarea configurada para compartir el espacio de nombres de procesos del host.

Los contenedores de Amazon ECS que se ejecutan con espacios de nombres expuestos pueden acceder potencialmente a recursos del sistema del host y a espacios de nombres de otros contenedores. Esta configuración podría permitir a un contenedor comprometido escapar de su límite de aislamiento y acceder a procesos, interfaces de red u otros recursos fuera del alcance previsto.

Un espacio de nombres de ID de proceso (PID) proporciona separación entre los procesos. Evita que los procesos del sistema estén visibles y permite reutilizar los PID, incluido el PID 1. Si el espacio de nombres PID del host se comparte con los contenedores, los contenedores pueden ver todos los

procesos del sistema host, lo que reduce el aislamiento a nivel de proceso. Esto podría provocar el acceso no autorizado a los procesos del host, incluida la posibilidad de manipularlos y terminarlos. Siguiendo los principios de seguridad estándar, mantenga un aislamiento adecuado del espacio de nombres para los contenedores.

Solución: actualice las definiciones de las tareas con los espacios de nombres expuestos

Abra la pestaña Recursos del resultado de exposición e identifique la definición de tarea con el espacio de nombres expuesto. Abra la definición de tarea en la consola de Amazon ECS. Busque la configuración de pidMode con el valor host, lo que compartiría los espacios de nombres de ID de proceso con el host. Elimine la configuración pidMode: host de las definiciones de tarea para garantizar que los contenedores se ejecuten con un aislamiento adecuado de espacios de nombres.

El servicio de Amazon ECS usa una definición de tarea configurada con credenciales en texto plano en las variables de entorno.

Los contenedores de Amazon ECS con credenciales en texto plano en las variables de entorno exponen información de autenticación confidencial que podría verse comprometida si un atacante obtiene acceso a la definición de tarea, al entorno del contenedor o a los registros del contenedor. Esto crea un riesgo de seguridad importante, ya que las credenciales filtradas podrían usarse para acceder a otros AWS servicios o recursos.

Corrección

Tome una o más de las siguientes medidas para hacer frente a esta exposición:

Cómo reemplazar credenciales en texto plano

En el resultado de exposición, identifique la definición de tarea que contiene credenciales en texto plano. Abra la definición de tarea en la consola de Amazon ECS. Busque variables de entorno en la definición del contenedor que contengan valores confidenciales como claves de acceso de AWS , contraseñas de bases de datos o tokens de API.

Considere las siguientes alternativas para transferir credenciales:

- En lugar de usar claves de AWS acceso, usa las funciones de ejecución de tareas y de ejecución de tareas de IAM para conceder permisos a tus contenedores.
- Guarda las credenciales como datos secretos AWS Secrets Manager y haz referencia a ellas en la definición de la tarea.

Actualizar definiciones de tareas

Cree una nueva revisión de la definición de tarea que gestione las credenciales de forma segura. Luego, actualice el servicio de Amazon ECS para usar la nueva revisión de la definición de tarea.

El servicio de Amazon ECS tiene un grupo de seguridad abierto

Los grupos de seguridad funcionan como firewalls virtuales para las tareas de Amazon ECS y controlan el tráfico de entrada y salida. Los grupos de seguridad abiertos, que permiten acceso sin restricciones desde cualquier dirección IP, pueden exponer los contenedores a acceso no autorizado, lo que aumenta el riesgo de exposición a herramientas automatizadas de detección y a ataques dirigidos. Siguiendo los principios de seguridad estándar, restrinja el acceso de los grupos de seguridad a direcciones IP y puertos específicos.

Corrección

Tome una o más de las siguientes medidas para hacer frente a esta exposición:

Revisión de las reglas del grupo de seguridad y evaluación de la configuración actual

Abra el recurso del grupo de seguridad de Amazon ECS. Evalúe qué puertos están abiertos y accesibles desde rangos amplios de direcciones IP, como `(0.0.0.0/0 or ::/0)`.

Modificación de reglas del grupo de seguridad

Modifique las reglas del grupo de seguridad para restringir el acceso únicamente a direcciones IP o rangos específicos y de confianza. Al actualizar las reglas del grupo de seguridad, considere separar los requisitos de acceso para distintos segmentos de red mediante la creación de reglas para cada rango de IP de origen requerido o la restricción del acceso únicamente a puertos específicos.

Modificación de reglas del grupo de seguridad

Considere las siguientes opciones para métodos de acceso alternativos:

- El Administrador de sesiones proporciona acceso seguro mediante intérprete de comandos a las instancias de Amazon EC2 sin necesidad de puertos de entrada, de administrar claves SSH ni de mantener hosts bastión.
- Las listas de control de acceso de red (NACL) ofrecen una capa adicional de seguridad en el nivel de la subred. A diferencia de los grupos de seguridad, las NACL no mantienen estado y requieren que se defina explícitamente tanto las reglas entrantes como las salientes.

El servicio Amazon ECS tiene direcciones IP públicas

A los servicios de Amazon ECS con direcciones IP públicas asignadas a sus tareas se accede directamente desde Internet. Si bien esto puede ser necesario para los servicios que deben estar disponibles públicamente, amplía la superficie expuesta a ataques y aumenta el riesgo de accesos no autorizados.

Corrección

Tome una o más de las siguientes medidas para hacer frente a esta exposición:

Identificación de servicios con direcciones IP públicas

En el resultado de exposición, identifique el servicio de Amazon ECS que tiene direcciones IP públicas asignadas a sus tareas. Busque el ajuste `assignPublicIp` con el valor `ENABLED` en la configuración del servicio.

Actualizar definiciones de tareas

Cree una nueva revisión de la definición de tarea que desactive las direcciones IP públicas. Luego, actualice el servicio de Amazon ECS para usar la nueva revisión de la definición de tarea.

Implementación de patrones de acceso de red privada

Para las instancias que ejecutan aplicaciones web, considere utilizar un equilibrador de carga (LB). Los equilibradores de carga se pueden configurar para permitir que las instancias se ejecuten en subredes privadas mientras el equilibrador de carga se ejecuta en una subred pública y gestiona el tráfico de Internet.

El servicio de Amazon ECS utiliza una definición de tarea configurada con el modo de redes del host habilitado.

Los contenedores de Amazon ECS que se ejecutan con el modo de redes del host comparten el espacio de nombres de red con el host, lo que permite acceso directo a las interfaces de red, puertos y tablas de enrutamiento del host. Esta configuración evita el aislamiento de red que proporcionan los contenedores, lo que puede exponer directamente a redes externas los servicios que se ejecutan en el contenedor y permitir que los contenedores modifiquen la configuración de red del host. Siguiendo los principios de seguridad estándar, mantenga un aislamiento de red adecuado para los contenedores.

Corrección

Tome una o más de las siguientes medidas para hacer frente a esta exposición:

Desactivación del modo de redes del host

En el resultado de exposición, identifique la definición de tarea con el modo de redes del host. Abra la definición de tarea en la consola de Amazon ECS. Busque el ajuste networkMode con el valor host en la definición de tarea.

Considere las siguientes opciones para desactivar el modo de redes del host:

- El modo de red `awsvpc` proporciona el nivel más sólido de aislamiento de red al asignar a cada tarea su propia interfaz de red elástica.
- El modo de red `bridge` proporciona aislamiento y permite asignaciones de puertos para exponer puertos específicos del contenedor al host.

Actualizar definiciones de tareas

Cree una nueva revisión de la definición de tarea con la configuración de modo de red actualizada. Luego, actualice el servicio de Amazon ECS para usar la nueva revisión de la definición de tarea.

Características de accesibilidad de los servicios de Amazon ECS

Estas son las características de accesibilidad de los servicios de Amazon ECS y las medidas de corrección sugeridas.

Se puede acceder al servicio Amazon ECS a través de Internet

Se puede acceder directamente a un servicio de Amazon ECS que ejecuta tareas en una subred pública desde Internet. Esto aumenta la superficie de ataque y el riesgo de acceso no autorizado. Siguiendo los principios de seguridad estándar, ejecute las tareas en subredes privadas y permita solo el acceso a Internet que su servicio requiera.

Corrección

Tome una o más de las siguientes medidas para hacer frente a esta exposición:

Ejecute tareas en una subred privada

Para sacar tus tareas de una subred pública, actualiza la configuración de red para tu tipo de lanzamiento:

- Para Fargate, especifica las subredes privadas en la configuración de red de tu servicio Amazon ECS y establécelas en. `assignPublicIp` `DISABLED` Amazon ECS aloja cada tarea en una

subred privada y enruta su tráfico saliente a través de una puerta de enlace NAT que usted asocia a la subred.

- Para EC2, lance las instancias de contenedor que proporcionan la capacidad de su clúster en subredes privadas. Las tareas utilizan la red privada del host y dirigen el tráfico saliente a través de una puerta de enlace NAT.

Utilice una puerta de enlace NAT para el acceso saliente

Para las tareas en una subred privada que requieren acceso saliente a Internet, utilice una puerta de enlace NAT. Puede usar una puerta de enlace NAT para permitir que las tareas inicien conexiones salientes a Internet e impedir las conexiones entrantes desde Internet. Para obtener más información, consulte Conectar las aplicaciones de Amazon ECS a Internet en la Guía para desarrolladores de Amazon ECS.

Utilice un balanceador de cargas para el acceso entrante

En el caso de los servicios que necesitan aceptar el tráfico de Internet, ejecuta tus tareas en subredes privadas detrás de un balanceador de cargas que se ejecute en una subred pública. Para aumentar la protección contra los bots y los exploits web, asocia el AWS Web Application Firewall (WAF) a tu balanceador de cargas. Para obtener más información, consulte Utilizar el equilibrio de carga para distribuir el tráfico del servicio Amazon ECS en la Guía para desarrolladores de Amazon ECS.

Condiciones de vulnerabilidad para los servicios de Amazon ECS

Aquí se presentan condiciones de vulnerabilidad para Amazon ECS y los pasos de remediación sugeridos.

El servicio de Amazon ECS tiene un contenedor con vulnerabilidades de software explotables a través de la red y con una alta probabilidad de explotación

1. Comprensión de la exposición

   Los resultados de vulnerabilidades de paquetes identifican los paquetes de software de su entorno de AWS expuestos a vulnerabilidades y riesgos comunes (CVE). Los atacantes pueden aprovechar las vulnerabilidades no parcheadas y poner en riesgo la confidencialidad, integridad o disponibilidad de los datos, así como acceder a otros sistemas. Las imágenes de contenedor de ECR pueden presentar resultados de vulnerabilidades de paquetes.
2. Remediación de la exposición

a. Actualización de la versión del paquete

   Revise el resultado de vulnerabilidad del paquete correspondiente a la imagen de contenedor de ECR. Actualice la versión del paquete según lo sugerido por Amazon Inspector. Para obtener más información, consulte Consulta de los detalles de los resultados de Amazon Inspector en la Guía del usuario de Amazon Inspector. La sección Remediación de los detalles del resultado en la consola de Amazon Inspectori ndica qué comandos puede ejecutar para actualizar el paquete.

b. Actualización de las imágenes base de contenedor

   Vuelva a compilar y actualice periódicamente las imágenes base de contenedor para mantener los contenedores actualizados. Al reconstruir una imagen, no incluya componentes innecesarios para reducir la superficie de ataque. Para obtener instrucciones sobre cómo volver a compilar una imagen de contenedor, consulte Cómo volver a compilar las imágenes con frecuencia.

El servicio de Amazon ECS tiene un contenedor con vulnerabilidades de software

Los paquetes de software que se instalan en contenedores de Amazon ECS pueden estar expuestos a vulnerabilidades y exposiciones comunes (CVE). Las vulnerabilidades de prioridad baja representan debilidades de seguridad con una gravedad o capacidad de explotación menor en comparación con las vulnerabilidades de prioridad alta. Si bien estas vulnerabilidades representan un riesgo menos inmediato, los atacantes aún pueden aprovechar estas vulnerabilidades no corregidas para comprometer la confidencialidad, la integridad o la disponibilidad de los datos, o para acceder a otros sistemas.

Corrección

Tome una o más de las siguientes medidas para hacer frente a esta exposición:

Actualizaciones de las imágenes de contenedores afectadas

Consulte la sección Referencias en la pestaña Vulnerabilidad de la condición. La documentación del proveedor puede incluir instrucciones específicas de remediación.

Aplique la remediación correspondiente según estas pautas generales:

- Actualice las imágenes de contenedor para usar versiones con parches de los paquetes afectados.
- Actualice las dependencias afectadas en la aplicación a sus versiones seguras más recientes.

Después de actualizar la imagen de contenedor, publíquela en el registro de contenedores y actualice la definición de tarea de Amazon ECS para usar la nueva imagen.

Consideraciones futuras

Para fortalecer aún más la posición de seguridad de las imágenes de contenedor, considere seguir las prácticas recomendadas de seguridad para tareas y contenedores de Amazon ECS. Amazon Inspector se puede configurar para analizar automáticamente vulnerabilidades y exposiciones comunes (CVE) en los contenedores. Amazon Inspector también se puede integrar con el CSPM de Security Hub para realizar remediaciones automáticas. Considere implementar una programación regular de aplicación de parches mediante Systems Manager Maintenance Windows para minimizar las interrupciones en los contenedores.

El servicio Amazon ECS tiene un contenedor con un sistema End-Of-Life operativo

El contenedor de Amazon ECS se basa en un sistema operativo al final de su vida útil que el desarrollador original ya no ofrece soporte ni mantenimiento. Esto expone al contenedor a vulnerabilidades de seguridad y posibles ataques. Cuando los sistemas operativos llegan al final de su vida útil, los proveedores suelen dejar de publicar nuevos avisos de seguridad. Los avisos de seguridad existentes también pueden eliminarse de los feeds de los proveedores. En consecuencia, Amazon Inspector podría dejar de generar resultados para las CVE conocidas, lo que crearía más brechas en la cobertura de seguridad.

Consulte los sistemas operativos descatalogados en la guía del usuario de Amazon Inspector para obtener información sobre los sistemas operativos que han llegado al final de su vida útil y que Amazon Inspector puede detectar.

Solución: actualice a una versión de sistema operativo compatible

Actualice a una versión compatible del sistema operativo. En el hallazgo de exposición, abra el recurso para acceder al recurso afectado. Antes de actualizar la versión del sistema operativo de la imagen del contenedor, consulta las versiones disponibles en los sistemas operativos compatibles en la guía del usuario de Amazon Inspector para ver una lista de las versiones del sistema operativo compatibles actualmente. Después de actualizar la imagen de contenedor, publíquela en el registro de contenedores y actualice la definición de tarea de Amazon ECS para usar la nueva imagen.

El servicio Amazon ECS tiene un contenedor con paquetes de software malintencionado

Los paquetes malintencionados son componentes de software que contienen código dañino diseñado para comprometer la confidencialidad, la integridad y la disponibilidad de sus sistemas y

datos. Los paquetes malintencionados representan una amenaza activa y crítica para las imágenes de los contenedores de Amazon ECS, ya que los atacantes pueden ejecutar código malintencionado automáticamente sin aprovechar una vulnerabilidad. Siga las prácticas recomendadas de seguridad y elimine los paquetes maliciosos para proteger sus contenedores de posibles ataques.

Solución: elimine los paquetes malintencionados

Revise los detalles del paquete malicioso en la sección Referencias de la pestaña Vulnerabilidad de la característica para comprender la amenaza. Elimine los paquetes maliciosos identificados de las imágenes de su contenedor y, a continuación, vuelva a crearlos. Para obtener más información, consulte ContainerDependency en la AWS Referencia de la API de Amazon ECS.

Después de actualizar la imagen de contenedor, publíquela en el registro de contenedores y actualice la definición de tarea de Amazon ECS para usar la nueva imagen. Para obtener más información, consulte Actualización de una definición de tarea de Amazon ECS mediante la consola en la Guía para desarrolladores de AWS Amazon ECS.

Características de impacto de los servicios de Amazon ECS

Los rasgos de impacto describen el radio de explosión potencial de una exposición. Security Hub analiza los permisos efectivos del AWS Identity and Access Management principal asociado al servicio Amazon ECS para determinar los recursos posteriores a los que podría acceder un atacante si el servicio se viera comprometido. Cada rasgo de impacto identifica un patrón de escalamiento de privilegios específico. Para reducir tu radio de ataque, revisa las rutas de permisos descritas en cada rasgo y elimina cualquier privilegio innecesario.

Siguiendo los principios de seguridad estándar, otorga el mínimo privilegio proporcionando solo los permisos necesarios para realizar una tarea. Sustituya las políticas generales por políticas más específicas que concedan solo las acciones y los recursos específicos que se necesitan. Para identificar los permisos no utilizados que desee eliminar, utilice IAM Access Analyzer para generar recomendaciones basadas en el historial de acceso. Para obtener más información, consulte las conclusiones sobre el acceso externo y no utilizado y sobre la aplicación de permisos con privilegios mínimos en la guía del usuario de IAM.

Tiene el control total de la ruta de ejecución privilegiada

El director asociado puede transferir una función e inyectar código en un recurso informático que ya tenga permisos elevados. Esto permite al principal obtener el control total sobre el ejecutor y realizar cualquier acción que permita la función del ejecutor.

Tiene una ruta directa de escalamiento de políticas

El director asociado puede modificar directamente las políticas de IAM para concederse permisos adicionales, aumentando así sus propios privilegios sin necesidad de recursos intermedios.

Tiene una ruta de secuestro de políticas de confianza

El director asociado puede modificar la política de confianza de una función de IAM para poder asumir esa función y obtener los permisos correspondientes.

Tiene una ruta de ransomware de datos

El director asociado puede cifrar o eliminar datos de una forma que podría utilizarse para el ransomware, por ejemplo, cifrando objetos de Amazon S3 con una AWS KMS clave gestionada por el cliente y, a continuación, modificando la política de claves.

Ha eliminado la ruta de restricción

El principal asociado puede eliminar las restricciones de seguridad, como los límites de permisos, las políticas de control de servicios o las declaraciones de denegación de políticas basadas en recursos, ampliando así lo que pueden hacer otros directores o el propio recurso.

Tiene el rol de pase, crea la ruta de ejecutor.

El principal asociado puede crear un nuevo recurso informático (como una función de Lambda o una instancia de Amazon EC2) y asignarle un rol privilegiado, lo que permite blanquear de manera efectiva sus propios permisos a través del nuevo recurso.

Tiene una ruta de ejecución existente (rol de intercambio).

El director asociado puede cambiar la función de IAM asociada a un recurso informático existente y sustituirla por una función más privilegiada para escalar el acceso.

Tiene una ruta de escalamiento de la cadena de funciones

El director asociado puede asumir una secuencia de funciones, en la que cada función de la cadena tiene permisos cada vez más amplios y, en última instancia, alcanza una función altamente privilegiada.

Tiene una ruta de ejecución privilegiada para inyectar código

El principal asociado puede inyectar código en un recurso informático en ejecución que tenga permisos elevados y ejecutar operaciones arbitrarias bajo la función privilegiada de ese recurso.

Ha deshabilitado la ruta del registro de auditoría

El director asociado puede deshabilitar los servicios de registro o supervisión, por ejemplo CloudTrail, cubrir eficazmente sus huellas durante una escalada o después de ella.

Tiene acceso a la ruta de ejecución existente

El principal asociado puede invocar un recurso informático existente o conectarse a él y usar su rol adjunto para realizar acciones privilegiadas.

Tiene una ruta de acuñación de credenciales

El director asociado puede crear nuevas credenciales a largo plazo (como claves de acceso o perfiles de inicio de sesión) para otros principales, estableciendo rutas de acceso persistentes que sobrevivan a la rotación de contraseñas o al vencimiento de la sesión.

Tiene una ruta de acceso a los datos con rol de pasante

El principal asociado puede crear un recurso de servicio y asignarle una función de acceso a datos confidenciales y obtener acceso indirecto a esos datos a través del nuevo recurso.

Tiene una ruta de secuestro de tareas de rol aprobado

El director asociado puede transferir un rol a una tarea programada o basada en eventos (como una función de Lambda activada por un evento), lo que le permite ejecutar código arbitrario con los permisos de ese rol.

Tiene una ruta de acceso a los datos de un solo salto

El director asociado puede acceder directamente a los recursos de datos confidenciales (como los cubos de Amazon S3 o las tablas de DynamoDB) mediante sus permisos actuales, sin necesidad de pasos de escalamiento intermedios.

Tiene una ruta de avance de la capacidad

El principal asociado tiene una ruta de escalamiento de privilegios que mejora sus capacidades generales más allá de lo que sugerirían los permisos que le han sido asignados directamente. Esta es una clasificación general para las rutas que no coinciden con un patrón más específico.

Remediación de exposiciones para clústeres de Amazon EKS

AWS Security Hub puede generar hallazgos de exposición para los clústeres de Amazon Elastic Kubernetes Service (Amazon EKS).

El clúster de Amazon EKS involucrado en un resultado de exposición y su información de identificación aparecen en la sección Recursos de los detalles del resultado. Puede recuperar estos detalles de los recursos en la consola de Security Hub o mediante programación utilizando la API CSPM GetFindingsV2 de Security Hub.

Después de identificar el recurso involucrado en un resultado de exposición, puede eliminar el recurso si no lo necesita. Eliminar un recurso no esencial puede reducir su perfil de exposición y sus costos. AWS Si el recurso es esencial, siga estos pasos de remediación recomendados para ayudar a mitigar el riesgo. Los temas de remediación se dividen según el tipo de condición.

Un único resultado de exposición puede incluir problemas identificados en varios temas de remediación. También es posible abordar un resultado de exposición y disminuir su nivel de gravedad con solo tratar uno de los temas de remediación. El enfoque de remediación adecuado depende de los requisitos y cargas de trabajo de la organización.

> **Note**
>
> La guía de remediación que se proporciona en este tema puede requerir consultas adicionales en otros AWS recursos.

Contenido

- Condiciones de configuración incorrecta para clústeres de Amazon EKS
  - El clúster de Amazon EKS permite acceso público
  - El clúster de Amazon EKS utiliza una versión de Kubernetes que no es compatible
  - El clúster de Amazon EKS utiliza secretos de Kubernetes sin cifrar
- Características de vulnerabilidad de los clústeres de Amazon EKS
  - El clúster de Amazon EKS tiene un contenedor con vulnerabilidades de software explotables a través de la red y con una alta probabilidad de explotación
  - El clúster de Amazon EKS tiene un contenedor con vulnerabilidades de software
  - El clúster de Amazon EKS tiene un contenedor con un End-Of-Life sistema operativo
  - El clúster de Amazon EKS tiene un contenedor con paquetes de software malintencionado
  - El clúster Amazon EKS contiene archivos maliciosos

Condiciones de configuración incorrecta para clústeres de Amazon EKS

Aquí se presentan condiciones de configuración incorrecta para clústeres de Amazon EKS y pasos de remediación sugeridos.

El clúster de Amazon EKS permite acceso público

El punto de conexión del clúster de Amazon EKS es el punto de conexión que utiliza para comunicarse con el servidor de la API de Kubernetes del clúster. De manera predeterminada, este punto de conexión es público en Internet. Los puntos de conexión públicos aumentan la superficie expuesta a ataques y el riesgo de acceso no autorizado al servidor de la API de Kubernetes, lo que podría permitir que atacantes accedan o modifiquen recursos del clúster o accedan a información confidencial. Siguiendo las prácticas recomendadas de seguridad, restrinja el acceso al punto final del clúster de Amazon EKS únicamente a los intervalos de IP necesarios.

Corrección

Tome una o más de las siguientes medidas para hacer frente a esta exposición:

Modificación del acceso al punto de conexión

En el resultado de exposición, abra el recurso. Esto abre el clúster de Amazon EKS afectado. Puede configurar el clúster para usar acceso privado, acceso público o ambos.

Con acceso privado, las solicitudes a la API de Kubernetes que se originan dentro de la VPC del clúster utilizan el punto de conexión de VPC privado. Con acceso público, las solicitudes a la API de Kubernetes que se originan fuera de la VPC del clúster utilizan el punto de conexión público.

Modificación o eliminación del acceso público al clúster

Para modificar el acceso al punto de conexión de un clúster existente, consulte Modificación del acceso al punto de conexión del clúster en la Guía de usuario del servicio de Amazon Elastic Kubernetes. Implemente reglas más restrictivas basadas en intervalos de direcciones IP específicos o en grupos de seguridad. Si es necesario un acceso público limitado, restrinja el acceso a intervalos específicos de bloques de CIDR o utilice listas de prefijos.

El clúster de Amazon EKS utiliza una versión de Kubernetes que no es compatible

Amazon EKS admite cada versión de Kubernetes durante un periodo limitado. La ejecución de clústeres con versiones de Kubernetes que no son compatibles puede exponer el entorno a

vulnerabilidades de seguridad, ya que los parches de CVE se dejarán de publicar para versiones obsoletas. Las versiones que no son compatibles pueden contener vulnerabilidades de seguridad conocidas que pueden ser aprovechadas por atacantes y carecen de características de seguridad que podrían estar disponibles en versiones más recientes. Siga las prácticas recomendadas de seguridad y mantenga su versión de Kubernetes actualizada.

Solución: actualice la versión de Kubernetes

En el resultado de exposición, abra el recurso. Esto abre el clúster de Amazon EKS afectado. Antes de actualizar su clúster, revise Versiones disponibles con soporte estándar en la Guía del usuario del Amazon Elastic Kubernetes Service para obtener una lista de las versiones de Kubernetes admitidas actualmente.

El clúster de Amazon EKS utiliza secretos de Kubernetes sin cifrar

Los secretos de Kubernetes se almacenan, de manera predeterminada, sin cifrar en el almacén de datos subyacente del servidor de la API (etcd). Cualquier persona con acceso a la API o con acceso a etcd puede recuperar o modificar un secreto. Para evitar esto, debe cifrar los secretos de Kubernetes en reposo. Si los secretos de Kubernetes no están cifrados, son vulnerables a accesos no autorizados si etcd se ve comprometido. Dado que los secretos suelen contener información confidencial como contraseñas y tokens de API, su exposición podría generar accesos no autorizados a otras aplicaciones y datos. Siga las prácticas recomendadas de seguridad y cifre toda la información confidencial almacenada en los secretos de Kubernetes.

Solución: cifra los secretos de Kubernetes

Amazon EKS admite el cifrado de los secretos de Kubernetes mediante claves de KMS a través de cifrado de sobre. Para habilitar el cifrado de los secretos de Kubernetes para el clúster de EKS, consulte Cifrado de secretos de Kubernetes con KMS en clústeres existentes en la Guía del usuario de Amazon EKS.

Características de vulnerabilidad de los clústeres de Amazon EKS

Aquí se presentan las condiciones de vulnerabilidad para clústeres de Amazon EKS.

El clúster de Amazon EKS tiene un contenedor con vulnerabilidades de software explotables a través de la red y con una alta probabilidad de explotación

Los paquetes de software instalados en clústeres de Amazon EKS pueden estar expuestos a vulnerabilidades y exposiciones comunes (CVE). Los CVE críticos representan importantes riesgos

de seguridad para su AWS entorno. Usuarios no autorizados pueden explotar estas vulnerabilidades sin parches para comprometer la confidencialidad, integridad o disponibilidad de los datos, o para acceder a otros sistemas. Las vulnerabilidades críticas con alta probabilidad de explotación representan amenazas de seguridad inmediatas, ya que el código de explotación puede estar disponible públicamente y ser utilizado activamente por atacantes o por herramientas automatizadas de detección. Siguiendo las prácticas recomendadas de seguridad, corrija estas vulnerabilidades para proteger la instancia de los ataques.

Solución: actualice las instancias afectadas

Actualice las imágenes de contenedores a versiones más recientes que incluyan correcciones de seguridad para las vulnerabilidades identificadas. Esto normalmente implica volver a compilar las imágenes de los contenedores con imágenes base o dependencias actualizadas y luego implementar las nuevas imágenes en el clúster de Amazon EKS.

El clúster de Amazon EKS tiene un contenedor con vulnerabilidades de software

Los paquetes de software instalados en clústeres de Amazon EKS pueden estar expuestos a vulnerabilidades y exposiciones comunes (CVE). Los CVE no críticos representan debilidades de seguridad con menor gravedad o capacidad de explotación en comparación con los CVE críticos. Si bien estas vulnerabilidades suponen un riesgo menos inmediato, los atacantes pueden seguir explotando estas vulnerabilidades no corregidas para comprometer la confidencialidad, la integridad o la disponibilidad de los datos, o para acceder a otros sistemas. Siguiendo las prácticas recomendadas de seguridad, corrija estas vulnerabilidades para proteger tu instancia de los ataques.

Solución: actualice las instancias afectadas

Actualice las imágenes de contenedores a versiones más recientes que incluyan correcciones de seguridad para las vulnerabilidades identificadas. Esto normalmente implica volver a compilar las imágenes de los contenedores con imágenes base o dependencias actualizadas y luego implementar las nuevas imágenes en el clúster de Amazon EKS.

El clúster de Amazon EKS tiene un contenedor con un End-Of-Life sistema operativo

La imagen del contenedor de Amazon EKS se basa en un sistema operativo al final de su vida útil que el desarrollador original ya no admite ni mantiene. Esto expone al contenedor a vulnerabilidades de seguridad y posibles ataques. Cuando los sistemas operativos llegan al final de su vida útil, los proveedores suelen dejar de publicar nuevos avisos de seguridad. Los avisos de seguridad existentes también pueden eliminarse de los feeds de los proveedores. En consecuencia, Amazon

Inspector podría dejar de generar hallazgos para las CVE conocidas, lo que crearía más brechas en la cobertura de seguridad.

Consulte los sistemas operativos descatalogados en la guía del usuario de Amazon Inspector para obtener información sobre los sistemas operativos que han llegado al final de su vida útil y que Amazon Inspector puede detectar.

Solución: actualice a una versión de sistema operativo compatible

Actualice a una versión compatible del sistema operativo. En el hallazgo de exposición, abra el recurso para acceder al recurso afectado. Antes de actualizar la versión del sistema operativo de la imagen del contenedor, consulta las versiones disponibles en los sistemas operativos compatibles en la guía del usuario de Amazon Inspector para ver una lista de las versiones del sistema operativo compatibles actualmente. Tras actualizar la imagen de su contenedor, reconstruya y vuelva a implementar los contenedores en el clúster de Amazon EKS.

El clúster de Amazon EKS tiene un contenedor con paquetes de software malintencionado

Los paquetes malintencionados son componentes de software que contienen código dañino diseñado para comprometer la confidencialidad, la integridad y la disponibilidad de sus sistemas y datos. Los paquetes malintencionados representan una amenaza activa y crítica para su clúster de Amazon EKS, ya que los atacantes pueden ejecutar código malicioso automáticamente sin aprovechar una vulnerabilidad. Siga las prácticas recomendadas de seguridad y elimine los paquetes malintencionados para proteger su clúster de posibles ataques.

Solución: elimina los paquetes malintencionados

Revise los detalles del paquete malicioso en la sección Referencias de la pestaña Vulnerabilidad de la característica para comprender la amenaza. Elimine los paquetes maliciosos identificados de las imágenes de su contenedor. A continuación, elimina los pods con la imagen comprometida.

Actualice sus implementaciones de Kubernetes para usar las imágenes de contenedor actualizadas. A continuación, implementa los cambios y vuelve a implementar los pods.

El clúster Amazon EKS contiene archivos maliciosos

Los archivos malintencionados contienen código dañino diseñado para comprometer la confidencialidad, la integridad y la disponibilidad de sus sistemas y datos. Los archivos malintencionados representan una amenaza activa y crítica para su clúster, ya que los atacantes

pueden ejecutar código malintencionado automáticamente sin aprovechar una vulnerabilidad. Siguiendo las prácticas recomendadas de seguridad, elimina los archivos malintencionados para proteger tu clúster de posibles ataques.

Solución: elimina los archivos malintencionados

Para identificar el volumen específico de Amazon Elastic Block Store (Amazon EBS) que contiene archivos malintencionados, consulte la sección Recursos donde encontrará información sobre el hallazgo de la característica. Una vez que haya identificado el volumen con el archivo malintencionado, elimine los archivos maliciosos identificados. Tras eliminar los archivos malintencionados, considere la posibilidad de realizar un análisis para asegurarse de que se hayan eliminado todos los archivos que pudiera haber instalado el archivo malintencionado. Para obtener más información, consulte Iniciar el análisis de On-demand malware GuardDuty en.

Remediación de exposiciones para usuarios de IAM

AWS Security Hub puede generar hallazgos de exposición para los usuarios de AWS Identity and Access Management (IAM).

En la consola de Security Hub, el usuario de IAM involucrado en un resultado de exposición y su información de identificación se enumeran en la sección Recursos de los detalles del resultado. Mediante programación, puede recuperar los detalles de los recursos con el GetFindingsV2 funcionamiento de la API CSPM de Security Hub.

Después de identificar el recurso involucrado en un resultado de exposición, puede eliminar el recurso si no lo necesita. Eliminar un recurso no esencial puede reducir su perfil de exposición y sus costos. AWS Si el recurso es esencial, siga estos pasos de remediación recomendados para ayudar a mitigar el riesgo. Los temas de remediación se dividen según el tipo de condición.

Un único resultado de exposición puede incluir problemas identificados en varios temas de remediación. También es posible abordar un resultado de exposición y disminuir su nivel de gravedad con solo tratar uno de los temas de remediación. El enfoque de remediación adecuado depende de los requisitos y cargas de trabajo de la organización.

> **Note**
>
> La guía de remediación que se proporciona en este tema puede requerir consultas adicionales en otros AWS recursos.

Las prácticas recomendadas de IAM indican que es conveniente crear roles de IAM o usar federación con un proveedor de identidades para acceder a AWS con credenciales temporales en lugar de crear usuarios individuales de IAM. Si esa es una opción para su organización y para su caso práctico, cambie a roles o federaciones en lugar de usar usuarios de IAM. Para obtener más información, consulte Usuarios de IAM en la Guía del usuario de IAM.

Contenido

- Condiciones de configuración incorrecta para usuarios de IAM
  - El usuario de IAM no tiene MFA habilitado
  - La AWS la cuenta del usuario de IAM tiene políticas de contraseñas débiles
  - El usuario de IAM tiene claves de acceso que no se han rotado
  - El usuario de IAM tiene una política que permite acceso sin restricciones al descifrado de claves de KMS
- Características de acceso no utilizadas para los usuarios de IAM
- Características de impacto para los usuarios de IAM
  - Tiene el control total de la ruta de ejecución privilegiada
  - Tiene una ruta directa de escalamiento de políticas
  - Tiene una ruta de secuestro de políticas de confianza
  - Tiene una ruta de ransomware de datos
  - Ha eliminado la ruta de restricción
  - Tiene el rol de pase, crea la ruta de ejecutor.
  - Tiene una ruta de ejecución existente (rol de intercambio).
  - Tiene una ruta de escalamiento de la cadena de funciones
  - Tiene una ruta de ejecución privilegiada para inyectar código
  - Ha deshabilitado la ruta del registro de auditoría
  - Tiene acceso a la ruta de ejecución existente
  - Tiene una ruta de acuñación de credenciales
  - Tiene una ruta de acceso a los datos con rol de pasante
  - Ha pasado el rol, la tarea, el secuestro, la ruta
  - Tiene una ruta de acceso a los datos de un solo salto
  - Tiene una ruta de avance de la capacidad

Condiciones de configuración incorrecta para usuarios de IAM

Aquí se presentan condiciones de configuración incorrecta para usuarios de IAM y pasos de remediación sugeridos.

El usuario de IAM no tiene MFA habilitado

Multi-factor La autenticación (MFA) añade una capa adicional de protección además del nombre de usuario y la contraseña. Cuando la MFA está habilitada y un usuario de IAM inicia sesión en un AWS sitio web, se le solicita su nombre de usuario, contraseña y un código de autenticación de su AWS dispositivo de MFA. La entidad de autenticación debe poseer un dispositivo que emita una clave sujeta a limitación temporal y debe tener conocimiento de una credencial. Sin la MFA, si la contraseña de un usuario se ve comprometida, el atacante obtiene acceso total a los permisos del usuario. AWS Siguiendo los principios de seguridad estándar, habilite la MFA para todas las cuentas y usuarios que tengan Consola de administración de AWS acceso.

Corrección

Tome una o más de las siguientes medidas para hacer frente a esta exposición:

Revisión de tipos de MFA

AWS admite los siguientes tipos de MFA:

- Claves de acceso y claves de seguridad
- Aplicaciones de autenticador virtual
- Tokens TOTP físicos

Aunque la autenticación con un dispositivo físico normalmente proporciona una protección de seguridad más estricta, usar cualquier tipo de MFA es más seguro que tener MFA desactivado.

Habilitar MFA

Para habilitar el tipo de MFA que se ajuste a sus requisitos, consulte Autenticación multifactor de AWS en IAM en la Guía del usuario de IAM. Siga los pasos correspondientes al tipo específico de MFA que desea implementar. Para organizaciones que administran muchos usuarios, quizá desee imponer el uso de MFA y exigir MFA para acceder a recursos sensibles.

La AWS la cuenta del usuario de IAM tiene políticas de contraseñas débiles

Las políticas de contraseñas ayudan a proteger contra accesos no autorizados mediante la aplicación obligatoria de requisitos mínimos de complejidad para las contraseñas de usuarios de IAM. Sin políticas de contraseñas sólidas, aumenta el riesgo de que las cuentas de usuario se vean comprometidas mediante adivinación de contraseñas o ataques de fuerza bruta. Siguiendo los principios de seguridad estándar, implementa una política de contraseñas seguras para garantizar que los usuarios creen contraseñas complejas y difíciles de adivinar.

Corrección

Tome una o más de las siguientes medidas para hacer frente a esta exposición:

Configuración de una política de contraseñas sólida

Vaya al panel de IAM y diríjase a la sección de configuración de la cuenta. Revise la configuración actual de la política de contraseñas de la cuenta, lo que incluye la longitud mínima, los tipos de caracteres requeridos y los parámetros de expiración de contraseñas.

Como mínimo, sigue estas prácticas recomendadas al configurar tu política de contraseñas:

- Exija al menos un carácter en mayúscula.
- Exija al menos un carácter en minúscula.
- Exija al menos un símbolo.
- Exija al menos un número
- Exija al menos ocho caracteres.

Consideraciones adicionales de seguridad

Considere estas medidas de seguridad adicionales además de una política de contraseñas sólida:

- MFA agrega una capa adicional de seguridad al requerir una forma adicional de autenticación. Esto ayuda a evitar accesos no autorizados incluso si las credenciales se ven comprometidas.
- Configuración de elementos de condición para restringir cuándo y cómo se pueden utilizar los permisos administrativos según factores como la dirección IP de origen o la antigüedad de la MFA.

El usuario de IAM tiene claves de acceso que no se han rotado

Las claves de acceso constan de un identificador de clave de acceso y una clave de acceso secreta que permiten el acceso programático a AWS los recursos. Cuando las claves de acceso permanecen sin cambios durante periodos prolongados, aumentan el riesgo de acceso no autorizado si llegan a verse comprometidas. Siguiendo las prácticas recomendadas de seguridad, rote las claves de acceso cada 90 días para minimizar la oportunidad de que los atacantes usen credenciales comprometidas.

Solución: rote las claves de acceso

En el resultado de exposición, abra el recurso. Se abre la ventana de detalles del usuario. Para rotar claves de acceso, consulte Administración de claves de acceso para usuarios de IAM en la Guía del usuario de IAM.

El usuario de IAM tiene una política que permite acceso sin restricciones al descifrado de claves de KMS

AWS KMS le permite crear y administrar las claves criptográficas que se utilizan para proteger sus datos. Las políticas de IAM que permiten permisos de AWS KMS descifrado sin restricciones (por ejemplo, `kms:Decrypt` o`kms:ReEncryptFrom`) en todas las claves de KMS pueden provocar el acceso no autorizado a los datos si las credenciales de un usuario de IAM se ven comprometidas. Si un atacante obtiene acceso a estas credenciales, podría descifrar cualquier dato cifrado en el entorno, lo que podría incluir información confidencial. Siguiendo las prácticas recomendadas de seguridad, implemente los privilegios mínimos limitando los permisos de AWS KMS descifrado únicamente a las claves específicas que los usuarios necesitan para sus funciones laborales.

Corrección

Tome una o más de las siguientes medidas para hacer frente a esta exposición:

Implementación del acceso a los privilegios mínimos

En el resultado de exposición, abra el recurso. Se abre la ventana de política de IAM. Busque permisos en KMS que permitan kms:Decrypt o `kms:ReEncryptFrom` o `KMS:*` con una especificación de recursos de `"*"`.

Actualice la política para restringir los permisos AWS KMS de descifrado únicamente a las claves específicas necesarias. Modifique la política para reemplazar el `"*"` recurso por los ARN específicos de las claves requeridas AWS KMS .

Consideraciones para configuraciones seguras

Considere agregar condiciones para restringir aún más cuándo se pueden utilizar estos permisos. Por ejemplo, puede limitar las operaciones de descifrado a puntos de conexión de VPC específicos o a intervalos concretos de direcciones IP de origen. También puede configurar políticas de claves para restringir aún más quién puede utilizar claves específicas de KMS.

Características de acceso no utilizadas para los usuarios de IAM

Cuando un usuario de IAM tiene permisos, claves de acceso o contraseñas no utilizados, Security Hub puede incluirlos como características contextuales al determinar la exposición de ese usuario. Estas características las genera el IAM Access Analyzer, administrado por el servicio, y proporcionan un contexto adicional sobre la postura de seguridad del usuario. Las características de acceso no utilizadas no son la causa principal de la detección de la exposición, pero indican que el usuario tiene más permisos de los necesarios, lo que aumenta el impacto potencial si las credenciales del usuario se ven comprometidas.

En el caso específico de los permisos no utilizados, puedes generar una recomendación de política de privilegios mínimos que muestre una política de reemplazo con un alcance limitado. Para obtener más información, consulte the section called “Recomendaciones de políticas”.

Características de impacto para los usuarios de IAM

Los rasgos de impacto describen el radio de explosión potencial de una exposición. Security Hub analiza los permisos efectivos del usuario AWS Identity and Access Management principal asociado al usuario de IAM para determinar los recursos intermedios a los que podría acceder un atacante si el usuario de IAM se viera comprometido. Cada rasgo de impacto identifica un patrón de escalamiento de privilegios específico. Para reducir tu radio de ataque, revisa las rutas de permisos descritas en cada rasgo y elimina cualquier privilegio innecesario.

Siguiendo los principios de seguridad estándar, otorga el mínimo privilegio proporcionando solo los permisos necesarios para realizar una tarea. Sustituya las políticas generales por políticas más específicas que concedan solo las acciones y los recursos específicos que se necesitan. Para identificar los permisos no utilizados que desee eliminar, utilice IAM Access Analyzer para generar recomendaciones basadas en el historial de acceso. Para obtener más información, consulte las conclusiones sobre el acceso externo y no utilizado y sobre la aplicación de permisos con privilegios mínimos en la guía del usuario de IAM.

Tiene el control total de la ruta de ejecución privilegiada

El director asociado puede transferir una función e inyectar código en un recurso informático que ya tenga permisos elevados. Esto permite al principal obtener el control total sobre el ejecutor y realizar cualquier acción que permita la función del ejecutor.

Tiene una ruta directa de escalamiento de políticas

El director asociado puede modificar directamente las políticas de IAM para concederse permisos adicionales, aumentando así sus propios privilegios sin necesidad de recursos intermedios.

Tiene una ruta de secuestro de políticas de confianza

El director asociado puede modificar la política de confianza de una función de IAM para poder asumir esa función y obtener los permisos correspondientes.

Tiene una ruta de ransomware de datos

El director asociado puede cifrar o eliminar datos de una forma que podría utilizarse para el ransomware, por ejemplo, cifrando objetos de Amazon S3 con una AWS KMS clave gestionada por el cliente y, a continuación, modificando la política de claves.

Ha eliminado la ruta de restricción

El principal asociado puede eliminar las restricciones de seguridad, como los límites de permisos, las políticas de control de servicios o las declaraciones de denegación de políticas basadas en recursos, ampliando así lo que pueden hacer otros directores o el propio recurso.

Tiene el rol de pase, crea la ruta de ejecutor.

El principal asociado puede crear un nuevo recurso informático (como una función de Lambda o una instancia de Amazon EC2) y asignarle un rol privilegiado, lo que permite blanquear de manera efectiva sus propios permisos a través del nuevo recurso.

Tiene una ruta de ejecución existente (rol de intercambio).

El director asociado puede cambiar la función de IAM asociada a un recurso informático existente y sustituirla por una función más privilegiada para escalar el acceso.

Tiene una ruta de escalamiento de la cadena de funciones

El director asociado puede asumir una secuencia de funciones, en la que cada función de la cadena tiene permisos cada vez más amplios y, en última instancia, alcanza una función altamente privilegiada.

Tiene una ruta de ejecución privilegiada para inyectar código

El principal asociado puede inyectar código en un recurso informático en ejecución que tenga permisos elevados y ejecutar operaciones arbitrarias bajo la función privilegiada de ese recurso.

Ha deshabilitado la ruta del registro de auditoría

El director asociado puede deshabilitar los servicios de registro o supervisión, por ejemplo CloudTrail, cubrir eficazmente sus huellas durante una escalada o después de ella.

Tiene acceso a la ruta de ejecución existente

El principal asociado puede invocar un recurso informático existente o conectarse a él y usar su rol adjunto para realizar acciones privilegiadas.

Tiene una ruta de acuñación de credenciales

El director asociado puede crear nuevas credenciales a largo plazo (como claves de acceso o perfiles de inicio de sesión) para otros principales, estableciendo rutas de acceso persistentes que sobrevivan a la rotación de contraseñas o al vencimiento de la sesión.

Tiene una ruta de acceso a los datos con rol de pasante

El principal asociado puede crear un recurso de servicio y asignarle una función de acceso a datos confidenciales y obtener acceso indirecto a esos datos a través del nuevo recurso.

Ha pasado el rol, la tarea, el secuestro, la ruta

El director asociado puede transferir un rol a una tarea programada o basada en eventos (como una función de Lambda activada por un evento), lo que le permite ejecutar código arbitrario con los permisos de ese rol.

Tiene una ruta de acceso a los datos de un solo salto

El director asociado puede acceder directamente a los recursos de datos confidenciales (como los cubos de Amazon S3 o las tablas de DynamoDB) mediante sus permisos actuales, sin necesidad de pasos de escalamiento intermedios.

Tiene una ruta de avance de la capacidad

El principal asociado tiene una ruta de escalamiento de privilegios que mejora sus capacidades generales más allá de lo que sugerirían los permisos que le han sido asignados directamente. Esta es una clasificación general para las rutas que no coinciden con un patrón más específico.

Remediar las exposiciones para AWS Lambda funciones

AWS Security Hub puede generar datos de exposición para AWS Lambda las funciones.

En la consola de Security Hub, la función de Lambda involucrada en un resultado de exposición y su información de identificación aparecen en la sección Recursos de los detalles del resultado. Mediante programación, puede recuperar los detalles de los recursos con el GetFindingsV2 funcionamiento de la API CSPM de Security Hub.

Después de identificar el recurso involucrado en un resultado de exposición, puede eliminar el recurso si no lo necesita. Eliminar un recurso no esencial puede reducir su perfil de exposición y sus costos. AWS Si el recurso es esencial, siga estos pasos de remediación recomendados para ayudar a mitigar el riesgo. Los temas de remediación se dividen según el tipo de condición.

Un único resultado de exposición puede incluir problemas identificados en varios temas de remediación. También es posible abordar un resultado de exposición y disminuir su nivel de gravedad con solo tratar uno de los temas de remediación. El enfoque de remediación adecuado depende de los requisitos y cargas de trabajo de la organización.

> **Note**
>
> La guía de remediación que se proporciona en este tema puede requerir consultas adicionales en otros AWS recursos.

Contenido

- Condiciones de configuración incorrecta para funciones de Lambda
  - La función de Lambda se implementa fuera de una Amazon VPC
  - Se puede acceder a la función Lambda a través de API Gateway sin autorización
- Condiciones de accesibilidad para funciones de Lambda
  - La función de Lambda se puede invocar de forma pública
- Condiciones de vulnerabilidad para funciones de Lambda

- La función de Lambda tiene vulnerabilidades de software explotables a través de la red
- La función Lambda tiene vulnerabilidades de software
- La función Lambda contiene paquetes de software malintencionado
- La función Lambda tiene vulnerabilidades de código
- Características de impacto de las funciones de Lambda
  - Tiene el control total de la ruta de ejecución privilegiada
  - Tiene una ruta directa de escalamiento de políticas
  - Tiene una ruta de secuestro de políticas de confianza
  - Tiene una ruta de ransomware de datos
  - Ha eliminado la ruta de restricción
  - Tiene el rol de pase, crea la ruta de ejecutor.
  - Tiene una ruta de ejecución existente (rol de intercambio).
  - Tiene una ruta de escalamiento de la cadena de funciones
  - Tiene una ruta de ejecución privilegiada para inyectar código
  - Ha deshabilitado la ruta del registro de auditoría
  - Tiene acceso a la ruta de ejecución existente
  - Tiene una ruta de acuñación de credenciales
  - Tiene una ruta de acceso a los datos con rol de pasante
  - Ha pasado el rol, la tarea, el secuestro, la ruta
  - Tiene una ruta de acceso a los datos de un solo salto
  - Tiene una trayectoria de avance de la capacidad

Condiciones de configuración incorrecta para funciones de Lambda

Aquí se presentan condiciones de configuración incorrecta para funciones de Lambda y pasos de remediación sugeridos.

La función de Lambda se implementa fuera de una Amazon VPC

Las funciones de Lambda, de forma predeterminada, se implementan con acceso a Internet pública. Esta configuración predeterminada permite a las funciones de Lambda acceder a los puntos finales de AWS servicio y a las API externas, pero también las expone a posibles riesgos de seguridad. Las funciones con acceso a Internet se podrían utilizar para exfiltrar datos, comunicarse con

servidores no autorizados o convertirse en puntos de entrada para actores externos si se ven comprometidas. Amazon VPC proporciona aislamiento de red al restringir que las funciones de Lambda se comuniquen únicamente con recursos dentro de la red privada definida. Siguiendo los principios de seguridad estándar, implemente las funciones de Lambda en una VPC para mejorar la seguridad mediante el aislamiento de la red.

Solución: adjunte la función a la VPC

En la búsqueda de exposición, elija el enlace del recurso. Esto abre la función Lambda en la consola Lambda. Para proteger la función de Lambda mediante la limitación del acceso de red, asóciela a una VPC que tenga los controles de red adecuados.

Antes de conectar la función a una VPC, planifique cualquier acceso al AWS servicio que pueda necesitar, ya que las funciones de subredes privadas sin puertas de enlace NAT o puntos de enlace de la VPC no pueden acceder a las API de servicio. AWS Para obtener información sobre cómo asociar una función de Lambda a una Amazon VPC en la cuenta, consulte Asociación de funciones de Lambda a una Amazon VPC en la Cuenta de AWS. Considera la posibilidad de usar puntos de enlace de la VPC para la conectividad de los servicios sin acceso a Internet si tu función requiere acceder a los servicios desde una subred privada. AWS Configure una puerta de enlace de NAT si necesita conectividad de salida a Internet desde subredes privadas.

Se puede acceder a la función Lambda a través de API Gateway sin autorización

Los métodos de API Gateway sin autorización permiten a cualquier persona que llame con acceso a la API Gateway invocar la función Lambda integrada sin verificar su identidad. Esta configuración crea riesgos de seguridad, ya que las personas que llaman pueden invocar la función Lambda sin la autorización adecuada, lo que puede provocar un uso indebido de las capacidades de la función, el consumo de recursos, el acceso a datos confidenciales u operaciones no autorizadas. Si bien API Gateway puede tener controles de acceso a nivel de red, la falta de autorización a nivel de método podría permitir la invocación gratuita de la función por parte de cualquier persona que llame con acceso de red a API Gateway. Siguiendo las prácticas recomendadas de seguridad, implemente los mecanismos de autorización adecuados para los métodos de API Gateway que se integran con las funciones de Lambda.

Solución: configurar la autenticación de API Gateway

En la pestaña Recursos de la exposición, elija el enlace del recurso para acceder al método API Gateway. Revise la configuración de autorización actual e implemente los mecanismos de autenticación adecuados.

API Gateway admite varias opciones de autenticación, como AWS IAM, los grupos de usuarios de Amazon Cognito, los autorizadores de Lambda y las claves de API. Elija el método de autenticación que mejor se adapte a sus requisitos de seguridad y a su caso de uso. Para obtener instrucciones detalladas sobre la configuración de la autenticación, consulte Controlar y administrar el acceso a una API REST en API Gateway en la Guía para desarrolladores de API Gateway.

Condiciones de accesibilidad para funciones de Lambda

A continuación se describen las condiciones de accesibilidad para funciones de Lambda y los pasos de remediación recomendados.

La función de Lambda se puede invocar de forma pública

Las políticas basadas en recursos de Lambda determinan quién puede invocar las funciones. Una función con una política de recursos que incluya «*» como principal (o ningún principal) permite que cualquier AWS usuario autenticado la invoque. Esta configuración supone un riesgo considerable, especialmente para funciones que procesan información confidencial, modifican recursos o tienen permisos elevados. Los usuarios no autorizados podrían aprovechar esta configuración para realizar operaciones no deseadas, exponer datos, manipular recursos o abusar de las capacidades de la función. Siguiendo las prácticas recomendadas de seguridad, restrinja el acceso a las funciones de Lambda solo a las entidades principales autorizadas.

Solución: modifique la política basada en los recursos de la función

En la pestaña Recursos del resultado de exposición, abra el recurso mediante el hipervínculo. Esto abre la función Lambda en la consola Lambda. Restrinja el acceso a su función de Lambda especificando solo los ID de AWS cuenta autorizados o los principales de IAM específicos (usuarios, funciones o servicios) en la política basada en recursos. Solo puede modificar políticas basadas en recursos mediante programación.

Condiciones de vulnerabilidad para funciones de Lambda

A continuación se presentan las condiciones de vulnerabilidad para funciones de Lambda y los pasos de remediación sugeridos.

La función de Lambda tiene vulnerabilidades de software explotables a través de la red

Los paquetes de software utilizados en el código de la función de Lambda pueden contener vulnerabilidades y exposiciones Comunes (CVE) con una alta probabilidad de explotación. Los CVE críticos representan importantes riesgos de seguridad para su entorno. AWS Los atacantes pueden

aprovechar las vulnerabilidades no parcheadas y poner en riesgo la confidencialidad, integridad o disponibilidad de los datos, así como acceder a otros sistemas. Las vulnerabilidades críticas con alta probabilidad de explotación representan amenazas de seguridad inmediatas, ya que el código de explotación puede estar disponible públicamente y ser utilizado activamente por atacantes o por herramientas automatizadas de detección. Siguiendo las prácticas recomendadas de seguridad, corrija estas vulnerabilidades para proteger su función de los ataques.

Solución: actualice las funciones afectadas

Revise la sección Referencias en la pestaña Vulnerabilidad correspondiente a esa condición. La documentación del proveedor puede incluir una guía de corrección específica. Actualice las bibliotecas vulnerables a sus versiones seguras más recientes según los procedimientos recomendados por el proveedor.

Normalmente, el flujo de trabajo de remediación depende de si implementó el paquete de Lambda mediante la carga de un archivo ZIP o la creación de una función de Lambda con una imagen de contenedor. Después de actualizar las bibliotecas, actualice el código de la función de Lambda para usar la versión corregida. Luego implemente la versión actualizada.

La función Lambda tiene vulnerabilidades de software

Las funciones de Lambda suelen utilizar bibliotecas y dependencias de terceros que pueden contener vulnerabilidades de seguridad con una gravedad o capacidad de explotación menor en comparación con los CVE críticos. Si bien es posible que estas vulnerabilidades no críticas no se puedan explotar de inmediato, aún constituyen debilidades de seguridad que se podrían combinar con otras vulnerabilidades y poner en riesgo la función. Con el tiempo, pueden aparecer nuevas técnicas de explotación que aumenten el riesgo asociado a estas vulnerabilidades. Siguiendo los principios de seguridad estándar, corrija estas vulnerabilidades para mantener un entorno seguro.

Solución: actualice las funciones afectadas

Revise la sección Referencias en la pestaña Vulnerabilidad correspondiente a esa condición. La documentación del proveedor puede incluir una guía de corrección específica. Actualice las bibliotecas vulnerables a sus versiones seguras más recientes según los procedimientos recomendados por el proveedor.

Normalmente, el flujo de trabajo de remediación depende de si implementó el paquete de Lambda mediante la carga de un archivo ZIP o la creación de una función de Lambda con una imagen de contenedor. Después de actualizar las bibliotecas, actualice el código de la función de Lambda para usar la versión corregida. Luego implemente la versión actualizada.

La función Lambda contiene paquetes de software malintencionado

Los paquetes malintencionados son componentes de software que contienen código dañino diseñado para comprometer la confidencialidad, la integridad y la disponibilidad de sus sistemas y datos. Los paquetes malintencionados representan una amenaza activa y crítica para su función de Lambda, ya que los atacantes pueden ejecutar código malintencionado automáticamente sin aprovechar una vulnerabilidad. Siga las prácticas recomendadas de seguridad y elimine los paquetes malintencionados para proteger su función Lambda de posibles ataques.

Solución: elimine los paquetes malintencionados

Revise los detalles del paquete malicioso en la sección Referencias de la pestaña Vulnerabilidad de la característica para comprender la amenaza. Elimine los paquetes maliciosos identificados del código de función y las dependencias. En el caso de las funciones que utilizan capas, compruebe si los paquetes malintencionados están instalados en alguna capa y elimínelos.

Actualice el paquete de implementación o la imagen del contenedor para excluir los paquetes malintencionados y, a continuación, implemente la versión actualizada. Para obtener instrucciones, consulte Implementar funciones de Lambda como archivos.zip para archivos.zip o Crear una función de Lambda con una imagen de contenedor para imágenes de contenedor.

La función Lambda tiene vulnerabilidades de código

El código de aplicación de la función Lambda contiene vulnerabilidades de seguridad que los actores de amenazas podrían aprovechar. Entre las vulnerabilidades del código se incluyen las filtraciones de datos, los fallos de inyección, la falta de cifrado y la criptografía débil, que se identifican mediante el análisis automatizado del código. Estas vulnerabilidades plantean riesgos de seguridad para su AWS entorno, ya que los atacantes pueden explotarlas para comprometer la confidencialidad, la integridad o la disponibilidad de los datos, o para acceder a otros sistemas. Las vulnerabilidades del código representan debilidades de seguridad que podrían combinarse con otros vectores de ataque para comprometer su funcionamiento. Siguiendo las prácticas recomendadas de seguridad, aborde estas vulnerabilidades de código para proteger su función de los ataques.

Solución: actualice las funciones afectadas

Consulte la sección Referencias en la pestaña Vulnerabilidad de la condición. Las conclusiones de Amazon Inspector pueden incluir directrices de corrección específicas y fragmentos de código que muestren las ubicaciones de código vulnerables. Solucione los problemas de seguridad identificados en el código de su función utilizando los bloques de código listos para usar proporcionados o implementando prácticas de codificación seguras.

Revisa siempre las sugerencias para corregir el código antes de adoptarlas, ya que es posible que tengas que editarlas para asegurarte de que el código funciona según lo previsto. Tras corregir las vulnerabilidades, actualiza el código de la función de Lambda para usar la versión corregida. Para obtener instrucciones, consulte Actualización del código de función en la Guía para AWS Lambda desarrolladores.

Luego implemente la versión actualizada. Para obtener instrucciones, consulte Implementar funciones de Lambda como archivos.zip para archivos.zip o Crear una función de Lambda con una imagen de contenedor para imágenes de contenedor. Para obtener más información sobre el escaneo de código de Amazon Inspector, consulte el escaneo de código Lambda de Amazon Inspector en la guía del usuario de Amazon Inspector.

Características de impacto de las funciones de Lambda

Los rasgos de impacto describen el radio de explosión potencial de una exposición. Security Hub analiza los permisos efectivos del AWS Identity and Access Management principal asociado a la función Lambda para determinar los recursos posteriores a los que podría acceder un atacante si la función se viera comprometida. Cada rasgo de impacto identifica un patrón de escalamiento de privilegios específico. Para reducir tu radio de ataque, revisa las rutas de permisos descritas en cada rasgo y elimina cualquier privilegio innecesario.

Siguiendo los principios de seguridad estándar, otorga el mínimo privilegio proporcionando solo los permisos necesarios para realizar una tarea. Sustituya las políticas generales por políticas más específicas que concedan solo las acciones y los recursos específicos que se necesitan. Para identificar los permisos no utilizados que desee eliminar, utilice IAM Access Analyzer para generar recomendaciones basadas en el historial de acceso. Para obtener más información, consulte las conclusiones sobre el acceso externo y no utilizado y sobre la aplicación de permisos con privilegios mínimos en la guía del usuario de IAM.

Tiene el control total de la ruta de ejecución privilegiada

El director asociado puede transferir una función e inyectar código en un recurso informático que ya tenga permisos elevados. Esto permite al principal obtener el control total sobre el ejecutor y realizar cualquier acción que permita la función del ejecutor.

Tiene una ruta directa de escalamiento de políticas

El director asociado puede modificar directamente las políticas de IAM para concederse permisos adicionales, aumentando así sus propios privilegios sin necesidad de recursos intermedios.

Tiene una ruta de secuestro de políticas de confianza

El director asociado puede modificar la política de confianza de una función de IAM para poder asumir esa función y obtener los permisos correspondientes.

Tiene una ruta de ransomware de datos

El director asociado puede cifrar o eliminar datos de una forma que podría utilizarse para el ransomware, por ejemplo, cifrando objetos de Amazon S3 con una AWS KMS clave gestionada por el cliente y, a continuación, modificando la política de claves.

Ha eliminado la ruta de restricción

El principal asociado puede eliminar las restricciones de seguridad, como los límites de permisos, las políticas de control de servicios o las declaraciones de denegación de políticas basadas en recursos, ampliando así lo que pueden hacer otros directores o el propio recurso.

Tiene el rol de pase, crea la ruta de ejecutor.

El principal asociado puede crear un nuevo recurso informático (como una función de Lambda o una instancia de Amazon EC2) y asignarle un rol privilegiado, lo que permite blanquear de manera efectiva sus propios permisos a través del nuevo recurso.

Tiene una ruta de ejecución existente (rol de intercambio).

El director asociado puede cambiar la función de IAM asociada a un recurso informático existente y sustituirla por una función más privilegiada para escalar el acceso.

Tiene una ruta de escalamiento de la cadena de funciones

El director asociado puede asumir una secuencia de funciones, en la que cada función de la cadena tiene permisos cada vez más amplios y, en última instancia, alcanza una función altamente privilegiada.

Tiene una ruta de ejecución privilegiada para inyectar código

El principal asociado puede inyectar código en un recurso informático en ejecución que tenga permisos elevados y ejecutar operaciones arbitrarias bajo la función privilegiada de ese recurso.

Ha deshabilitado la ruta del registro de auditoría

El director asociado puede deshabilitar los servicios de registro o supervisión, por ejemplo CloudTrail, cubrir eficazmente sus huellas durante una escalada o después de ella.

Tiene acceso a la ruta de ejecución existente

El principal asociado puede invocar un recurso informático existente o conectarse a él y usar su rol adjunto para realizar acciones privilegiadas.

Tiene una ruta de acuñación de credenciales

El director asociado puede crear nuevas credenciales a largo plazo (como claves de acceso o perfiles de inicio de sesión) para otros principales, estableciendo rutas de acceso persistentes que sobrevivan a la rotación de contraseñas o al vencimiento de la sesión.

Tiene una ruta de acceso a los datos con rol de pasante

El principal asociado puede crear un recurso de servicio y asignarle una función de acceso a datos confidenciales y obtener acceso indirecto a esos datos a través del nuevo recurso.

Ha pasado el rol, la tarea, el secuestro, la ruta

El director asociado puede transferir un rol a una tarea programada o basada en eventos (como una función de Lambda activada por un evento), lo que le permite ejecutar código arbitrario con los permisos de ese rol.

Tiene una ruta de acceso a los datos de un solo salto

El director asociado puede acceder directamente a los recursos de datos confidenciales (como los cubos de Amazon S3 o las tablas de DynamoDB) mediante sus permisos actuales, sin necesidad de pasos de escalamiento intermedios.

Tiene una trayectoria de avance de la capacidad

El principal asociado tiene una ruta de escalamiento de privilegios que mejora sus capacidades generales más allá de lo que sugerirían los permisos que le han sido asignados directamente. Esta es una clasificación general para las rutas que no coinciden con un patrón más específico.

Cómo corregir las exposiciones de las instancias y clústeres de Amazon RDS

AWS Security Hub puede generar hallazgos de exposición para instancias y clústeres de Amazon RDS.

En la consola de Security Hub, la instancia o el clúster de Amazon RDS involucrados en la búsqueda de exposición y su información de identificación aparecen en la sección Recursos de los detalles de

la búsqueda. Puede recuperar los detalles de los recursos mediante programación utilizando la API GetFindingsV2 CSPM de Security Hub.

Después de identificar el recurso involucrado en un resultado de exposición, puede eliminar el recurso si no lo necesita. Eliminar un recurso no esencial puede reducir su perfil de exposición y sus costos. AWS Si el recurso es esencial, siga estos pasos de remediación recomendados para ayudar a mitigar el riesgo. Los temas de remediación se dividen según el tipo de condición.

Un único resultado de exposición puede incluir problemas identificados en varios temas de remediación. También es posible abordar un resultado de exposición y disminuir su nivel de gravedad con solo tratar uno de los temas de remediación. El enfoque de remediación adecuado depende de los requisitos y cargas de trabajo de la organización.

> **Note**
>
> La guía de remediación que se proporciona en este tema puede requerir consultas adicionales en otros AWS recursos.

Contenido

- Características de configuración incorrecta de las instancias y los clústeres de Amazon RDS
  - La instancia de base de datos de Amazon RDS está configurada con acceso público
  - El clúster de base de datos de Amazon RDS tiene una instantánea que se comparte públicamente
  - La instancia de base de datos de Amazon RDS tiene una instantánea que se comparte públicamente
  - La instancia de base de datos de Amazon RDS tiene una instantánea que no está cifrada en reposo
  - El clúster de base de datos de Amazon RDS tiene una instantánea que no está cifrada en reposo
  - La instancia de base de datos de Amazon RDS tiene un grupo de seguridad abierto
  - La instancia de base de datos de Amazon RDS tiene desactivada la autenticación de base de datos mediante IAM
  - La instancia de base de datos de Amazon RDS utiliza el nombre de usuario administrativo predeterminado

- El clúster de base de datos de Amazon RDS utiliza el nombre de usuario de administrador predeterminado
- La instancia de base de datos de Amazon RDS tiene desactivadas las actualizaciones automáticas de versiones secundarias.
- La instancia de base de datos de Amazon RDS tiene desactivadas las copias de seguridad automáticas
- La instancia de base de datos de Amazon RDS tiene desactivada la protección contra eliminación
- El clúster de base de datos de Amazon RDS tiene desactivada la protección contra eliminación
- La instancia de base de datos de Amazon RDS utiliza el puerto predeterminado para el motor de base de datos
- La instancia de base de datos de Amazon RDS no está cubierta por un plan de copia de seguridad
- Características de los datos confidenciales de las instancias de base de datos de Amazon RDS
  - La instancia de base de datos de Amazon RDS contiene datos confidenciales

Características de configuración incorrecta de las instancias y los clústeres de Amazon RDS

A continuación se describen las características de configuración incorrecta y los pasos de corrección para las instancias y los clústeres de Amazon RDS.

La instancia de base de datos de Amazon RDS está configurada con acceso público

Las instancias de Amazon RDS con acceso público pueden quedar potencialmente expuestas a través de internet mediante sus puntos de conexión. Aunque el acceso público a veces es necesario para la funcionalidad de la instancia, esta configuración puede servir como un vector de ataque para que usuarios no autorizados intenten acceder a la base de datos. Las bases de datos a las que se puede acceder públicamente pueden quedar expuestas a detecciones de puertos, ataques de fuerza bruta y otros intentos de explotación. Siguiendo los principios de seguridad estándar, limite la exposición pública de los recursos de su base de datos.

Solución: modifique la configuración de acceso público

En el hallazgo de exposición, elija el enlace del recurso. Esto abre la instancia de base de datos afectada en la consola de Amazon RDS. Evalúe si la instancia de base de datos necesita acceso público según la arquitectura de la aplicación. Para obtener más información, consulte Configuración del acceso público o privado en Amazon RDS.

El clúster de base de datos de Amazon RDS tiene una instantánea que se comparte públicamente

Cualquier persona puede acceder a las instantáneas públicas Cuenta de AWS, lo que podría exponer los datos confidenciales a usuarios no autorizados. Cualquier persona Cuenta de AWS tiene permiso para copiar estas instantáneas públicas y crear instancias de base de datos a partir de ellas, lo que podría provocar filtraciones de datos o un acceso no autorizado a los datos. Siguiendo las prácticas recomendadas de seguridad, restrinja el acceso a sus instantáneas de Amazon RDS únicamente a organizaciones de confianza Cuentas de AWS .

Solución: configure una instantánea de Amazon RDS para un acceso privado

En el resultado de exposición, abra el recurso mediante el hipervínculo. Para obtener información sobre cómo modificar la configuración de uso compartido de instantáneas, consulte Compartir una instantánea en la Guía del usuario de Amazon Aurora. Para obtener información sobre cómo dejar de compartir instantáneas, consulte Cómo detener el uso compartido de instantáneas en la Guía del usuario de Amazon Aurora.

La instancia de base de datos de Amazon RDS tiene una instantánea que se comparte públicamente

Cualquier persona puede acceder a las instantáneas públicas Cuenta de AWS, lo que podría exponer los datos confidenciales a usuarios no autorizados. Cualquier persona Cuenta de AWS tiene permiso para copiar estas instantáneas públicas y crear instancias de base de datos a partir de ellas, lo que podría provocar filtraciones de datos o un acceso no autorizado a los datos. Siguiendo las prácticas recomendadas de seguridad, restrinja el acceso a sus instantáneas de Amazon RDS únicamente a organizaciones de confianza Cuentas de AWS .

Solución: configure una instantánea de Amazon RDS para un acceso privado

En el resultado de exposición, abra el recurso mediante el hipervínculo. Para obtener información sobre cómo modificar la configuración de uso compartido de instantáneas, consulte Compartir una instantánea de base de datos en la guía del usuario de Amazon RDS. Para obtener información sobre cómo dejar de compartir instantáneas, consulte Dejar de compartir una instantánea de base de datos en la Guía del usuario de Amazon RDS. .

La instancia de base de datos de Amazon RDS tiene una instantánea que no está cifrada en reposo

Las instantáneas no cifradas de instancias de base de datos de Amazon RDS pueden exponer información confidencial si un usuario no autorizado obtiene acceso a la capa de almacenamiento. Sin cifrado, los datos en las instantáneas podrían quedar expuestos por accesos no autorizados.

Esto genera un riesgo de filtración de datos y de incumplimientos normativos. Siguiendo las mejores prácticas de seguridad, cifre todos los recursos de la base de datos y sus copias de seguridad para mantener la confidencialidad de los datos.

Solución: actualice los recursos afectados

En el hallazgo de exposición, elija el enlace del recurso. Esto abre la instantánea afectada en la consola de Amazon RDS. No puede cifrar directamente una instantánea existente que no esté cifrada.

En su lugar, cree una copia cifrada de la instantánea sin cifrar. Para obtener instrucciones detalladas, consulte Cómo copiar y cifrar los recursos de Amazon RDS de instantáneas de clústeres de bases de datos en la Guía del usuario de Amazon Aurora.

El clúster de base de datos de Amazon RDS tiene una instantánea que no está cifrada en reposo

Las instantáneas no cifradas de clústeres de base de datos de Amazon RDS pueden exponer información confidencial si un usuario no autorizado obtiene acceso a la capa de almacenamiento. Sin cifrado, los datos en las instantáneas podrían quedar expuestos por accesos no autorizados. Esto genera un riesgo de filtración de datos y de incumplimientos normativos. Siguiendo las prácticas recomendadas de seguridad, cifre todos los recursos de la base de datos y sus copias de seguridad para mantener la confidencialidad de los datos.

Solución: cree una copia cifrada de la instantánea

En la búsqueda de exposición, elija el enlace del recurso. Esto abre la instantánea afectada en la consola de Amazon RDS. No puede cifrar directamente una instantánea existente que no esté cifrada.

En su lugar, cree una copia cifrada de la instantánea sin cifrar. Para obtener instrucciones detalladas, consulte Cómo copiar y cifrar los recursos de Amazon RDS de instantáneas de clústeres de bases de datos en la Guía del usuario de Amazon Aurora.

La instancia de base de datos de Amazon RDS tiene un grupo de seguridad abierto

Los grupos de seguridad funcionan como firewalls virtuales para que las instancias de Amazon RDS controlen el tráfico entrante y saliente. Los grupos de seguridad abiertos, que permiten acceso sin restricciones desde cualquier dirección IP, pueden exponer las instancias de base de datos a accesos no autorizados y posibles ataques. Siguiendo los principios de seguridad estándar, restrinja

el acceso de los grupos de seguridad a direcciones IP y puertos específicos para mantener el principio de privilegio mínimo.

Corrección

Tome una o más de las siguientes medidas para hacer frente a esta exposición:

Revisión de las reglas del grupo de seguridad y evaluación de la configuración actual

En el resultado de exposición, abra el recurso correspondiente al grupo de seguridad de la instancia de base de datos. Evalúe qué puertos están abiertos y accesibles desde rangos amplios de direcciones IP, como `(0.0.0.0/0 or ::/0)`. Para obtener información sobre la visualización de los detalles del grupo de seguridad, consulte DescribeSecurityGroups la referencia de la API de Amazon Elastic Compute Cloud.

Modificación de reglas del grupo de seguridad

Modifique las reglas del grupo de seguridad para restringir el acceso únicamente a direcciones IP o rangos específicos y de confianza. Al actualizar las reglas del grupo de seguridad, considere separar los requisitos de acceso para distintos segmentos de red mediante la creación de reglas para cada rango de IP de origen requerido o la restricción del acceso únicamente a puertos específicos. Para modificar las reglas del grupo de seguridad, consulte Configuración de reglas de grupos de seguridad en la Guía del usuario de Amazon EC2. Para modificar el puerto predeterminado de una instancia de base de datos de Amazon RDS existente, consulte Cómo modificar el clúster de base de datos mediante la consola, la CLI y la API en la Guía del usuario de Amazon Aurora.

La instancia de base de datos de Amazon RDS tiene desactivada la autenticación de base de datos mediante IAM

La autenticación de base de datos mediante IAM permite autenticarse en la base de datos de Amazon RDS mediante credenciales de IAM en lugar de contraseñas de base de datos. Esto aporta varias ventajas de seguridad, como la administración centralizada de accesos, el uso de credenciales temporales y la posibilidad de evitar almacenar contraseñas de base de datos en el código de la aplicación. La autenticación de bases de datos de IAM permite autenticar las instancias de bases de datos con un token de autenticación en lugar de una contraseña. Como resultado, el tráfico de red hacia la instancia de base de datos y desde esta se cifra mediante SSL. Sin autenticación de IAM, las bases de datos suelen depender de autenticación basada en contraseñas, lo que puede derivar en la reutilización de contraseñas y contraseñas débiles. Siga las prácticas recomendadas de seguridad y habilite la autenticación de bases de datos de IAM.

Solución: habilite la autenticación de la base de datos de IAM

En la búsqueda de exposición, elija el enlace del recurso. Esto abre la instancia de base de datos afectada en la consola de Amazon RDS. Puede habilitar la autenticación de base de datos con IAM en las opciones de Base de datos.

Para obtener más información, consulte Habilitación y desactivación de la autenticación de base de datos con IAM en la Guía del usuario de Amazon RDS. Después de habilitar la autenticación con IAM, actualice las instancias de base de datos para que utilicen autenticación mediante IAM en lugar de autenticación basada en contraseñas.

La instancia de base de datos de Amazon RDS utiliza el nombre de usuario administrativo predeterminado

El uso de nombres de usuario predeterminados (por ejemplo, «admin» o «root») para las instancias de base de datos aumenta el riesgo de seguridad, ya que son ampliamente conocidos y suelen ser blanco de ataques de fuerza bruta. Los nombres de usuario predeterminados facilitan los esfuerzos de usuarios no autorizados por acceder a la base de datos. Cuando se usan nombres de usuario predeterminados, los atacantes únicamente necesitan obtener las contraseñas, en lugar de necesitar ambas piezas (nombre de usuario y contraseña) para acceder a la base de datos. Siguiendo las prácticas recomendadas de seguridad, utilice nombres de usuario de administrador únicos para la instancia de base de datos a fin de mejorar la seguridad en la oscuridad y reducir el riesgo de intentos de acceso no autorizado.

Solución: configure un nombre de usuario de administrador único

En la búsqueda de exposición, elija el enlace del recurso. Esto abre la instancia de base de datos afectada en la consola de Amazon RDS. No puede cambiar el nombre de usuario de administrador de una instancia de base de datos de Amazon RDS existente. Para crear un nombre de administrador único, debe crear una nueva instancia de base de datos con un nombre personalizado y migrar los datos.

El clúster de base de datos de Amazon RDS utiliza el nombre de usuario de administrador predeterminado

El uso de nombres de usuario predeterminados (por ejemplo, «admin» o «root») para las instancias de base de datos aumenta el riesgo de seguridad, ya que son ampliamente conocidos y suelen ser blanco de ataques de fuerza bruta. Los nombres de usuario predeterminados facilitan los esfuerzos de usuarios no autorizados por acceder a la base de datos. Cuando se usan nombres de usuario predeterminados, los atacantes únicamente necesitan obtener las contraseñas, en lugar de necesitar ambas piezas (nombre de usuario y contraseña) para acceder a la base de datos. Siguiendo las prácticas recomendadas de seguridad, utilice nombres de usuario de administrador únicos para

la instancia de base de datos a fin de mejorar la seguridad en la oscuridad y reducir el riesgo de intentos de acceso no autorizado.

Solución: configure un nombre de usuario de administrador único

En la búsqueda de exposición, elija el enlace del recurso. Esto abre la instancia de base de datos afectada en la consola de Amazon RDS. No puede cambiar el nombre de usuario de administrador de una instancia de base de datos de Amazon RDS existente. Para crear un nombre de administrador único, debe crear una nueva instancia de base de datos con un nombre personalizado y migrar los datos.

La instancia de base de datos de Amazon RDS tiene desactivadas las actualizaciones automáticas de versiones secundarias.

Las actualizaciones automáticas de versiones secundarias garantizan que las instancias de Amazon RDS reciban automáticamente las nuevas versiones secundarias del motor de base de datos en cuanto estén disponibles. Estas actualizaciones suelen incluir parches de seguridad importantes y correcciones de errores que ayudan a mantener la seguridad y la estabilidad de la base de datos. La base de datos corre el riesgo de operar con vulnerabilidades de seguridad conocidas que ya han sido corregidas en versiones secundarias más recientes. Sin actualizaciones automáticas, las instancias de base de datos pueden acumular vulnerabilidades de seguridad a medida que se descubren nuevos CVE. Siguiendo las prácticas recomendadas de seguridad, habilite las actualizaciones automáticas de versiones secundarias para todas las instancias de Amazon RDS.

Solución: habilite las actualizaciones automáticas de versiones secundarias

En la búsqueda de exposición, elija el enlace del recurso. Esto abre la instancia de base de datos afectada en la consola de Amazon RDS. Puede ver la configuración de actualizaciones secundarias automáticas en la pestaña Mantenimiento y copias de seguridad.

Para obtener más información, consulte Actualizaciones automáticas de versiones secundarias de Amazon RDS para MySQL. También puede configurar su período de mantenimiento para que se produzca durante los períodos de baja actividad de la base de datos.

La instancia de base de datos de Amazon RDS tiene desactivadas las copias de seguridad automáticas

Las copias de seguridad automáticas permiten realizar una recuperación a un momento específico para las instancias de Amazon RDS, con lo cual es posible restaurar la base de datos a cualquier punto dentro del periodo de retención. Cuando las copias de seguridad automáticas están

desactivadas, se corre el riesgo de perder datos en caso de eliminación maliciosa, corrupción de datos u otros escenarios de pérdida de datos. En situaciones de actividad maliciosa, como ataques de ransomware, eliminación de tablas o corrupción de datos, la capacidad de restaurar a un punto en el tiempo previo al incidente reduce lo que tarda en recuperarse. Siguiendo las prácticas recomendadas de seguridad, habilite las copias de seguridad automatizadas con un período de retención adecuado para todas las bases de datos de producción.

La instancia de base de datos de Amazon RDS tiene desactivada la protección contra eliminación

La protección contra eliminación es una característica que ayuda a evitar que las instancias de base de datos se eliminen de manera no intencional o maliciosa. Cuando la protección contra eliminación está desactivada, la base de datos puede ser eliminada por cualquier usuario con los permisos suficientes, lo que puede derivar en pérdida de datos o tiempo de inactividad en la aplicación. Los atacantes pueden eliminar la base de datos, lo que provocaría interrupciones del servicio, pérdida de datos y tiempos de recuperación más prolongados. Siguiendo las prácticas recomendadas de seguridad, habilite la protección contra la eliminación de sus instancias de base de datos de RDS para evitar la eliminación malintencionada.

Solución: habilite la protección contra eliminaciones para su clúster de base de datos de Amazon RDS

En la búsqueda de exposición, elija el enlace del recurso. Esto abre el clúster de base de datos afectado.

El clúster de base de datos de Amazon RDS tiene desactivada la protección contra eliminación

La protección contra eliminación es una característica que ayuda a evitar que las instancias de base de datos se eliminen de manera no intencional o maliciosa. Cuando la protección contra eliminación está desactivada, la base de datos puede ser eliminada por cualquier usuario con los permisos suficientes, lo que puede derivar en pérdida de datos o tiempo de inactividad en la aplicación. Los atacantes pueden eliminar la base de datos, lo que provocaría interrupciones del servicio, pérdida de datos y tiempos de recuperación más prolongados. Siguiendo las prácticas recomendadas de seguridad, habilite la protección contra la eliminación de los clústeres de bases de datos de RDS para evitar la eliminación malintencionada.

Solución: habilite la protección contra eliminaciones para su clúster de base de datos de Amazon RDS

En la búsqueda de exposición, elija el enlace del recurso. Esto abre el clúster de base de datos afectado.

La instancia de base de datos de Amazon RDS utiliza el puerto predeterminado para el motor de base de datos

Las instancias de Amazon RDS que utilizan puertos predeterminados para los motores de base de datos pueden enfrentar riesgos de seguridad más elevados, ya que estos puertos predeterminados son ampliamente conocidos y suelen ser objetivo de herramientas de detección automatizada. Modificar la instancia de base de datos para que utilice puertos no predeterminados agrega una capa adicional de seguridad, ya que dificulta que usuarios no autorizados realicen ataques automatizados o dirigidos contra la base de datos. Los puertos predeterminados suelen ser analizados con frecuencia por actores no autorizados, lo que puede convertir la instancia de base de datos en un objetivo. Siguiendo las prácticas recomendadas de seguridad, cambie el puerto predeterminado por un puerto personalizado para reducir el riesgo de ataques automatizados o dirigidos.

Corrección

Tome una o más de las siguientes medidas para hacer frente a esta exposición:

Actualice los recursos afectados

En la búsqueda de exposición, elija el enlace del recurso. Esto abre la instancia de base de datos afectada en la consola de Amazon RDS.

Actualización de las cadenas de conexión de las aplicaciones

Después de cambiar el puerto, actualice todas las aplicaciones y servicios que se conectan a la instancia de Amazon RDS de modo que utilicen el nuevo número de puerto.

La instancia de base de datos de Amazon RDS no está cubierta por un plan de copia de seguridad

AWS Backup es un servicio de copia de seguridad totalmente gestionado que centraliza y automatiza la copia de seguridad de los datos en todas partes. Servicios de AWS Si la instancia de base de datos no está cubierta por un plan de copia de seguridad, corre el riesgo de perder datos en caso de eliminación maliciosa, corrupción de datos u otros escenarios de pérdida de datos. En situaciones de actividad maliciosa, como ataques de ransomware, eliminación de tablas o corrupción de datos, la capacidad de restaurar a un punto en el tiempo previo al incidente reduce lo que tarda en recuperarse. Siguiendo las prácticas recomendadas de seguridad, incluya sus instancias de Amazon RDS en un plan de respaldo para garantizar la protección de los datos.

Solución: cree y asigne un plan de respaldo para su instancia de base de datos

En la búsqueda de exposición, elija el enlace del recurso. Esto abre la instancia de base de datos afectada en la consola de Amazon RDS. Considere cuál frecuencia de copias de seguridad, periodo de retención y reglas de ciclo de vida son las más adecuadas para las aplicaciones.

Características de los datos confidenciales de las instancias de base de datos de Amazon RDS

Estas son las características de los datos confidenciales de las instancias de base de datos de Amazon RDS y las medidas de corrección sugeridas.

La instancia de base de datos de Amazon RDS contiene datos confidenciales

Un análisis de seguridad de los datos ha confirmado que hay registros confidenciales en la instancia de base de datos de Amazon RDS. Un producto de seguridad de datos integrado establece esta característica cuando inspecciona el contenido de la instancia de base de datos e identifica los registros que requieren protección.

La presencia de datos confidenciales aumenta el impacto de cualquier otra debilidad en la misma instancia de base de datos. Una ruta de red o una configuración de acceso permisiva que, de otro modo, expondría los datos de la aplicación, expone los registros regulados o confidenciales. Un agente de amenazas que acceda a la instancia de base de datos puede consultar y copiar esos registros de forma masiva y conservarlos fuera de su entorno. El autor de la amenaza también puede usar cualquier credencial recuperada para autenticarse en otros sistemas. Siguiendo las prácticas recomendadas de seguridad, recomendamos restringir el acceso a la red y a la identidad a las instancias de base de datos de Amazon RDS que almacenan registros confidenciales y cifrar esos registros en reposo y en tránsito.

La información confidencial puede incluir:

- Credenciales, como contraseñas, claves de acceso y cadenas de conexión
- Información de identificación personal
- Información financiera, como números de cuenta y datos de tarjetas de pago
- Contenido confidencial que requiere protección

Eliminar los registros confidenciales es la única forma de eliminar este rasgo. Si su carga de trabajo requiere que la instancia de base de datos almacene datos confidenciales, las siguientes prácticas recomendadas de seguridad reducen el riesgo de exposición.

Revise los datos confidenciales de la instancia de base de datos

En el resultado de exposición, abra el recurso mediante el hipervínculo. Esto abre la instancia de base de datos afectada. Anote el identificador de la instancia de base de datos y registre los grupos de seguridad de VPC que figuran en Conectividad y seguridad. Revise el resultado de seguridad de los datos que registró los registros confidenciales para determinar qué bases de datos, esquemas y tablas los contienen.

Según el tipo de información confidencial identificada, implemente los controles de seguridad apropiados:

- Restrinja el acceso a la red entrante: en la consola de Amazon RDS, elija Bases de datos, seleccione la instancia de base de datos y elija Conectividad y seguridad. Abra cada grupo de seguridad de VPC adjunto y revise sus reglas de entrada. Sustituya cualquier regla que permita la portabilidad de la base de datos desde `0.0.0.0/0` o `::/0` por los rangos de CIDR o los identificadores de grupos de seguridad específicos que utilizan sus aplicaciones. Para obtener más información, consulte Control de acceso con grupos de seguridad en la Guía del usuario de Amazon RDS.
- Elimine la accesibilidad pública: en la consola de Amazon RDS, seleccione la instancia de base de datos, elija Modificar y, en Conectividad, defina el acceso público como No accesible públicamente. Coloque la instancia de base de datos en subredes privadas que no tengan una ruta a una puerta de enlace a Internet. Acceda a él desde sus aplicaciones a través de la VPC, AWS Direct Connect o una conexión VPN. Para obtener más información, consulte Working with a DB instance in a VPC (Uso de una instancia de base de datos en una VPC) en la Guía del usuario de Amazon RDS.
- Limite quién puede autenticarse en la base de datos: conceda a cada aplicación y usuario solo los privilegios de base de datos necesarios para su funcionamiento. Revoca el acceso de lectura a las tablas que contienen registros confidenciales a cualquier usuario de la base de datos que no lo necesite. Utilice la autenticación de bases de datos de IAM para que las identidades de IAM y los tokens de corta duración controlen el acceso en lugar de las contraseñas de larga duración de las bases de datos. Para obtener más información, consulte la autenticación de bases de datos de IAM en la Guía del usuario de Amazon RDS.
- Cifre los registros confidenciales en reposo: en la consola de Amazon RDS, seleccione la instancia de base de datos y elija la pestaña Configuración para comprobar si la instancia de base de datos utiliza el cifrado. No puede habilitar el cifrado en reposo en una instancia de base de datos no cifrada existente. Para cifrar sus datos, cree una instantánea de la instancia de base de datos. Copie la instantánea y seleccione una clave de AWS KMS para la copia y, a continuación, restaure la copia de la instantánea cifrada en una nueva instancia de base de datos. Vuelva a dirigir las aplicaciones al nuevo punto final y elimine la instancia de base de datos no cifrada y sus

instantáneas. Para obtener más información, consulte Cifrar los recursos de Amazon RDS en la Guía del usuario de Amazon RDS.

- Exija el cifrado en tránsito: configure los clientes de su base de datos para que se conecten con ellos SSL/TLS mediante el paquete de certificados de Amazon RDS. Imponga las conexiones cifradas en la instancia de base de datos mediante el parámetro que su motor de base de datos proporciona para tal fin. Para obtener más información, consulte Uso SSL/TLS para cifrar una conexión a una instancia de base de datos o un clúster en la Guía del usuario de Amazon RDS.
- Supervise el acceso a la instancia de base de datos: publique los registros del motor de base de datos en Amazon CloudWatch Logs y revíselos para ver si hay conexiones procedentes de fuentes inesperadas y si hay consultas en las tablas que contienen registros confidenciales. Para obtener más información, consulte la sección Supervisión de los archivos de registro de Amazon RDS en la Guía del usuario de Amazon RDS.

Remediación de las exposiciones de los buckets de Amazon S3

AWS Security Hub puede generar hallazgos de exposición para los buckets de Amazon Simple Storage Service (Amazon S3).

En la consola de Security Hub, el bucket de Amazon S3 involucrado en un resultado de exposición y su información de identificación aparecen en la sección Recursos de los detalles del resultado. De forma programática, puede recuperar los detalles de los recursos con el GetFindingsV2 funcionamiento de la API CSPM de Security Hub.

Después de identificar el recurso involucrado en un resultado de exposición, puede eliminar el recurso si no lo necesita. Eliminar un recurso no esencial puede reducir su perfil de exposición y sus costos. AWS Si el recurso es esencial, siga estos pasos de remediación recomendados para ayudar a mitigar el riesgo. Los temas de remediación se dividen según el tipo de condición.

Un único resultado de exposición puede incluir problemas identificados en varios temas de remediación. También es posible abordar un resultado de exposición y disminuir su nivel de gravedad con solo tratar uno de los temas de remediación. El enfoque de remediación adecuado depende de los requisitos y cargas de trabajo de la organización.

> **Note**
>
> La guía de remediación que se proporciona en este tema puede requerir consultas adicionales en otros AWS recursos.

Contenido

- Condiciones de configuración incorrecta para buckets de Amazon S3
  - El bucket de Amazon S3 tiene el control de versiones desactivado
  - El bucket de Amazon S3 tiene desactivado el bloqueo de objetos
  - El bucket de Amazon S3 no está cifrado en reposo con AWS KMS claves
  - Multi-factor La eliminación de la autenticación (MFA) está inhabilitada en un bucket de Amazon S3 versionado
  - El bucket de Amazon S3 permite acceder a directores de otros AWS cuentas para modificar los permisos del bucket
- Condiciones de accesibilidad de los buckets de Amazon S3
  - El bucket de Amazon S3 tiene acceso público de lectura
  - El bucket de Amazon S3 tiene acceso de escritura público
- Condiciones de información confidencial para buckets de Amazon S3
  - El bucket de Amazon S3 contiene datos confidenciales

Condiciones de configuración incorrecta para buckets de Amazon S3

Estas son condiciones de configuración incorrecta en buckets de Amazon S3 y los pasos de remediación sugeridos.

El bucket de Amazon S3 tiene el control de versiones desactivado

El control de versiones de Amazon S3 permite conservar múltiples variantes de un mismo objeto dentro del bucket. Cuando el control de versiones está deshabilitado, Amazon S3 almacena solo la versión más reciente de cada objeto, lo que significa que si los objetos se eliminan o sobrescriben de forma accidental o malintencionada, no se pueden recuperar. Versioning-enabled Los buckets brindan protección contra la eliminación accidental, los errores de las aplicaciones y los incidentes de seguridad, como los ataques de ransomware, en los que pueden producirse modificaciones o eliminaciones no autorizadas de los datos. Siguiendo las prácticas recomendadas de seguridad, habilite el control de versiones de los buckets que contengan datos importantes que, en caso de pérdida, resultaría difícil o imposible recrear.

Solución: habilite el control de versiones

Para habilitar el control de versiones de Amazon S3 en un bucket, consulte Habilitar el control de versiones en cubos en la guía del usuario de Amazon S3. Cuando habilite el control de versiones,

considere implementar reglas de ciclo de vida para administrar el almacenamiento, ya que el control de versiones conserva múltiples copias de los objetos.

El bucket de Amazon S3 tiene desactivado el bloqueo de objetos

El bloqueo de objetos de Amazon S3 proporciona un modelo de escritura única y lectura múltiple (WORM) para los objetos de S3, lo que evita que se eliminen o sobrescriban durante un periodo establecido o de manera indefinida. Cuando el bloqueo de objetos está desactivado, los objetos pueden quedar expuestos a eliminaciones, modificaciones o cifrados accidentales o maliciosos, por ejemplo, durante un ataque de ransomware. El bloqueo de objetos resulta especialmente importante para cumplir requisitos normativos que exigen almacenamiento inmutable de datos y para protegerse contra amenazas sofisticadas, como ataques de ransomware que intentan cifrar la información. Al habilitar el bloqueo de objetos, puede aplicar políticas de retención como una capa adicional de protección y crear una estrategia de copias de seguridad inmutables para los datos críticos. Siguiendo las prácticas recomendadas de seguridad, habilite el bloqueo de objetos para evitar la modificación malintencionada de sus objetos.

Solución: configure S3 Object Lock

Tenga en cuenta que el bloqueo de objetos solo se puede habilitar al crear un bucket nuevo, por lo que será necesario crear un bucket con el bloqueo de objetos habilitado. Para migraciones de gran tamaño, considere usar Operaciones por lotes para copiar los objetos en el nuevo bucket. Antes de bloquear cualquier objeto, también debe habilitar el control de versiones de Amazon S3 y el bloqueo de objetos en el bucket. Dado que el bloqueo de objetos solo se puede habilitar en buckets nuevos, deberá migrar los datos existentes a un bucket nuevo con el bloqueo de objetos habilitado. Para obtener información sobre cómo configurar el bloqueo de objetos en un bucket, consulte Configurar el bloqueo de objetos de Amazon S3 en la guía del usuario de Amazon S3. Tras configurar el bloqueo de objetos, elija un modo de retención adecuado en función del entorno.

El bucket de Amazon S3 no está cifrado en reposo con AWS KMS claves

Amazon S3 aplica cifrado del lado del servidor con claves administradas de Amazon S3 como nivel predeterminado de cifrado para todos los buckets nuevos. Si bien las claves administradas por Amazon S3 proporcionan una sólida protección de cifrado, no ofrecen el mismo nivel de control de acceso y capacidades de auditoría que AWS Key Management Service las claves. Cuando se utilizan claves de KMS, el acceso a los objetos requiere permisos tanto para el bucket de Amazon S3 como para la clave de KMS que cifró el objeto. Esto resulta especialmente importante para información confidencial para la cual se necesita un control detallado sobre quién puede acceder a los objetos cifrados y un registro de auditoría exhaustivo del uso de las claves de cifrado. Siguiendo

las prácticas recomendadas de seguridad, utilice las claves de KMS para cifrar los depósitos que contienen datos confidenciales o para entornos con requisitos de cumplimiento estrictos.

Solución: configure la clave de bucket de S3

Para configurar un bucket para que utilice una clave de bucket de Amazon S3 para objetos nuevos, consulte Configurar el bucket para usar una clave de bucket de Amazon S3 con SSE-KMS objetos nuevos en la guía del usuario de Amazon S3. Para obtener información sobre cómo cifrar un objeto existente, consulte Cifrar objetos con las operaciones por lotes de Amazon S3 en el blog de AWS almacenamiento.

Al implementar el AWS KMS cifrado, tenga en cuenta lo siguiente:

- Administración de claves: decida si va a utilizar una clave AWS gestionada o una clave gestionada por el cliente (CMK). Las CMK ofrecen a los clientes control total sobre el ciclo de vida y el uso de sus claves. Para obtener más información sobre la diferencia entre estos dos tipos de claves, consulte Comparación de claves de AWS KMS en la Guía del desarrollador de AWS Key Management Service .
- Rotación de claves: para aplicar medidas de seguridad adicionales, habilite la rotación automática de claves para las claves de KMS. Para obtener más información, consulte Habilitación de la rotación automática de claves en la Guía del desarrollador de AWS Key Management Service .

Multi-factor La eliminación de la autenticación (MFA) está inhabilitada en un bucket de Amazon S3 versionado

Multi-factor La eliminación mediante autenticación (MFA) proporciona un nivel adicional de seguridad para su bucket de Amazon S3. Requiere autenticación multifactor para operaciones destructivas de Amazon S3. Cuando la eliminación mediante MFA está desactivada, los usuarios con permisos adecuados pueden eliminar permanentemente versiones de objetos o suspender el control de versiones en el bucket sin tener que superar desafíos de autenticación adicionales. La habilitación de la eliminación mediante MFA ayuda a proteger los datos contra eliminaciones no autorizadas o accidentales y brinda mayor protección frente a ataques de ransomware, amenazas internas y errores operativos. La eliminación mediante MFA es especialmente valiosa para buckets que contienen datos críticos o sujetos a requisitos de cumplimiento en materia de información confidencial que se deben proteger contra eliminaciones no autorizadas. Siguiendo las prácticas recomendadas de seguridad, habilite la MFA en sus buckets de Amazon S3.

Corrección

Tome una o más de las siguientes medidas para hacer frente a esta exposición:

Revisión de tipos de MFA

AWS admite los siguientes tipos https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa.html#id_credentials_mfa-types de MFA. Aunque la autenticación con un dispositivo físico normalmente proporciona una protección de seguridad más estricta, usar cualquier tipo de MFA es más seguro que tener MFA desactivado.

Habilitación de MFA en el nivel de la política de recursos

Uso de la clave de condición de `aws:MultiFactorAuthAge` en una política de bucket para exigir MFA en operaciones sensibles. Para obtener más información, consulte Exigir la MFA en la guía del usuario de Amazon S3.

Habilitar MFA

Para habilitar la eliminación de MFA, primero asegúrese de que el control de versiones esté habilitado en el bucket de Amazon S3. La eliminación de MFA solo se admite en los buckets que tienen habilitado el control de versiones. Para obtener información sobre cómo habilitar el control de versiones de Amazon S3, consulte Habilitar el control de versiones en cubos en la guía del usuario de Amazon S3. La eliminación de MFA no se puede habilitar a través de la consola de Amazon S3. Debe usar la API de Amazon S3 o la AWS CLI. Para obtener más información, consulte Configurar la eliminación de MFA en la guía del usuario de Amazon S3.

El bucket de Amazon S3 permite acceder a directores de otros AWS cuentas para modificar los permisos del bucket

Las políticas de bucket de Amazon S3 controlan el acceso a los buckets y objetos. Cuando las políticas del bucket permiten a los directores de otras AWS cuentas modificar los permisos del bucket, los usuarios no autorizados pueden reconfigurar el bucket. Si las credenciales principales externas se ven comprometidas, los usuarios no autorizados pueden hacerse con el control de tu bucket, lo que puede provocar filtraciones de datos o interrupciones del servicio. Siguiendo los principios de seguridad estándar, restringe las acciones de administración de permisos únicamente a los directores de confianza.

Corrección

Tome una o más de las siguientes medidas para hacer frente a esta exposición:

Revisión e identificación de las políticas del bucket

En la exposición, identifique el bucket de Amazon S3 en el campo ARN. En la consola de Amazon S3, seleccione el bucket y vaya a la pestaña Permisos para revisar la política de bucket. Revise la política de permisos asociada al bucket. Busque declaraciones de política que otorguen acciones como `s3:PutBucketPolicy, s3:PutBucketAcl, s3:DeleteBucketPolicy, s3:*` ,o declaraciones de política que permitan acceso a entidades principales externas a la cuenta, según lo indicado en la declaración de entidad principal.

Modificación de la política de bucket

Modifique la política de cubos para eliminar o restringir las acciones concedidas a otras AWS cuentas:

- Elimine las declaraciones de política que otorguen a cuentas externas acciones de administración de permisos.
- Si se requiere el acceso multicuenta, sustituya los permisos (`s3:*`) amplios por acciones específicas que no incluyan la administración de los permisos de los buzones.

Para obtener información sobre cómo modificar una política de bucket, consulte Cómo agregar una política de bucket mediante la consola de Amazon S3 en la Guía del usuario de Amazon S3.

Condiciones de accesibilidad de los buckets de Amazon S3

A continuación se presentan las condiciones de accesibilidad de los buckets de Amazon S3 y los pasos sugeridos para su remediación.

El bucket de Amazon S3 tiene acceso público de lectura

Los buckets de Amazon S3 con acceso público de lectura permiten que cualquier persona en Internet vea el contenido del bucket. Si bien esto puede ser necesario para sitios web públicos o recursos compartidos, puede generar riesgos de seguridad si el bucket contiene información confidencial. El acceso público de lectura puede provocar visualización y descarga no autorizada, lo que puede derivar en filtraciones de datos si se almacena información confidencial en esos buckets. Siguiendo los principios de seguridad estándar, restrinja el acceso a los buckets de Amazon S3 a los usuarios y sistemas necesarios.

Corrección

Tome una o más de las siguientes medidas para hacer frente a esta exposición:

Bloqueo del acceso público a nivel de bucket

Amazon S3 ofrece opciones de bloqueo de acceso público que se pueden configurar tanto a nivel de bucket como a nivel de cuenta para evitar el acceso público, independientemente de las políticas de bucket o de las ACL. Para obtener más información, consulte Bloquear el acceso público a su almacenamiento de Amazon S3 en la Guía del usuario de Amazon S3. Después de bloquear el acceso público, revise la configuración de control de acceso del bucket para asegurarse de que se ajuste a los requisitos de acceso. Luego revise la política de bucket de Amazon S3 para definir explícitamente quién puede acceder al bucket. Para ver ejemplos de políticas de cubos, consulte Ejemplos de políticas de cubos de Amazon S3 en la guía del usuario de Amazon S3.

Métodos de acceso alternativos

Si se requiere acceso público de lectura, considere estas alternativas más seguras:

- Amazon CloudFront: úselo CloudFront con una identidad de acceso de origen (OAI) o un control de acceso de origen (OAC) para permitir el acceso de lectura desde un bucket privado de Amazon S3. Esta alternativa restringe el acceso directo a su bucket de Amazon S3 y, al mismo tiempo, permite el acceso público al contenido a través de él. CloudFront Para obtener más información, consulte Restringir el acceso a un origen de Amazon S3 en la Guía para CloudFront desarrolladores de Amazon.
- URL prefirmadas: use URL prefirmadas para proporcionar acceso temporal a objetos específicos. Para obtener más información, consulte Compartir objetos con URL prefirmadas en la guía del usuario de Amazon S3.

El bucket de Amazon S3 tiene acceso de escritura público

Los buckets de Amazon S3 con acceso público de escritura permiten que cualquier persona en Internet cargue, modifique o elimine objetos en el bucket. Esto genera riesgos de seguridad significativos, incluido el potencial de que alguien cargue archivos maliciosos, modifique archivos existentes o elimine datos. El acceso público de escritura crea vulnerabilidades de seguridad que pueden ser aprovechadas por atacantes. Siguiendo los principios de seguridad estándar, restrinja el acceso de escritura a los buckets de Amazon S3 únicamente a los usuarios y sistemas necesarios.

Corrección

Tome una o más de las siguientes medidas para hacer frente a esta exposición:

Bloqueao del acceso público a nivel de cuenta y de bucket

Amazon S3 ofrece opciones de bloqueo de acceso público que se pueden configurar tanto a nivel de bucket como a nivel de cuenta para impedir el acceso público, independientemente de las políticas

de bucket o de las ACL. Para obtener más información, consulte Bloquear el acceso público a su almacenamiento de Amazon S3 en la Guía del usuario de Amazon S3.

Modificación de las políticas de bucket

Para un enfoque más detallado al eliminar el acceso público de escritura, revise la política de bucket. Puede buscar `s3:PutObject`, `s3:DeleteObject` o `s3:*`. Para obtener más información sobre la administración de las políticas de cubos, consulte las políticas de cubos de Amazon S3 en la guía del usuario de Amazon S3.

Métodos de acceso alternativos

Si se requiere acceso de escritura pública, considere estas alternativas más seguras:

- URL prefirmadas: use URL prefirmadas para proporcionar acceso temporal a objetos específicos. Para obtener más información, consulte Compartir objetos con URL prefirmadas en la Guía del usuario de Amazon S3.
- Proxy de Amazon API Gateway: utilice un intermediario como API Gateway AWS Lambda para validar y autorizar las solicitudes antes de escribirlas en su bucket de Amazon S3. Este enfoque garantiza que los clientes nunca escriban directamente en el bucket. Para obtener más información, consulte el tutorial: Creación de una API REST como proxy de Amazon S3 en la Guía para desarrolladores de API Gateway.
- Amazon CloudFront: úselo CloudFront con un control de acceso de Origin (OAC) configurado para firmar siempre las solicitudes. Habilite los métodos PUT y POST para permitir las escrituras autenticadas sin exponer directamente su bucket de Amazon S3. Configure su política de cubos para restringir `s3:DeleteObject` los permisos únicamente a las personas principales autorizadas, de modo que los usuarios no autorizados no puedan eliminar los objetos que desea conservar. Para obtener más información, consulte Restringir el acceso a un origen de Amazon S3 en la Guía para CloudFront desarrolladores de Amazon.

Condiciones de información confidencial para buckets de Amazon S3

A continuación se presentan las condiciones de información confidencial para los buckets de Amazon S3 y los pasos de remediación sugeridos.

El bucket de Amazon S3 contiene datos confidenciales

Un análisis de seguridad de los datos ha confirmado que hay datos confidenciales en el bucket de Amazon S3. Un producto de seguridad de datos integrado establece esta característica cuando

inspecciona los objetos del bucket e identifica el contenido que requiere protección. Security Hub notifica la característica de la misma manera, independientemente del producto que haya realizado la inspección.

La información confidencial puede incluir:

- Credenciales
- Información de identificación personal
- Información financiera
- Contenido confidencial que requiere protección

Si la información confidencial se expone por una configuración incorrecta o por acceso no autorizado, esto puede generar infracciones de cumplimiento, filtraciones de datos, robo de identidad o pérdidas financieras. Siga las prácticas recomendadas de seguridad para garantizar la clasificación adecuada de los datos y la supervisión continua de los datos confidenciales en sus buckets de Amazon S3.

Corrección

Para eliminar esta característica, elimine los datos confidenciales del bucket. Si su carga de trabajo requiere que el depósito almacene datos confidenciales, implemente los siguientes controles de seguridad para reducir el riesgo de exposición.

Revisa los datos confidenciales del bucket

En la búsqueda de exposición, elija Abrir recurso. Revise el resultado de seguridad de los datos en el que se registraron los datos confidenciales para determinar qué objetos o prefijos los contienen. Si la detección provino de Macie, el tipo de hallazgo describe la categoría de datos confidenciales. Para obtener más información, consulte los tipos de hallazgos de Macie en la guía del usuario de Amazon Macie.

Según el tipo de información confidencial identificada, implemente los controles de seguridad apropiados:

- Restricción del acceso al bucket: revise los permisos del bucket para asegurarse de que sigan el principio de privilegio mínimo. Use políticas de IAM, políticas de bucket y ACL para restringir el acceso. Para obtener más información, consulte la administración de identidades y accesos para Amazon S3 en la guía del usuario de Amazon S3.
- Habilitación del cifrado del lado del servidor: habilite el cifrado del lado del servidor con claves de KMS para obtener una protección adicional. Para obtener más información, consulte Uso

del cifrado del lado del servidor con claves de AWS KMS (SSE-KMS) en la guía del usuario de Amazon S3.

- Redacte o transforme los datos confidenciales: si no es necesario que los objetos conserven valores confidenciales, utilícelos AWS Glue DataBrew para preparar los datos. Aplique las transformaciones de enmascaramiento, reemplazo o generación de hash que eliminen esos valores antes de que los sistemas posteriores consuman los datos. Escriba la salida preparada en un bucket independiente que tenga sus propios controles de acceso. Para obtener más información, consulte ¿Qué es AWS Glue DataBrew? en la Guía para desarrolladores de AWS Glue DataBrew .

Cómo corregir las exposiciones de las instancias de cuadernos de Amazon SageMaker

AWS Security Hub puede generar datos de exposición para las instancias de SageMaker ordenadores portátiles de Amazon.

En la consola de Security Hub, la instancia del bloc de notas implicada en la detección de una exposición y su información identificativa aparecen en la sección Recursos de los detalles de la búsqueda. Puede recuperar los detalles de los recursos mediante programación utilizando la API GetFindingsV2 CSPM de Security Hub.

Después de identificar el recurso involucrado en un resultado de exposición, puede eliminar el recurso si no lo necesita. Eliminar un recurso no esencial puede reducir su perfil de exposición y sus costos. AWS Si el recurso es esencial, siga estos pasos de remediación recomendados para ayudar a mitigar el riesgo. Los temas de remediación se dividen según el tipo de condición.

Un único resultado de exposición puede incluir problemas identificados en varios temas de remediación. También es posible abordar un resultado de exposición y disminuir su nivel de gravedad con solo tratar uno de los temas de remediación. El enfoque de remediación adecuado depende de los requisitos y cargas de trabajo de la organización.

> **Note**
>
> La guía de remediación que se proporciona en este tema puede requerir consultas adicionales en otros AWS recursos.

Contenido

- Características de configuración incorrecta de las instancias de Amazon Notebook SageMaker
  - La instancia de Amazon SageMaker Notebook tiene habilitado el acceso directo a Internet
  - La instancia de Amazon SageMaker Notebook tiene habilitado el acceso root
- Características de los datos confidenciales de las instancias de Amazon SageMaker Notebook
  - La instancia de Amazon SageMaker Notebook contiene datos confidenciales
- Características de impacto de las instancias de Amazon SageMaker Notebook
  - Tiene el control total de la ruta de ejecución privilegiada
  - Tiene una ruta directa de escalamiento de políticas
  - Tiene una ruta de secuestro de políticas de confianza
  - Tiene una ruta de ransomware de datos
  - Ha eliminado la ruta de restricción
  - Tiene el rol de pase, crea la ruta de ejecutor.
  - Tiene una ruta de ejecución existente (rol de intercambio).
  - Tiene una ruta de escalamiento de la cadena de funciones
  - Tiene una ruta de ejecución privilegiada para inyectar código
  - Ha deshabilitado la ruta del registro de auditoría
  - Tiene acceso a la ruta de ejecución existente
  - Tiene una ruta de acuñación de credenciales
  - Tiene una ruta de acceso a los datos con rol de pasante
  - Ha pasado el rol, la tarea, el secuestro, la ruta
  - Tiene una ruta de acceso a los datos de un solo salto
  - Tiene una ruta de avance de la capacidad

Características de configuración incorrecta de las instancias de Amazon Notebook SageMaker

Estas son las características de configuración incorrecta de las instancias de SageMaker cuadernos de Amazon y las medidas de corrección sugeridas.

La instancia de Amazon SageMaker Notebook tiene habilitado el acceso directo a Internet

Cuando `DirectInternetAccess` está habilitada en una instancia de Amazon SageMaker Notebook, el tráfico saliente se dirige a Internet a través de una pasarela de traducción de direcciones de SageMaker-managed red (NAT). Esto proporciona una ruta de salida que se puede

utilizar para filtrar datos o como canal de mando y control en caso de que el portátil esté en peligro. Siga las prácticas recomendadas de seguridad, inhabilite el acceso directo a Internet y coloque las instancias de los ordenadores portátiles en una VPC con puntos de conexión de VPC para los servicios necesarios. AWS

Corrección

Tome una o más de las siguientes medidas para hacer frente a esta exposición:

Deshabilitar el acceso directo a Internet

La `DirectInternetAccess` configuración no se puede cambiar después de crear una instancia de bloc de notas. Para inhabilitarla, crea una nueva instancia de bloc de notas con el `DirectInternetAccess` valor establecido `Disabled` en en una subred privada de una VPC y, a continuación, migra los blocs de notas y los datos de la instancia existente. Para obtener instrucciones, consulte Cómo conectar una instancia de bloc de notas de una VPC a recursos externos en la Guía para desarrolladores de Amazon. SageMaker

Configurar puntos de conexión de VPC

Cuando el acceso directo a Internet está inhabilitado, la instancia del bloc de notas requiere puntos de enlace de la VPC para acceder a AWS servicios como Amazon S3 y la API de Amazon. SageMaker Cree puntos de enlace de VPC de interfaz para los servicios que necesita su bloc de notas. Para obtener información sobre los puntos finales de la VPC, consulte ¿Qué es? AWS PrivateLink en la Guía. AWS PrivateLink

La instancia de Amazon SageMaker Notebook tiene habilitado el acceso root

Cuando `RootAccess` está habilitada en una instancia de Amazon SageMaker Notebook, los usuarios tienen todos los privilegios de OS-level root. El acceso root permite realizar modificaciones arbitrarias del sistema, crear puertas traseras persistentes e instalar paquetes sin restricciones. Siguiendo las prácticas recomendadas de seguridad, deshabilita el acceso raíz para las instancias de ordenadores portátiles, a menos que sea necesario de forma explícita para tu flujo de trabajo.

Solución: inhabilite el acceso root

No puede cambiar la `RootAccess` configuración en una instancia de notebook en ejecución. Para inhabilitarla, detenga la instancia y, a continuación, actualice la configuración de la instancia `RootAccess` para establecerla en`Disabled`. La mayoría de los flujos de trabajo de los ordenadores portátiles, incluida la instalación de paquetes con configuraciones del ciclo de vida `pip` y la ejecución de las mismas, siguen funcionando sin acceso root. Para obtener instrucciones, consulte Controlar

el acceso root a una instancia de Amazon SageMaker Notebook en la Guía para SageMaker desarrolladores de Amazon.

Consideraciones adicionales

Si se requiere el acceso root para tareas específicas, considere la posibilidad de utilizar en su lugar las libretas de Amazon SageMaker Studio, que proporcionan entornos aislados basados en contenedores con controles de acceso más granulares. También puedes usar las configuraciones del ciclo de vida para preinstalar los paquetes necesarios en el momento de la creación de la instancia, lo que reduce la necesidad de acceso raíz durante el uso normal.

Características de los datos confidenciales de las instancias de Amazon SageMaker Notebook

Estas son las características de los datos confidenciales de las instancias de SageMaker cuadernos de Amazon y las medidas de corrección sugeridas.

La instancia de Amazon SageMaker Notebook contiene datos confidenciales

Un análisis de seguridad de los datos ha confirmado que hay datos confidenciales en la instancia del SageMaker bloc de notas de Amazon. Un producto de seguridad de datos integrado establece esta característica. El producto inspecciona los archivos, las salidas y el almacenamiento adjunto del portátil e identifica el contenido que requiere protección. Registramos esta característica en Security Hub de forma sistemática, independientemente del producto integrado que haya realizado la inspección.

Los datos confidenciales aumentan el impacto de cualquier otro punto débil en la misma instancia de portátil. Un rol de ejecución permisivo, una ruta de salida directa a Internet o un acceso demasiado amplio exponen el contenido regulado o confidencial. Un agente de amenazas que acceda a la libreta puede leer y copiar esos registros de los archivos de la libreta, de las celdas de salida y de los puntos de control guardados. De este modo, el autor de la amenaza puede conservar esos registros fuera de su entorno. También pueden usar cualquier credencial que se encuentre en el cuaderno para autenticarse en otros sistemas.

Siguiendo las prácticas recomendadas de seguridad, recomendamos restringir el acceso a las instancias de los ordenadores portátiles que contengan datos confidenciales y cifrar el almacenamiento adjunto en reposo.

La información confidencial puede incluir:

- Credenciales, como contraseñas, claves de acceso y cadenas de conexión

- Información de identificación personal
- Información financiera, como números de cuenta y datos de tarjetas de pago
- Contenido confidencial que requiere protección

Eliminar los datos confidenciales del portátil es la única forma de eliminar esta característica. Si el portátil debe hacer referencia a datos confidenciales, las siguientes prácticas recomendadas de seguridad reducen el riesgo de exposición.

Revise los datos confidenciales de la instancia del portátil

En el resultado de exposición, abra el recurso mediante el hipervínculo. De este modo, se abre la instancia de bloc de notas afectada. Anote el nombre de la instancia del bloc de notas, la AWS cuenta y la AWS región. Revisa el resultado de seguridad de los datos en el que se registraron los datos confidenciales para determinar qué archivos, celdas de salida o puntos de control del bloc de notas los contienen.

Según el tipo de información confidencial identificada, implemente los controles de seguridad apropiados:

- Elimine los valores confidenciales del bloc de notas: elimine los valores confidenciales del código del bloc de notas y borre las celdas de salida que los contienen. Elimine los puntos de control guardados y las copias exportadas que conserven los valores. Si un valor debe permanecer referenciado, sustitúyalo por un marcador de posición tokenizado o enmascarado. Para obtener más información, consulte Uso de instancias de SageMaker bloc de notas de Amazon en la Guía para desarrolladores de Amazon. SageMaker
- Cambia las credenciales expuestas: si el bloc de notas contenía credenciales, trátalas como si estuvieran comprometidas. Desactive y rote las credenciales y, a continuación, revise los registros de auditoría del sistema afectado para ver si utilizan los valores expuestos. Recupere los datos confidenciales en tiempo de ejecución AWS Secrets Manager mediante un rol de ejecución limitado en lugar de incluirlos en el contenido del bloc de notas. Para obtener más información, consulte Rotate AWS Secrets Manager Secrets en la Guía del usuario. AWS Secrets Manager
- Restrinja quién puede abrir la instancia del bloc de notas: conceda acceso solo a las identidades de IAM que lo necesiten. Limite la función de ejecución a las acciones y los recursos específicos que utiliza el bloc de notas. Controle quién puede abrir el bloc de notas restringiendo los `sagemaker:CreatePresignedNotebookInstanceUrl` permisos. Para obtener más información, consulte los ejemplos de políticas SageMaker basadas en la identidad de Amazon en la Guía para SageMaker desarrolladores de Amazon.

- Cifre el almacenamiento del bloc de notas en reposo: adjunte una AWS KMS clave a la instancia del bloc de notas para que el volumen de almacenamiento que contiene los archivos del bloc de notas y los puntos de control esté cifrado en reposo. Utilice una clave gestionada por el cliente para controlar la política de claves. Conceda `kms:Decrypt` esa clave solo a las identidades que necesitan leer el cuaderno. Para obtener más información, consulte Proteger los datos en reposo mediante el cifrado en la Guía para SageMaker desarrolladores de Amazon.
- Supervise el acceso a la instancia del bloc AWS CloudTrail de notas: compruebe si hay `sagemaker:CreatePresignedNotebookInstanceUrl` llamadas o accesos desde identidades o fuentes inesperadas. Para obtener más información, consulte Registrar las llamadas a la SageMaker API de Amazon AWS CloudTrail en la Guía para SageMaker desarrolladores de Amazon.

Características de impacto de las instancias de Amazon SageMaker Notebook

Los rasgos de impacto describen el radio de explosión potencial de una exposición. Security Hub analiza los permisos efectivos del AWS Identity and Access Management principal asociado a la instancia del SageMaker portátil para determinar los recursos posteriores a los que podría acceder un atacante si la instancia del portátil se viera comprometida. Cada rasgo de impacto identifica un patrón de escalamiento de privilegios específico. Para reducir tu radio de ataque, revisa las rutas de permisos descritas en cada rasgo y elimina cualquier privilegio innecesario.

Siguiendo los principios de seguridad estándar, otorga el mínimo privilegio proporcionando solo los permisos necesarios para realizar una tarea. Sustituya las políticas generales por políticas más específicas que concedan solo las acciones y los recursos específicos que se necesitan. Para identificar los permisos no utilizados que desee eliminar, utilice IAM Access Analyzer para generar recomendaciones basadas en el historial de acceso. Para obtener más información, consulte las conclusiones sobre el acceso externo y no utilizado y sobre la aplicación de permisos con privilegios mínimos en la guía del usuario de IAM.

Tiene el control total de la ruta de ejecución privilegiada

El director asociado puede transferir una función e inyectar código en un recurso informático que ya tenga permisos elevados. Esto permite al principal obtener el control total sobre el ejecutor y realizar cualquier acción que permita la función del ejecutor.

Tiene una ruta directa de escalamiento de políticas

El director asociado puede modificar directamente las políticas de IAM para concederse permisos adicionales, aumentando así sus propios privilegios sin necesidad de recursos intermedios.

Tiene una ruta de secuestro de políticas de confianza

El director asociado puede modificar la política de confianza de una función de IAM para poder asumir esa función y obtener los permisos correspondientes.

Tiene una ruta de ransomware de datos

El director asociado puede cifrar o eliminar datos de una forma que podría utilizarse para el ransomware, por ejemplo, cifrando objetos de Amazon S3 con una AWS KMS clave gestionada por el cliente y, a continuación, modificando la política de claves.

Ha eliminado la ruta de restricción

El principal asociado puede eliminar las restricciones de seguridad, como los límites de permisos, las políticas de control de servicios o las declaraciones de denegación de políticas basadas en recursos, ampliando así lo que pueden hacer otros directores o el propio recurso.

Tiene el rol de pase, crea la ruta de ejecutor.

El principal asociado puede crear un nuevo recurso informático (como una función de Lambda o una instancia de Amazon EC2) y asignarle un rol privilegiado, lo que permite blanquear de manera efectiva sus propios permisos a través del nuevo recurso.

Tiene una ruta de ejecución existente (rol de intercambio).

El director asociado puede cambiar la función de IAM asociada a un recurso informático existente y sustituirla por una función más privilegiada para escalar el acceso.

Tiene una ruta de escalamiento de la cadena de funciones

El director asociado puede asumir una secuencia de funciones, en la que cada función de la cadena tiene permisos cada vez más amplios y, en última instancia, alcanza una función altamente privilegiada.

Tiene una ruta de ejecución privilegiada para inyectar código

El principal asociado puede inyectar código en un recurso informático en ejecución que tenga permisos elevados y ejecutar operaciones arbitrarias bajo la función privilegiada de ese recurso.

Ha deshabilitado la ruta del registro de auditoría

El director asociado puede deshabilitar los servicios de registro o supervisión, por ejemplo CloudTrail, cubrir eficazmente sus huellas durante una escalada o después de ella.

Tiene acceso a la ruta de ejecución existente

El principal asociado puede invocar o conectarse a un recurso informático existente y usar su rol adjunto para realizar acciones privilegiadas.

Tiene una ruta de acuñación de credenciales

El director asociado puede crear nuevas credenciales a largo plazo (como claves de acceso o perfiles de inicio de sesión) para otros principales, estableciendo rutas de acceso persistentes que sobrevivan a la rotación de contraseñas o al vencimiento de la sesión.

Tiene una ruta de acceso a los datos con rol de pasante

El principal asociado puede crear un recurso de servicio y asignarle una función de acceso a datos confidenciales y obtener acceso indirecto a esos datos a través del nuevo recurso.

Ha pasado el rol, la tarea, el secuestro, la ruta

El director asociado puede transferir un rol a una tarea programada o basada en eventos (como una función de Lambda activada por un evento), lo que le permite ejecutar código arbitrario con los permisos de ese rol.

Tiene una ruta de acceso a los datos de un solo salto

El director asociado puede acceder directamente a los recursos de datos confidenciales (como los cubos de Amazon S3 o las tablas de DynamoDB) mediante sus permisos actuales, sin necesidad de pasos de escalamiento intermedios.

Tiene una ruta de avance de la capacidad

El principal asociado tiene una ruta de escalamiento de privilegios que mejora sus capacidades generales más allá de lo que sugerirían los permisos que le han sido asignados directamente. Esta es una clasificación general para las rutas que no coinciden con un patrón más específico.

Cómo corregir las exposiciones de las máquinas virtuales de Azure

AWS Security Hub puede generar datos de exposición para las máquinas virtuales de Azure.

En la consola de Security Hub, la máquina virtual de Azure implicada en la detección de una exposición y su información de identificación aparecen en la sección Recursos de los detalles de

la búsqueda. Puede recuperar los detalles de los recursos mediante programación mediante la API GetFindingsV2 CSPM de Security Hub.

Después de identificar el recurso involucrado en un resultado de exposición, puede eliminar el recurso si no lo necesita. Eliminar un recurso no esencial puede reducir su perfil de exposición y sus costos. AWS Si el recurso es esencial, siga estos pasos de remediación recomendados para ayudar a mitigar el riesgo. Los temas de remediación se dividen según el tipo de condición.

Un único resultado de exposición puede incluir problemas identificados en varios temas de remediación. También es posible abordar un resultado de exposición y disminuir su nivel de gravedad con solo tratar uno de los temas de remediación. El enfoque de remediación adecuado depende de los requisitos y cargas de trabajo de la organización.

> **Note**
>
> La guía de corrección que se proporciona en este tema puede requerir consultas adicionales en otros recursos de Microsoft Azure.

Contenido

- Características de configuración incorrecta de las máquinas virtuales de Azure
  - La máquina virtual de Azure tiene un grupo de seguridad de red abierto
  - La máquina virtual de Azure tiene una regla de seguridad que permite el acceso mediante SSH o RDP
  - La función asociada a la máquina virtual de Azure tiene una asignación de funciones de acceso administrativo
  - La máquina virtual Azure tiene un sistema operativo que ha llegado al final de su vida útil
- Características de accesibilidad de las máquinas virtuales de Azure
  - Se puede acceder a la máquina virtual de Azure a través de Internet
- Características de vulnerabilidad de las máquinas virtuales de Azure
  - La máquina virtual de Azure presenta vulnerabilidades de software que se pueden explotar en la red con una alta probabilidad de explotación
  - La máquina virtual Azure tiene vulnerabilidades de software
  - La máquina virtual Azure tiene paquetes de software malintencionado

Características de configuración incorrecta de las máquinas virtuales de Azure

Estas son las características de errores de configuración de las máquinas virtuales de Azure y las medidas de corrección sugeridas.

La máquina virtual de Azure tiene un grupo de seguridad de red abierto

Un grupo de seguridad de red (NSG) actúa como un firewall virtual para su máquina virtual de Azure y filtra el tráfico entrante y saliente con un conjunto de reglas de seguridad priorizadas. Un grupo de seguridad de red abierto contiene reglas que permiten el acceso sin restricciones desde cualquier fuente (por ejemplo, una fuente de o). `Any` `0.0.0.0/0` Estas reglas pueden exponer su máquina virtual a un acceso no autorizado desde Internet. Siguiendo los principios de seguridad estándar, restrinja las reglas de los grupos de seguridad de red únicamente a las direcciones IP, los puertos y los protocolos específicos que requiere su carga de trabajo.

Corrección

Tome una o más de las siguientes medidas para hacer frente a esta exposición:

Revise las reglas del grupo de seguridad de la red y evalúe la configuración actual

Identifique el grupo de seguridad de red asociado a la interfaz de red o subred de la máquina virtual y revise sus reglas de seguridad de entrada. Evalúe qué puertos permiten el tráfico desde amplios rangos de fuentes, como `Any` O. `0.0.0.0/0` Las reglas se procesan en orden de prioridad, así que asegúrese de que una regla permisiva no prevalezca sobre una más restrictiva. Para obtener más información, consulte Grupos de seguridad de red en la documentación de Microsoft Azure.

Restrinja las reglas de los grupos de seguridad

Modifique o elimine las reglas que permiten el acceso sin restricciones. Sustituya una fuente amplia, por ejemplo, por direcciones IP confiables, rangos de CIDR, etiquetas de servicio o grupos de seguridad de aplicaciones específicos a los que se deba acceder. `Any` Limite el rango de puertos de destino solo a los puertos que usa su carga de trabajo. Para obtener más información, consulte Administrar grupos de seguridad de red en la documentación de Microsoft Azure.

La máquina virtual de Azure tiene una regla de seguridad que permite el acceso mediante SSH o RDP

Los protocolos de administración remota, como SSH (puerto 22) y RDP (puerto 3389), permiten a los usuarios conectarse a las máquinas virtuales de Azure y administrarlas desde ubicaciones remotas. Cuando la regla de un grupo de seguridad de red permite estos puertos desde Internet (una fuente de `Any` o`0.0.0.0/0`), la superficie de ataque de la máquina virtual aumenta considerablemente

y queda expuesta a ataques de fuerza bruta y basados en credenciales. Siga los principios de seguridad estándar, limite el acceso remoto a direcciones IP específicas y confiables, o elimine por completo el acceso directo a Internet a estos puertos.

Corrección

Tome una o más de las siguientes medidas para hacer frente a esta exposición:

Restrinja la regla del grupo de seguridad de la red

Limite el acceso mediante SSH y RDP a determinadas direcciones IP confiables o rangos de CIDR`Any`, o elimine la regla de entrada si no es necesario el acceso remoto desde Internet. Para obtener más información, consulte Administrar grupos de seguridad de red en la documentación de Microsoft Azure.

Use Azure Bastion para una conectividad segura

En lugar de exponer los puertos SSH o RDP a Internet, use Azure Bastion para conectarse a su máquina virtual a través de TLS sin una dirección IP pública ni abrir puertos de entrada. Para obtener más información, consulte Azure Bastion en la documentación de Microsoft Azure.

Utilice el acceso justo a tiempo a las máquinas virtuales

Habilite el acceso justo a tiempo a las máquinas virtuales (JIT) en Microsoft Defender for Cloud para que los puertos de administración, como SSH y RDP, permanezcan cerrados de forma predeterminada y abiertos solo para las solicitudes aprobadas y con un límite de tiempo desde una dirección IP de origen específica. Para obtener más información, consulte Habilitar el acceso justo a tiempo en la documentación de Microsoft Azure.

La función asociada a la máquina virtual de Azure tiene una asignación de funciones de acceso administrativo

Puede asignar una identidad administrada a una máquina virtual de Azure y asignarle funciones de control de acceso basado en roles (Azure RBAC) de Azure para acceder a otros recursos de Azure. Cuando la identidad asociada tiene una asignación de funciones administrativas (por ejemplo, `Owner` o`Contributor`) en un ámbito amplio, normalmente concede permisos que van mucho más allá de lo que requiere la carga de trabajo. Si la máquina virtual se ve comprometida, un atacante puede usar estos permisos excesivos para moverse lateralmente por el entorno, acceder a los datos o manipular los recursos. Siguiendo los principios de seguridad estándar, conceda el mínimo privilegio asignando solo los permisos que necesita la carga de trabajo.

Corrección

Tome una o más de las siguientes medidas para hacer frente a esta exposición:

Revise e identifique las asignaciones de funciones administrativas

En el portal de Azure, revise las asignaciones de funciones para la identidad asociada a la máquina virtual. Busque funciones de administrador privilegiadas`Owner`, como`Contributor`, o`User Access Administrator`, y funciones personalizadas que utilicen un comodín (`*`) en sus `Actions` funciones. Para obtener más información, consulte Listar las asignaciones de funciones de Azure en la documentación de Microsoft Azure.

Implementación del acceso a los privilegios mínimos

Sustituya las asignaciones de funciones administrativas por la función integrada con menos privilegios, que solo otorga los permisos que requiere la carga de trabajo. Asígnelo al ámbito más limitado (recurso o grupo de recursos) que se adapte a sus necesidades. Al crear funciones personalizadas, especifique `Actions` y de `DataActions` forma explícita en lugar de utilizar un comodín. Para obtener más información, consulte las prácticas recomendadas para Azure RBAC en la documentación de Microsoft Azure.

La máquina virtual Azure tiene un sistema operativo que ha llegado al final de su vida útil

La máquina virtual de Azure ejecuta un sistema operativo al final de su vida útil que su proveedor ya no ofrece soporte ni mantenimiento. Cuando un sistema operativo llega al final de su vida útil, el proveedor deja de publicar actualizaciones y avisos de seguridad, lo que deja permanentemente sin corregir las vulnerabilidades conocidas y expone a la máquina virtual a los ataques. Siga las prácticas recomendadas de seguridad y actualice a una versión de sistema operativo compatible.

Solución: actualice a una versión de sistema operativo compatible

Planifique una actualización local o migre la carga de trabajo a una máquina virtual que ejecute una versión de sistema operativo compatible. Antes de actualizar, confirme la compatibilidad de las aplicaciones y realice una copia de seguridad o una instantánea para poder revertirla si es necesario. Para Windows, siga las instrucciones de actualización vigentes; para Linux, siga las instrucciones de actualización de su proveedor de distribución. Para obtener más información, consulte Realizar una actualización local de una máquina virtual de Windows Server en la documentación de Microsoft Azure.

Características de accesibilidad de las máquinas virtuales de Azure

Estas son las características de accesibilidad de las máquinas virtuales de Azure y los pasos de corrección sugeridos.

Se puede acceder a la máquina virtual de Azure a través de Internet

Una máquina virtual de Azure con puertos a los que se pueda acceder desde Internet podría estar expuesta a un ataque. Se puede acceder a una máquina virtual cuando tiene una dirección IP pública. También se puede acceder a ella cuando un balanceador de cargas, una puerta de enlace de aplicaciones u otra ruta de red permite el tráfico entrante desde Internet. Siguiendo los principios de seguridad estándar, implemente controles de acceso a la red con los privilegios mínimos restringiendo el tráfico entrante solo a las fuentes y los puertos necesarios.

Corrección

Tome una o más de las siguientes medidas para hacer frente a esta exposición:

Restrinja o elimine la exposición a Internet

Compruebe si la máquina virtual requiere una dirección IP pública. Si no es así, desasocie la dirección IP pública de la interfaz de red y, en su lugar, utilice una dirección IP privada. Si sigue siendo necesaria la conectividad saliente a Internet, utilice una puerta de enlace NAT.

Si se requiere acceso entrante, coloque la máquina virtual detrás de un balanceador de carga, un firewall de Azure o una puerta de enlace de aplicaciones en lugar de exponerla directamente. Para obtener más información, consulte las direcciones IP públicas en la documentación de Microsoft Azure.

Refuerce las reglas de los grupos de seguridad de la red entrante

Modifique o elimine las reglas de los grupos de seguridad de red entrantes que permiten el acceso sin restricciones (`Anyo0.0.0.0/0`) y restrinjan el acceso a los rangos de fuentes, puertos y protocolos específicos que requiere su carga de trabajo. Para obtener más información, consulte los grupos de seguridad de red en la documentación de Microsoft Azure.

Use Azure Bastion para el acceso de administración

Para la conectividad de administración, use Azure Bastion para acceder a la máquina virtual a través de TLS sin una dirección IP pública ni puertos abiertos. SSH/RDP Para obtener más información, consulte Azure Bastion en la documentación de Microsoft Azure.

Características de vulnerabilidad de las máquinas virtuales de Azure

Estas son las características de vulnerabilidad de las máquinas virtuales de Azure y las medidas de corrección sugeridas.

La máquina virtual de Azure presenta vulnerabilidades de software que se pueden explotar en la red con una alta probabilidad de explotación

Las vulnerabilidades y exposiciones comunes (CVE) pueden afectar a los paquetes de software instalados en las máquinas virtuales de Azure. Una vulnerabilidad de alta prioridad se puede explotar en la red con una alta probabilidad de explotación. Esto representa una amenaza inmediata para la seguridad, ya que es posible que el código de explotación ya esté a disposición del público y que los atacantes o las herramientas de análisis automatizadas lo utilicen activamente. Corrija estas vulnerabilidades con prontitud para proteger su máquina virtual.

Corrección

Tome una o más de las siguientes medidas para hacer frente a esta exposición:

Revise y corrija el hallazgo

Utilice la evaluación de vulnerabilidades de Microsoft Defender for Cloud para revisar las CVE afectadas y los pasos de corrección de la máquina virtual. El panel de detalles de cada hallazgo incluye los CVE relevantes y las soluciones recomendadas. Para obtener más información, consulte Cómo corregir las vulnerabilidades de las máquinas en la documentación de Microsoft Azure.

Aplica las actualizaciones

Use Azure Update Manager para evaluar e implementar las actualizaciones del sistema operativo y el software en sus máquinas virtuales según un cronograma. Si no hay ninguna actualización disponible, considere la posibilidad de eliminar o deshabilitar el software vulnerable, o de restringir el acceso de red al mismo, hasta que se publique un parche. Para obtener más información, consulte Azure Update Manager en la documentación de Microsoft Azure.

Consideraciones futuras

Para evitar que ocurran problemas en el futuro, permita que Microsoft Defender para servidores analice continuamente sus máquinas virtuales en busca de vulnerabilidades y establezca un programa de aplicación de parches regular con Azure Update Manager. Para obtener más información, consulte Microsoft Defender para servidores en la documentación de Microsoft Azure.

La máquina virtual Azure tiene vulnerabilidades de software

Las vulnerabilidades y exposiciones comunes (CVE) pueden afectar a los paquetes de software instalados en las máquinas virtuales de Azure. Las vulnerabilidades no críticas representan debilidades de seguridad con menor gravedad o capacidad de explotación que las vulnerabilidades

de alta prioridad. Si bien representan un riesgo menos inmediato, los atacantes pueden aprovechar las vulnerabilidades que no han sido reparadas para comprometer la confidencialidad, la integridad o la disponibilidad de los datos, o para acceder a otros sistemas. Siguiendo las prácticas recomendadas de seguridad, corrija estas vulnerabilidades para proteger su máquina virtual de los ataques.

Corrección

Tome una o más de las siguientes medidas para hacer frente a esta exposición:

Revise y corrija el hallazgo

Utilice la evaluación de vulnerabilidades de Microsoft Defender for Cloud para revisar las CVE afectadas y siga los pasos de corrección que figuran en el panel de detalles de búsqueda. Para obtener más información, consulta Cómo corregir las vulnerabilidades de las máquinas en la documentación de Microsoft Azure.

Aplica las actualizaciones

Use Azure Update Manager para evaluar e implementar las actualizaciones del sistema operativo y del software en sus máquinas virtuales. Para administrar las actualizaciones de manera uniforme y escalable, configure la aplicación de parches programada. Para obtener más información, consulte Azure Update Manager en la documentación de Microsoft Azure.

La máquina virtual Azure tiene paquetes de software malintencionado

Los paquetes malintencionados son componentes de software que contienen código dañino diseñado para comprometer la confidencialidad, la integridad y la disponibilidad de sus sistemas y datos. Los paquetes malintencionados representan una amenaza activa y crítica para su máquina virtual, ya que los atacantes pueden ejecutar el código malintencionado automáticamente sin aprovechar una vulnerabilidad independiente. Siga las prácticas recomendadas de seguridad y elimine los paquetes malintencionados para proteger su máquina virtual de posibles ataques.

Solución: investigue y elimine los paquetes malintencionados

Revise los detalles de los hallazgos para comprender la amenaza e identificar los paquetes afectados y, a continuación, elimine los paquetes identificados mediante el administrador de paquetes adecuado para el sistema operativo. Tras la eliminación, realice un análisis para confirmar que no queda ningún componente malintencionado relacionado. Para obtener más información, consulte Microsoft Defender para servidores en la documentación de Microsoft Azure.

Cómo corregir las exposiciones de los contenedores de blobs de Azure Storage

AWS Security Hub puede generar datos de exposición para los contenedores de blobs de Azure Storage.

En la consola de Security Hub, el contenedor de blobs de Azure Storage implicado en la búsqueda de una exposición y su información de identificación aparecen en la sección Recursos de los detalles de la búsqueda. Puede recuperar los detalles de los recursos mediante programación mediante la API GetFindingsV2 CSPM de Security Hub.

Después de identificar el recurso involucrado en un resultado de exposición, puede eliminar el recurso si no lo necesita. Eliminar un recurso no esencial puede reducir su perfil de exposición y sus costos. AWS Si el recurso es esencial, siga estos pasos de remediación recomendados para ayudar a mitigar el riesgo. Los temas de remediación se dividen según el tipo de condición.

Un único resultado de exposición puede incluir problemas identificados en varios temas de remediación. También es posible abordar un resultado de exposición y disminuir su nivel de gravedad con solo tratar uno de los temas de remediación. El enfoque de remediación adecuado depende de los requisitos y cargas de trabajo de la organización.

> **Note**
>
> La guía de corrección que se proporciona en este tema puede requerir consultas adicionales en otros recursos de Microsoft Azure.

Contenido

- Características de accesibilidad de los contenedores de blobs de Azure Storage
  - La cuenta de almacenamiento permite el acceso anónimo a los blobs
- Características de configuración incorrecta de los contenedores de blobs de Azure Storage
  - La cuenta de almacenamiento no requiere HTTPS para las operaciones de transferencia
  - La cuenta de almacenamiento no está cifrada con claves administradas por el cliente
  - La cuenta de almacenamiento permite el acceso entre inquilinos
  - La cuenta de almacenamiento tiene deshabilitada la eliminación automática de blob
  - La cuenta de almacenamiento permite la eliminación permanente de los blobs que se han eliminado temporalmente
  - El contenedor de blobs de Azure Storage tiene deshabilitado el control de versiones de blobs

- El contenedor de almacenamiento no tiene una política de inmutabilidad

Características de accesibilidad de los contenedores de blobs de Azure Storage

Estas son las características de accesibilidad de los contenedores de blobs de Azure Storage y las medidas de corrección sugeridas.

La cuenta de almacenamiento permite el acceso anónimo a los blobs

Cuando el acceso de lectura anónimo está habilitado, los clientes no autenticados pueden leer los datos de los blobs sin autorización. Cuando la cuenta de almacenamiento permite el acceso anónimo (público) a los blobs y el nivel de acceso de un contenedor lo permite, cualquier usuario de la Internet pública puede leer los datos de ese contenedor. Siguiendo los principios de seguridad estándar, no permitas el acceso anónimo a nivel de cuenta y exige que se autoricen todas las solicitudes, a menos que tu situación dependa explícitamente del acceso de lectura pública.

Corrección

Tome una o más de las siguientes medidas para hacer frente a esta exposición:

No permita el acceso anónimo a la cuenta de almacenamiento

Establezca la `AllowBlobPublicAccess` propiedad de la cuenta de almacenamiento en`false`. Si no se permite el acceso anónimo a nivel de cuenta, se anula la configuración de acceso de todos los contenedores de la cuenta y se bloquean las futuras solicitudes anónimas. Para obtener más información, consulte Impedir el acceso de lectura anónima en la documentación de Microsoft Azure.

Establezca el nivel de acceso al contenedor como privado

Si los contenedores individuales se configuraron para el acceso público, defina el nivel de acceso anónimo de cada contenedor `Private` para que todas las solicitudes requieran autorización. Antes de cambiar la configuración, revise las aplicaciones cliente que puedan depender del acceso anónimo. Para obtener más información, consulte Configurar el acceso de lectura anónimo en la documentación de Microsoft Azure.

Características de configuración incorrecta de los contenedores de blobs de Azure Storage

Estas son las características de errores de configuración de los contenedores de blobs de Azure Storage y las medidas de corrección sugeridas.

La cuenta de almacenamiento no requiere HTTPS para las operaciones de transferencia

Cuando una cuenta de almacenamiento no requiere una transferencia segura, acepta solicitudes a través de HTTP sin cifrar. Los datos y las credenciales enviados a través de HTTP pueden ser interceptados o modificados en tránsito por un atacante en la ruta de la red. Siguiendo los principios de seguridad estándar, exige una transferencia segura para que la cuenta solo acepte solicitudes a través de HTTPS.

Corrección

Tome una o más de las siguientes medidas para hacer frente a esta exposición:

Exija una transferencia segura

Habilite la propiedad requerida para la transferencia segura en la cuenta de almacenamiento (la `enableHttpsTrafficOnly` propiedad). Cuando se requiere una transferencia segura, se rechaza cualquier solicitud realizada a través de HTTP. Para obtener más información, consulte Exigir una transferencia segura en la documentación de Microsoft Azure.

Aplicar una versión mínima de TLS

Establezca la versión TLS mínima de la cuenta de almacenamiento en 1.2 (la `minimumTlsVersion` propiedad) para que se rechacen las solicitudes que utilizan versiones de protocolo más antiguas y menos seguras. Confirme que sus clientes admiten TLS 1.2 antes de aplicar esta configuración. Para obtener más información, consulte Configurar la versión mínima de TLS para una cuenta de almacenamiento en la documentación de Microsoft Azure.

La cuenta de almacenamiento no está cifrada con claves administradas por el cliente

De forma predeterminada, Azure Storage cifra los datos en reposo con claves. Microsoft-managed Customer-managed las claves (CMK) le permiten controlar la clave que protege sus datos, incluida la posibilidad de rotar, revocar y auditar el acceso a la clave. Si los requisitos de cumplimiento de su organización exigen controlar las claves de cifrado, la ausencia de claves administradas por el cliente es un problema. Siguiendo las prácticas recomendadas de protección de datos, configure la cuenta de almacenamiento para usar las claves administradas por el cliente almacenadas en Azure Key Vault o en un HSM administrado.

Solución: configure las claves administradas por el cliente

Guarde una clave en Azure Key Vault o Azure Key Vault Managed HSM, con la protección de borrado y eliminación parcial habilitada. Otorgue la identidad administrada y `unwrapkey` los

permisos y `getwrapkey`, a continuación, configure la cuenta de almacenamiento para usar esa clave para el cifrado. Puedes cambiar entre las claves administradas por el cliente y Microsoft-managed las claves en cualquier momento. Para obtener más información, consulte Customer-managed las claves para el cifrado del almacenamiento en la documentación de Microsoft Azure.

La cuenta de almacenamiento permite el acceso entre inquilinos

Cross-tenant La configuración de acceso, como la replicación de objetos entre inquilinos o la delegación de firmas de acceso compartido (SAS) entre inquilinos, puede provocar que los datos abandonen el inquilino de Microsoft Entra propietario de la cuenta de almacenamiento. Si su carga de trabajo no requiere compartir datos entre inquilinos, si deja habilitada esta configuración, aumenta el riesgo de que los datos salgan del límite de inquilinos. Siguiendo los principios de seguridad estándar, desactiva el acceso entre inquilinos, a menos que sea obligatorio de forma explícita.

Solución: inhabilite la configuración de acceso entre inquilinos

En la cuenta de almacenamiento, deshabilite la replicación de objetos entre arrendatarios (establecida `allowCrossTenantReplication` en`false`) y, cuando sea posible, restrinja la delegación de SAS entre arrendatarios. Revise sus requisitos de replicación y uso compartido antes de realizar el cambio. Para obtener más información, consulte la descripción general de la cuenta de Azure Storage en la documentación de Microsoft Azure.

La cuenta de almacenamiento tiene deshabilitada la eliminación automática de blob

La eliminación gradual de blobs protege los blobs, las instantáneas y las versiones individuales contra la eliminación y la sobrescritura accidentales o malintencionadas. Conserva los datos eliminados durante un período de retención configurable, durante el cual puede restaurarlos. Cuando la eliminación parcial está desactivada, los datos de blob borrados o sobrescritos no se pueden recuperar, lo que expone a la cuenta a una pérdida permanente de datos. Siguiendo las prácticas recomendadas de protección de datos, habilita la eliminación gradual de blobs con un período de retención adecuado.

Solución: habilite la eliminación gradual de blob

Habilita la eliminación gradual de bloques en la cuenta de almacenamiento y establece un período de retención (de 1 a 365 días) que cumpla tus requisitos de recuperación. Para una protección más completa, habilita también la eliminación parcial de contenedores y el control de versiones de blobs. Para obtener más información, consulte la sección Eliminación parcial de blobs en la documentación de Microsoft Azure.

La cuenta de almacenamiento permite la eliminación permanente de los blobs que se han eliminado temporalmente

Cuando se permite la eliminación permanente (la `allowPermanentDelete` propiedad lo `estrue`), los blobs y las instantáneas eliminadas temporalmente se pueden eliminar antes de que expire el período de retención de la eliminación gradual. Esto debilita la protección que brinda la eliminación parcial, ya que un usuario o un responsable comprometido puede destruir permanentemente los datos recuperables antes de que expire el período de retención. Siguiendo las prácticas recomendadas en materia de protección de datos, no permitas la eliminación permanente de las manchas eliminadas temporalmente, a menos que tengas un requisito específico y bien entendido.

Solución: inhabilite la eliminación permanente

Establezca la `allowPermanentDelete` propiedad de la cuenta de almacenamiento para `false` que los blobs y las instantáneas eliminados temporalmente puedan recuperarse durante todo el período de retención. Para obtener más información, consulte la sección Eliminación parcial de blobs en la documentación de Microsoft Azure.

El contenedor de blobs de Azure Storage tiene deshabilitado el control de versiones de blobs

El control de versiones de blobs mantiene automáticamente las versiones anteriores de un blob. Cuando se modifica o elimina un blob, el estado anterior se conserva como una versión anterior que se puede restaurar. Cuando el control de versiones está deshabilitado, las sobrescrituras y eliminaciones no se pueden revertir a un estado anterior, lo que aumenta el riesgo de que los datos se pierdan o se dañen de forma irrecuperable. Si sigue las prácticas recomendadas de protección de datos, habilite el control de versiones de blobs junto con la eliminación parcial para lograr una protección óptima de los datos.

Solución: habilite el control de versiones de blobs

Habilite el control de versiones en el servicio de blobs de la cuenta de almacenamiento. Para controlar el costo de retener muchas versiones, utilice una política de administración del ciclo de vida para eliminar automáticamente las versiones antiguas. Para obtener más información, consulte el control de versiones de blobs en la documentación de Microsoft Azure.

El contenedor de almacenamiento no tiene una política de inmutabilidad

Una política de inmutabilidad almacena los datos de los blobs en un estado WORM (escritura única, lectura múltiple). En este estado, los datos no se pueden modificar ni eliminar durante un intervalo específico (una política de retención basada en el tiempo) ni hasta que se elimine la retención

legal. Sin una política de inmutabilidad, los datos críticos para la empresa o relevantes para el cumplimiento del contenedor se pueden sobrescribir o eliminar, incluso por parte de los usuarios con privilegios. Cuando se apliquen requisitos normativos o de integridad de los datos, configure una política de inmutabilidad para el contenedor.

Solución: configure una política de inmutabilidad

Configure una política de retención temporal o una retención legal del contenedor. Bloquee la política basada en el tiempo cuando finalicen las pruebas para que los datos estén completamente protegidos en estado WORM. Habilite la eliminación parcial antes de aplicar políticas de inmutabilidad para obtener una protección adicional. Para obtener más información, consulte Almacenamiento inmutable de datos de blobs en la documentación de Microsoft Azure.

Cómo corregir las exposiciones de las bases de datos SQL de Azure

AWS Security Hub puede generar hallazgos de exposición para las bases de datos SQL de Azure.

En la consola de Security Hub, la base de datos SQL de Azure implicada en un hallazgo de exposición y su información de identificación aparecen en la sección Recursos de los detalles del hallazgo. Puede recuperar los detalles de los recursos mediante programación mediante la API GetFindingsV2 CSPM de Security Hub.

Después de identificar el recurso involucrado en un resultado de exposición, puede eliminar el recurso si no lo necesita. Eliminar un recurso no esencial puede reducir su perfil de exposición y sus costos. AWS Si el recurso es esencial, siga estos pasos de remediación recomendados para ayudar a mitigar el riesgo. Los temas de remediación se dividen según el tipo de condición.

Un único resultado de exposición puede incluir problemas identificados en varios temas de remediación. También es posible abordar un resultado de exposición y disminuir su nivel de gravedad con solo tratar uno de los temas de remediación. El enfoque de remediación adecuado depende de los requisitos y cargas de trabajo de la organización.

> **Note**
>
> La guía de corrección que se proporciona en este tema puede requerir consultas adicionales en otros recursos de Microsoft Azure.

Contenido

- Características de configuración incorrecta de las bases de datos SQL de Azure
  - La base de datos SQL de Azure tiene habilitado el acceso a la red pública
  - La base de datos Azure SQL no exige la AD-only autenticación de Azure
  - La base de datos SQL de Azure usa un nombre de usuario de administrador común o predeterminado
  - La base de datos SQL de Azure tiene deshabilitada la copia de seguridad georedundante

Características de configuración incorrecta de las bases de datos SQL de Azure

Estas son las características de errores de configuración de las bases de datos SQL de Azure y las medidas de corrección sugeridas.

La base de datos SQL de Azure tiene habilitado el acceso a la red pública

Cuando el acceso a la red pública está habilitado en el servidor lógico, se puede acceder a la base de datos a través de un punto final público y puede aceptar conexiones desde la Internet pública (según las reglas del firewall). Un punto final público aumenta la superficie de ataque de la base de datos y la expone a intentos de conexión no autorizados. Siguiendo los principios de seguridad estándar, deshabilite el acceso a la red pública y conéctese a la base de datos de forma privada, o restrinja estrictamente las reglas del firewall del servidor.

Corrección

Tome una o más de las siguientes medidas para hacer frente a esta exposición:

Deshabilite el acceso a la red pública y utilice el enlace privado

Establezca el acceso a la red pública del servidor lógico `Disabled` y conéctese a la base de datos a través de un punto final privado (Azure Private Link) dentro de su red virtual. Esto mantiene el tráfico de la base de datos en la red troncal de Azure y fuera de la Internet pública. Para obtener más información, consulte los controles de acceso a la red para Azure SQL Database en la documentación de Microsoft Azure.

Restrinja las reglas de firewall si se requiere acceso público

Si debe mantener habilitado el acceso público, elimine cualquier regla que permita el acceso completo a Internet y desactive Permitir que los servicios y recursos de Azure accedan a este servidor cuando no sea necesario. Limite las reglas de firewall a nivel de servidor a las direcciones

IP de confianza específicas que necesite su carga de trabajo. Para obtener más información, consulte los controles de acceso a la red para Azure SQL Database en la documentación de Microsoft Azure.

Aplicar una versión mínima de TLS

Establezca la versión mínima de TLS del servidor lógico en 1.2 para que se rechacen las conexiones que utilizan versiones de protocolo más antiguas y menos seguras. Confirme que sus clientes admiten TLS 1.2 antes de aplicar esta configuración. Para obtener más información, consulte la configuración de conectividad de Azure SQL Database en la documentación de Microsoft Azure.

La base de datos Azure SQL no exige la AD-only autenticación de Azure

Cuando no se aplica la Entra-only autenticación de Microsoft (anteriormente denominada AD-only autenticación de Azure), el servidor lógico también acepta la autenticación de SQL, que se basa en las contraseñas almacenadas y administradas en la base de datos. La autenticación SQL es más susceptible al robo de credenciales y a los ataques de fuerza bruta, y no se beneficia de los controles centralizados de Microsoft Entra, como el acceso condicional y la autenticación multifactorial. Siguiendo los principios de seguridad estándar, aplique la Entra-only autenticación de Microsoft para que solo puedan conectarse las identidades de Microsoft Entra.

Solución: exija la autenticación de Microsoft Entra-only

Establezca un administrador de Microsoft Entra para el servidor lógico y, a continuación, habilite la Entra-only autenticación de Microsoft. Esto desactiva la autenticación de SQL para que solo las identidades de Microsoft Entra puedan conectarse al servidor y a sus bases de datos. Confirme que sus aplicaciones admiten la autenticación de Microsoft Entra antes de aplicar esta configuración. Para obtener más información, consulte la Entra-only autenticación de Microsoft en la documentación de Microsoft Azure.

La base de datos SQL de Azure usa un nombre de usuario de administrador común o predeterminado

El inicio de sesión de administrador del servidor lógico utiliza un nombre de usuario conocido o común`sqladmin`, como`admin`, `osa`. Los nombres de usuario de los administradores habituales son predecibles, lo que hace que el servidor sea un blanco más fácil para los ataques de fuerza bruta y de uso indebido de credenciales, ya que el atacante solo necesita adivinar la contraseña. Siguiendo los principios de seguridad estándar, evite los nombres de usuario de administrador comunes o predeterminados y centralice el acceso administrativo a través de Microsoft Entra ID.

Solución: utilice un administrador que no sea el predeterminado y utilice la autenticación Entra de Microsoft

Evite los nombres de inicio de sesión de administrador predecibles. Siempre que sea posible, aplique la Entra-only autenticación de Microsoft y gestione el acceso administrativo a través de las identidades y los grupos de Microsoft Entra, en lugar de mediante un inicio de sesión de administrador de SQL. Siga las prácticas recomendadas de seguridad de Azure SQL para administrar los inicios de sesión y el acceso con privilegios mínimos. Para obtener más información, consulte las prácticas recomendadas de seguridad de Azure SQL Database en la documentación de Microsoft Azure.

La base de datos SQL de Azure tiene deshabilitada la copia de seguridad georedundante

Azure SQL Database almacena las copias de seguridad automatizadas en un almacenamiento georredundante de forma predeterminada, que replica las copias de seguridad en una región emparejada y permite la restauración geográfica durante una interrupción regional. Cuando la redundancia del almacenamiento de copias de seguridad se establece en almacenamiento redundante localmente o redundante por zonas, la restauración geográfica no está disponible. No puede recuperar la base de datos en otra región si la región principal deja de estar disponible. Siguiendo las prácticas recomendadas de protección de datos, utilice un almacenamiento de respaldo con redundancia geográfica para las bases de datos que requieran resistir las interrupciones regionales.

Corrección

Tome una o más de las siguientes medidas para hacer frente a esta exposición:

Configure el almacenamiento de copias de seguridad con redundancia geográfica

Establezca la redundancia del almacenamiento de respaldo de la base de datos en almacenamiento georredundante (GRS) o almacenamiento redundante por zonas geográficas (GZRS) para que la restauración geográfica esté disponible. Los cambios se aplicarán a las copias de seguridad futuras y pueden tardar hasta 48 horas en surtir efecto. Para obtener más información, consulte Copias de seguridad automatizadas en Azure SQL Database en la documentación de Microsoft Azure.

Configure la retención a largo plazo

Para las bases de datos con requisitos de cumplimiento o recuperación a largo plazo, configure una política de retención a largo plazo (LTR). La LTR conserva las copias de seguridad completas

durante un máximo de 10 años, además de la retención predeterminada a corto plazo. Para obtener más información, consulte la Long-term retención en Azure SQL Database en la documentación de Microsoft Azure.

Cómo corregir las exposiciones de las cuentas de Azure Cosmos DB

AWS Security Hub puede generar datos de exposición para las cuentas de Azure Cosmos DB.

En la consola de Security Hub, la cuenta de Azure Cosmos DB implicada en la detección de una exposición y su información de identificación aparecen en la sección Recursos de los detalles de la búsqueda. Puede recuperar los detalles de los recursos mediante programación mediante la API GetFindingsV2 CSPM de Security Hub.

Después de identificar el recurso involucrado en un resultado de exposición, puede eliminar el recurso si no lo necesita. Eliminar un recurso no esencial puede reducir su perfil de exposición y sus costos. AWS Si el recurso es esencial, siga estos pasos de remediación recomendados para ayudar a mitigar el riesgo. Los temas de remediación se dividen según el tipo de condición.

Un único resultado de exposición puede incluir problemas identificados en varios temas de remediación. También es posible abordar un resultado de exposición y disminuir su nivel de gravedad con solo tratar uno de los temas de remediación. El enfoque de remediación adecuado depende de los requisitos y cargas de trabajo de la organización.

> **Note**
>
> La guía de corrección que se proporciona en este tema puede requerir consultas adicionales en otros recursos de Microsoft Azure.

Contenido

- Características de configuración incorrecta de las cuentas de Azure Cosmos DB
  - La cuenta Azure Cosmos DB tiene habilitado el acceso a la red pública
  - La cuenta Azure Cosmos DB no utiliza copias de seguridad continuas

Características de configuración incorrecta de las cuentas de Azure Cosmos DB

Estas son las características de configuración incorrecta de las cuentas de Azure Cosmos DB y las medidas de corrección sugeridas.

La cuenta Azure Cosmos DB tiene habilitado el acceso a la red pública

Cuando el acceso a la red pública está habilitado, se puede acceder a la cuenta de Azure Cosmos DB a través de un punto final público. Puede aceptar conexiones desde la Internet pública, con sujeción a las reglas del firewall y de la red virtual. Un punto final público aumenta la superficie de ataque de su cuenta y la expone a intentos de conexión no autorizados y a posibles filtraciones de datos. Siguiendo los principios de seguridad estándar, deshabilita el acceso a la red pública y conéctate a la cuenta de forma privada, o restringe estrictamente las reglas del firewall de la cuenta.

Corrección

Tome una o más de las siguientes medidas para hacer frente a esta exposición:

Deshabilite el acceso a la red pública y utilice el enlace privado

Establezca la `publicNetworkAccess` propiedad de la cuenta en un punto final privado (Azure Private Link) dentro de su red virtual `Disabled` y conéctese a través de él. Cuando se combinan con políticas grupales de seguridad de red restrictivas, los terminales privados ayudan a reducir el riesgo de filtración de datos. Para obtener más información, consulte Configurar Azure Private Link en la documentación de Microsoft Azure.

Restrinja las reglas de firewall si se requiere acceso público

Si debe mantener habilitado el acceso público, configure las reglas del firewall IP y las reglas de la red virtual para permitir solo las fuentes confiables específicas que requiere su carga de trabajo, en lugar de permitir todas las redes. Para obtener más información, consulte Configurar el firewall IP en la documentación de Microsoft Azure.

La cuenta Azure Cosmos DB no utiliza copias de seguridad continuas

Con el modo de copia de seguridad continua, puede usar la restauración puntual para recuperarse de una escritura o eliminación accidental. También puede restaurar una base de datos o un contenedor eliminados a cualquier fecha y hora dentro del período de retención. Cuando la cuenta utiliza el modo de copia de seguridad periódica en lugar de una copia de seguridad continua, no puede realizar una restauración puntual de autoservicio. Esta limitación aumenta el tiempo de recuperación y el riesgo de pérdida de datos tras un cambio accidental o malintencionado. Siguiendo las prácticas recomendadas de protección de datos, habilite el modo de respaldo continuo cuando su carga de trabajo lo permita.

Solución: habilite el modo de respaldo continuo

Configure la cuenta para usar el modo de respaldo continuo (nivel de 7 o 30 días), de modo que la restauración puntual esté disponible. Revise las limitaciones actuales y las API compatibles antes de migrar del respaldo periódico al continuo. Para obtener más información, consulte Copia de seguridad continua con restauración puntual en la documentación de Microsoft Azure.

Cómo corregir las exposiciones de las aplicaciones de Azure Function

AWS Security Hub puede generar datos de exposición para las aplicaciones de Azure Function.

En la consola de Security Hub, la aplicación Azure Function implicada en la detección de una exposición y su información de identificación aparecen en la sección Recursos de los detalles de la búsqueda. Puede recuperar los detalles de los recursos mediante programación mediante la API GetFindingsV2 CSPM de Security Hub.

Después de identificar el recurso involucrado en un resultado de exposición, puede eliminar el recurso si no lo necesita. Eliminar un recurso no esencial puede reducir su perfil de exposición y sus costos. AWS Si el recurso es esencial, siga estos pasos de remediación recomendados para ayudar a mitigar el riesgo. Los temas de remediación se dividen según el tipo de condición.

Un único resultado de exposición puede incluir problemas identificados en varios temas de remediación. También es posible abordar un resultado de exposición y disminuir su nivel de gravedad con solo tratar uno de los temas de remediación. El enfoque de remediación adecuado depende de los requisitos y cargas de trabajo de la organización.

> **Note**
>
> La guía de corrección que se proporciona en este tema puede requerir consultas adicionales en otros recursos de Microsoft Azure.

Contenido

- Características de configuración incorrecta de las aplicaciones de Azure Function
  - La aplicación Azure Function se implementa fuera de una red virtual
  - La función asociada a la aplicación Azure Function tiene una asignación de funciones de acceso administrativo
- Características de accesibilidad de las aplicaciones de Azure Function
  - La aplicación Azure Function permite la invocación anónima de activadores HTTP

- Características de vulnerabilidad de las aplicaciones de Azure Function
  - La aplicación Azure Function presenta vulnerabilidades de software que se pueden explotar en la red con una alta probabilidad de explotación
  - La aplicación Azure Function tiene vulnerabilidades de software
  - La aplicación Azure Function contiene paquetes de software malintencionado

Características de configuración incorrecta de las aplicaciones de Azure Function

Estas son las características de errores de configuración de las aplicaciones de Azure Function y las medidas de corrección sugeridas.

La aplicación Azure Function se implementa fuera de una red virtual

Cuando una aplicación Function no está integrada con una red virtual, sus puntos finales y su tráfico saliente atraviesan la red pública en lugar de atravesar los límites de la red privada. Cuando la aplicación Function no está integrada con una red virtual, no puede aplicar controles a nivel de red, como puntos finales privados, grupos de seguridad de red y acceso saliente restringido. Esta brecha aumenta la exposición de la aplicación. Siguiendo los principios de seguridad estándar, integre la aplicación Function con una red virtual y utilice terminales privados cuando su plan de alojamiento lo permita.

Corrección

Tome una o más de las siguientes medidas para hacer frente a esta exposición:

Integre la aplicación Function con una red virtual

Habilite la integración de redes virtuales para la aplicación Function. Cuando tu plan de alojamiento lo permita (Flex Consumption, Elastic Premium o Dedicated), usa terminales privados para que solo se pueda acceder a la aplicación desde tu red. Para obtener más información, consulte las opciones de red de Azure Functions en la documentación de Microsoft Azure.

Restrinja el acceso entrante

En los planes de alojamiento que no admiten terminales privados, usa restricciones de acceso para permitir el tráfico entrante únicamente desde rangos de direcciones IP confiables e inhabilita el acceso a la red pública cuando no sea necesario. Para obtener más información, consulta Cómo configurar las restricciones de acceso en la documentación de Microsoft Azure.

La función asociada a la aplicación Azure Function tiene una asignación de funciones de acceso administrativo

Puede asignar una identidad administrada a una aplicación Azure Function y asignarle funciones de control de acceso basado en roles (Azure RBAC) de Azure para acceder a otros recursos de Azure. Cuando la identidad asociada tiene una asignación de funciones administrativas (como `Owner` o`Contributor`) en un ámbito amplio, normalmente otorga permisos que van mucho más allá de lo que requiere la aplicación. Si la aplicación Function se ve comprometida, un atacante puede usar estos permisos excesivos para moverse lateralmente por el entorno, acceder a los datos o manipular los recursos. Siguiendo los principios de seguridad estándar, otorga el mínimo privilegio asignando solo los permisos que la aplicación necesita.

Corrección

Tome una o más de las siguientes medidas para hacer frente a esta exposición:

Revise e identifique las asignaciones de funciones administrativas

En el portal de Azure, revise las asignaciones de funciones para la identidad asociada a la aplicación Function. Busque funciones de administrador privilegiadas`Owner`, como`Contributor`, o`User Access Administrator`, y funciones personalizadas que usen un comodín (`*`) en sus `Actions` funciones. Para obtener más información, consulte Listar las asignaciones de funciones de Azure en la documentación de Microsoft Azure.

Implementación del acceso a los privilegios mínimos

Sustituya las asignaciones de funciones administrativas por la función integrada con menos privilegios, que solo conceda los permisos que requiere la aplicación, y asígnela según el ámbito más limitado que se adapte a sus necesidades. Use una identidad administrada en lugar de secretos almacenados para las conexiones a otros servicios de Azure. Para obtener más información, consulte las prácticas recomendadas para Azure RBAC en la documentación de Microsoft Azure.

Características de accesibilidad de las aplicaciones de Azure Function

Estas son las características de accesibilidad de las aplicaciones de Azure Function y las medidas de corrección sugeridas.

La aplicación Azure Function permite la invocación anónima de activadores HTTP

Una HTTP-triggered función cuyo nivel de autorización esté establecido en se `anonymous` puede invocar a través de Internet sin ninguna clave de acceso ni autenticación. Los activadores

HTTP anónimos exponen la lógica de la función a las llamadas no autenticadas, lo que puede provocar abusos, exposición de datos o denegación de acceso al monedero si se invoca de forma incontrolada. Siguiendo los principios de seguridad estándar, exige claves de autenticación o acceso para las funciones, a menos que se requiera explícitamente el acceso anónimo HTTP-triggered .

Corrección

Tome una o más de las siguientes medidas para hacer frente a esta exposición:

Exija autorización para los activadores HTTP

Aumente el nivel de autorización del activador HTTP de `anonymous` a `function` aproximadamente, de `admin` modo que las solicitudes incluyan una clave de acceso válida y requieran HTTPS. Para una protección más sólida, habilite el servicio de aplicaciones Authentication/Authorization o inicie la aplicación con Azure API Management. Para obtener más información, consulte Proteger Azure Functions en la documentación de Microsoft Azure.

Exija la autenticación con un proveedor de identidades administrado

Como las claves de acceso son un control de autorización y no una autenticación, habilite la autenticación mediante App Service (Easy Auth) con Microsoft Entra ID para que las personas que llamen tengan que presentar una identidad válida. Deshabilite también los puntos finales administrativos (las `/admin` rutas) cuando no los necesite. Para obtener más información, consulte Proteger Azure Functions en la documentación de Microsoft Azure.

Características de vulnerabilidad de las aplicaciones de Azure Function

Estas son las características de vulnerabilidad de las aplicaciones de Azure Function y las medidas de corrección sugeridas.

La aplicación Azure Function presenta vulnerabilidades de software que se pueden explotar en la red con una alta probabilidad de explotación

Las vulnerabilidades y exposiciones comunes (CVE) pueden afectar a los paquetes de software y las dependencias de la aplicación Function. Una vulnerabilidad de alta prioridad es la que se puede explotar en la red con una alta probabilidad de explotación, lo que representa una amenaza inmediata para la seguridad, ya que es posible que el código de explotación ya esté disponible públicamente y los atacantes lo utilicen activamente. Corrija estas vulnerabilidades con prontitud para proteger su aplicación Function.

Corrección

Tome una o más de las siguientes medidas para hacer frente a esta exposición:

Actualice las dependencias afectadas

Revisa las CVE afectadas del hallazgo y, a continuación, actualiza los paquetes y dependencias vulnerables a sus versiones seguras más recientes y vuelve a implementar la aplicación. Mantén la aplicación Function en un tiempo de ejecución compatible para que las actualizaciones de seguridad de la plataforma sigan aplicándose. Para obtener más información, consulte Microsoft Defender for App Service en la documentación de Microsoft Azure.

Consideraciones futuras

Para evitar que esto ocurra en el futuro, integra el análisis de dependencias y vulnerabilidades en tu proceso de creación e implementación, y usa Microsoft Defender for Cloud para supervisar la configuración y detectar vulnerabilidades en tu aplicación. Para obtener más información, consulta Microsoft Defender for App Service en la documentación de Microsoft Azure.

La aplicación Azure Function tiene vulnerabilidades de software

Las vulnerabilidades y exposiciones comunes (CVE) pueden afectar a los paquetes de software y las dependencias de la aplicación Function. Las vulnerabilidades no críticas representan debilidades de seguridad con menor gravedad o capacidad de explotación que las vulnerabilidades de alta prioridad. Si bien representan un riesgo menos inmediato, los atacantes pueden aprovechar las vulnerabilidades que no han sido reparadas para comprometer la confidencialidad, la integridad o la disponibilidad de los datos, o para acceder a otros sistemas. Siguiendo las prácticas recomendadas de seguridad, corrija estas vulnerabilidades para proteger tu aplicación Function.

Solución: actualice las dependencias afectadas

Actualice los paquetes y dependencias vulnerables a sus versiones seguras más recientes y vuelva a implementar la aplicación. Si no hay ninguna actualización disponible, considera la posibilidad de eliminar o deshabilitar el componente vulnerable hasta que se publique un parche. Para obtener más información, consulte Microsoft Defender for App Service en la documentación de Microsoft Azure.

La aplicación Azure Function contiene paquetes de software malintencionado

Los paquetes malintencionados son componentes de software que contienen código dañino diseñado para comprometer la confidencialidad, la integridad y la disponibilidad de los sistemas y los datos. Los paquetes malintencionados representan una amenaza activa y crítica para tu aplicación Function, ya que los atacantes pueden ejecutar el código malicioso automáticamente sin aprovechar

una vulnerabilidad independiente. Siguiendo las prácticas recomendadas de seguridad, elimina los paquetes maliciosos para proteger tu aplicación Function de posibles ataques.

Solución: Investiga y elimina los paquetes maliciosos

Revisa los detalles de los hallazgos para identificar los paquetes afectados, eliminarlos de las dependencias de tu proyecto, reconstruirlos a partir de una fuente confiable y volver a implementar la aplicación. Tras la corrección, audita la cadena de suministro de dependencias para confirmar que no queda ningún componente malintencionado relacionado. Para obtener más información, consulte Microsoft Defender for App Service en la documentación de Microsoft Azure.

Cómo corregir las exposiciones de las aplicaciones de Azure Container

AWS Security Hub puede generar datos de exposición para las aplicaciones de Azure Container.

En la consola de Security Hub, la aplicación Azure Container implicada en la detección de una exposición y su información de identificación aparecen en la sección Recursos de los detalles de la búsqueda. Puede recuperar los detalles de los recursos mediante programación mediante la API GetFindingsV2 CSPM de Security Hub.

Después de identificar el recurso involucrado en un resultado de exposición, puede eliminar el recurso si no lo necesita. Eliminar un recurso no esencial puede reducir su perfil de exposición y sus costos. AWS Si el recurso es esencial, siga estos pasos de remediación recomendados para ayudar a mitigar el riesgo. Los temas de remediación se dividen según el tipo de condición.

Un único resultado de exposición puede incluir problemas identificados en varios temas de remediación. También es posible abordar un resultado de exposición y disminuir su nivel de gravedad con solo tratar uno de los temas de remediación. El enfoque de remediación adecuado depende de los requisitos y cargas de trabajo de la organización.

> **Note**
>
> La guía de corrección que se proporciona en este tema puede requerir consultas adicionales en otros recursos de Microsoft Azure.

Contenido

- Características de configuración incorrecta de las aplicaciones de Azure Container
  - La aplicación Azure Container tiene credenciales de texto sin cifrar en las variables de entorno

- La aplicación Azure Container tiene un grupo de seguridad de red abierto
- La aplicación Azure Container tiene una identidad administrada que no tiene el mínimo privilegio
- La función asociada a la aplicación Azure Container tiene una asignación de funciones de acceso administrativo
- Características de accesibilidad de las aplicaciones de Azure Container
  - Se puede acceder a la aplicación Azure Container a través de Internet

Características de configuración incorrecta de las aplicaciones de Azure Container

Estas son las características de configuración incorrecta de las aplicaciones de Azure Container y las medidas de corrección sugeridas.

La aplicación Azure Container tiene credenciales de texto sin cifrar en las variables de entorno

La aplicación Container transfiere datos secretos, como cadenas de conexión, claves de API o contraseñas, al contenedor como variables de entorno de texto sin formato. La configuración, los registros o un contenedor comprometido pueden exponer las credenciales en texto sin cifrar en las variables de entorno, lo que permite a un atacante reutilizarlas para acceder a otros sistemas. Siguiendo los principios de seguridad estándar, almacene los valores confidenciales como secretos y haga referencia a ellos en lugar de incluirlos en texto plano.

Corrección

Tome una o más de las siguientes medidas para hacer frente a esta exposición:

Transfiera las credenciales a secretos

Sustituya los valores de las variables de entorno en texto plano por los secretos de las aplicaciones de contenedor o haga referencia a los secretos almacenados en Azure Key Vault. Actualice el contenedor para leer los valores de esas referencias secretas. Cambie cualquier credencial que haya estado expuesta anteriormente en texto plano. Para obtener más información, consulte Administrar secretos en Azure Container Apps en la documentación de Microsoft Azure.

Utilice una identidad gestionada siempre que sea posible

Para las conexiones a los servicios de Azure que la admiten, usa la identidad administrada de la aplicación Container en lugar de almacenar un secreto. Para obtener más información, consulte Identidades administradas en Azure Container Apps en la documentación de Microsoft Azure.

La aplicación Azure Container tiene un grupo de seguridad de red abierto

El grupo de seguridad de red que protege el entorno de la aplicación Container contiene reglas que permiten el acceso sin restricciones desde cualquier fuente (por ejemplo, una fuente de `Any` o`0.0.0.0/0`). Un grupo de seguridad de red abierto expone el entorno de la aplicación Container al acceso no autorizado desde Internet. Siguiendo los principios de seguridad estándar, restrinja las reglas de los grupos de seguridad de red únicamente a las direcciones IP, los puertos y los protocolos específicos que requiere su carga de trabajo.

Corrección

Tome una o más de las siguientes medidas para hacer frente a esta exposición:

Restrinja las reglas de los grupos de seguridad

Revisa el grupo de seguridad de red asociado a la subred del entorno de la aplicación Container y modifica o elimina las reglas que permiten el acceso sin restricciones. Sustituya una fuente amplia, por ejemplo, por `Any` los rangos de confianza específicos que requiere su carga de trabajo. Para obtener más información, consulte Redes en Azure Container Apps en la documentación de Microsoft Azure.

Configure las restricciones de entrada de IP

Además de las reglas de los grupos de seguridad de red en la subred del entorno, configure las restricciones de entrada de IP en la propia aplicación contenedora para permitir o denegar el tráfico entrante por rango de direcciones IP. Para obtener más información, consulte Configurar las restricciones de entrada de IP en Azure Container Apps en la documentación de Microsoft Azure.

La aplicación Azure Container tiene una identidad administrada que no tiene el mínimo privilegio

La aplicación Container tiene una identidad administrada a la que se le otorga más acceso del que requiere la carga de trabajo. Una identidad gestionada con privilegios excesivos amplía el radio de ataque si la aplicación Container se ve comprometida, ya que un atacante puede actuar con todos los permisos de la identidad. Siguiendo los principios de seguridad estándar, concede a la identidad solo los permisos que necesita la carga de trabajo, en el ámbito más limitado posible.

Solución: defina la identidad gestionada con el mínimo privilegio

Revisa las asignaciones de funciones concedidas a la identidad gestionada de la aplicación Container y elimina las que no sean obligatorias. Asigne el rol integrado con menos privilegios al ámbito más limitado (recurso o grupo de recursos) que se adapte a sus necesidades. Para obtener

más información, consulte las prácticas recomendadas para Azure RBAC en la documentación de Microsoft Azure.

La función asociada a la aplicación Azure Container tiene una asignación de funciones de acceso administrativo

La identidad administrada asociada a la aplicación Container tiene una asignación de funciones administrativas (como `Owner` o`Contributor`) en un ámbito amplio. Esta asignación normalmente otorga permisos mucho más allá de lo que requiere la carga de trabajo. Si la aplicación Container se ve comprometida, un atacante puede usar estos permisos excesivos para moverse lateralmente por el entorno, acceder a los datos o manipular los recursos. Siguiendo los principios de seguridad estándar, otorga el mínimo privilegio asignando solo los permisos que la aplicación necesita.

Corrección

Tome una o más de las siguientes medidas para hacer frente a esta exposición:

Revise e identifique las asignaciones de funciones administrativas

En el portal de Azure, revise las asignaciones de funciones de la identidad asociada a la aplicación Container. Busque funciones de administrador privilegiadas`Owner`, como`Contributor`, o`User Access Administrator`, y funciones personalizadas que usen un comodín (`*`) en sus `Actions` funciones. Para obtener más información, consulte Listar las asignaciones de funciones de Azure en la documentación de Microsoft Azure.

Implementación del acceso a los privilegios mínimos

Sustituya las asignaciones de funciones administrativas por la función integrada con menos privilegios, que solo conceda los permisos que requiere la aplicación, y asígnela según el ámbito más limitado que se adapte a sus necesidades. Para obtener más información, consulte las prácticas recomendadas para Azure RBAC en la documentación de Microsoft Azure.

Características de accesibilidad de las aplicaciones de Azure Container

Estas son las características de accesibilidad de las aplicaciones de Azure Container y las medidas de corrección sugeridas.

Se puede acceder a la aplicación Azure Container a través de Internet

Se puede acceder a la aplicación Container desde la Internet pública, ya sea porque la entrada externa está habilitada (`ingress.external`está configurada en`true`) o porque su entorno tiene una dirección IP pública. La accesibilidad pública aumenta la superficie de ataque de la aplicación

Container y la expone a solicitudes no autorizadas. Siguiendo los principios de seguridad estándar, deshabilita la entrada externa cuando no sea necesaria, usa un entorno interno o coloca la aplicación detrás de un punto de entrada controlado y autenticado.

Corrección

Tome una o más de las siguientes medidas para hacer frente a esta exposición:

Restrinja o elimine la entrada externa

Configure el ingreso como interno si solo es necesario acceder a la aplicación desde su red o entorno virtual. Si se requiere acceso público, restrinja el acceso con restricciones de IP de entrada. Delante la aplicación con una puerta de enlace como Azure Application Gateway o Azure Front Door.

Estas pasarelas proporcionan autenticación y un firewall para aplicaciones web. Para obtener más información, consulte Ingress in Azure Container Apps en la documentación de Microsoft Azure.

Utilice un entorno interno

Para evitar asignar una dirección IP pública, implemente la aplicación Container en un entorno interno (integrado en la red virtual) que utilice una dirección IP privada y exponga solo los puntos finales que deben ser públicos a través de un punto de entrada controlado. Para obtener más información, consulte Redes en Azure Container Apps en la documentación de Microsoft Azure.

Exija HTTPS y autenticación para el acceso público

Cuando la entrada deba permanecer pública, deshabilite las conexiones inseguras (configuradas en`false`) `allowInsecure` para que el tráfico solo se distribuya a través de HTTPS. Activa la función de autenticación integrada con Microsoft Entra ID para que se rechacen las solicitudes no autenticadas. Para obtener más información, consulte Autenticación y autorización en Azure Container Apps en la documentación de Microsoft Azure.

Cómo corregir las exposiciones de los clústeres de Azure Kubernetes Service

AWS Security Hub puede generar datos de exposición para los clústeres de Azure Kubernetes Service (AKS).

En la consola de Security Hub, el clúster de AKS implicado en una búsqueda de exposición y su información de identificación aparecen en la sección Recursos de los detalles de la búsqueda. Mediante programación, puede recuperar los detalles de los recursos utilizando la API GetFindingsV2 CSPM de Security Hub.

Después de identificar el recurso involucrado en un resultado de exposición, puede eliminar el recurso si no lo necesita. Eliminar un recurso no esencial puede reducir su perfil de exposición y sus costos. AWS Si el recurso es esencial, siga estos pasos de remediación recomendados para ayudar a mitigar el riesgo. Los temas de remediación se dividen según el tipo de condición.

Un único resultado de exposición puede incluir problemas identificados en varios temas de remediación. También es posible abordar un resultado de exposición y disminuir su nivel de gravedad con solo tratar uno de los temas de remediación. El enfoque de remediación adecuado depende de los requisitos y cargas de trabajo de la organización.

> **Note**
>
> La guía de corrección que se proporciona en este tema puede requerir consultas adicionales en otros recursos de Microsoft Azure.

Contenido

- Características de configuración incorrecta de los clústeres de Azure Kubernetes Service
  - El clúster de Azure Kubernetes Service ejecuta una versión de Kubernetes no compatible
  - El clúster de Azure Kubernetes Service tiene secretos de Kubernetes sin cifrar
- Características de accesibilidad de los clústeres de Azure Kubernetes Service
  - El clúster de Azure Kubernetes Service permite el acceso público

Características de configuración incorrecta de los clústeres de Azure Kubernetes Service

Estas son las características de configuración incorrecta de los clústeres de Azure Kubernetes Service y las medidas de corrección sugeridas.

El clúster de Azure Kubernetes Service ejecuta una versión de Kubernetes no compatible

El clúster de AKS ejecuta una versión de Kubernetes que Microsoft ya no admite. Las versiones de Kubernetes que no son compatibles dejan de recibir parches de seguridad y correcciones de errores, lo que deja sin resolver las vulnerabilidades conocidas en el plano de control y en los componentes del nodo y expone al clúster a los ataques. Siguiendo las prácticas recomendadas de seguridad, mantén el clúster en una versión de Kubernetes compatible.

Solución: actualice a una versión de Kubernetes compatible

Actualiza el plano de control del clúster y los grupos de nodos a una versión de Kubernetes compatible. Como las versiones secundarias no se pueden omitir, actualice de forma secuencial cada versión secundaria y aplique el parche más reciente. Revisa los cambios más importantes de cada versión antes de actualizarla.

Considere la posibilidad de habilitar las actualizaciones automáticas para mantenerse actualizadas. Para obtener más información, consulte las versiones de Kubernetes compatibles en AKS en la documentación de Microsoft Azure.

El clúster de Azure Kubernetes Service tiene secretos de Kubernetes sin cifrar

De forma predeterminada, el clúster almacena los secretos de Kubernetes en el almacén de datos etcd sin cifrarlos mediante una clave controlada por el cliente. Sin el cifrado inactivo mediante un servicio de administración de claves, cualquier persona que acceda a los datos de etcd subyacentes puede leer valores secretos confidenciales, como las credenciales y los tokens. Siguiendo las prácticas recomendadas de protección de datos, habilite el cifrado etcd de KMS para que los secretos de Kubernetes se cifre en reposo con una clave en Azure Key Vault.

Corrección

Tome una o más de las siguientes medidas para hacer frente a esta exposición:

Habilite el cifrado KMS, etc.

Configure el clúster para que utilice el cifrado etcd del Servicio de administración de claves (KMS) con una clave almacenada en Azure Key Vault. Otorgue al clúster permisos para cifrar y descifrar la identidad del clúster sobre la clave. Re-encrypt los secretos existentes después de habilitar la función. Activa la protección de borrado y eliminación parcial en el almacén de claves para que la clave no se pierda. Para obtener más información, consulte el cifrado KMS etcd en AKS en la documentación de Microsoft Azure.

Habilite la protección de eliminación parcial y purga en el almacén de claves para que la clave no se pierda. Para obtener más información, consulte el cifrado KMS etcd en AKS en la documentación de Microsoft Azure.

Almacene los secretos en Azure Key Vault

Para evitar almacenar valores confidenciales como secretos de Kubernetes en etcd, utilice el proveedor Azure Key Vault para el controlador CSI de Secrets Store para montar los secretos, las claves y los certificados de Azure Key Vault en pods durante el tiempo de ejecución. Para obtener

más información, consulte el proveedor de Azure Key Vault para el controlador CSI de Secrets Store en la documentación de Microsoft Azure.

Características de accesibilidad de los clústeres de Azure Kubernetes Service

Estas son las características de accesibilidad de los clústeres de Azure Kubernetes Service y las medidas de corrección sugeridas.

El clúster de Azure Kubernetes Service permite el acceso público

El servidor de API es el punto final que usas para comunicarte con el plano de control de Kubernetes del clúster. Se puede acceder al clúster desde Internet cuando el punto final del servidor de API es público o cuando las cargas de trabajo están expuestas a través de un balanceador de cargas público o una entrada. Los terminales públicos aumentan la superficie de ataque y el riesgo de acceso no autorizado a tu servidor de API de Kubernetes. Es posible que los atacantes accedan a los recursos del clúster o los modifiquen y lean datos confidenciales. Siguiendo las prácticas recomendadas de seguridad, restringe el acceso al servidor de API y a las cargas de trabajo del clúster únicamente a los rangos de IP necesarios.

Corrección

Toma una o más de las siguientes medidas para hacer frente a esta exposición:

Restrinja el acceso al servidor de API

Utilice un clúster privado para que solo se pueda acceder al servidor de API desde su red virtual o configure intervalos de IP autorizados para limitar las direcciones de origen que pueden llegar al punto final del servidor de API público. Para obtener más información, consulte los clústeres privados de Azure Kubernetes Service en la documentación de Microsoft Azure.

Limite la exposición pública de las cargas de trabajo

Revise los servicios expuestos a través de los balanceadores de cargas públicos o la entrada, y restrinja o elimine la exposición pública cuando no sea necesaria. Usa balanceadores de carga internos, reglas de grupos de seguridad de red y un firewall de aplicaciones web en un punto de entrada controlado para las cargas de trabajo a las que se debe acceder desde Internet. Para obtener más información, consulte Conceptos de red para AKS en la documentación de Microsoft Azure.

Cómo corregir las exposiciones de los usuarios de Azure Graph

AWS Security Hub puede generar hallazgos de exposición para los usuarios de Azure Graph.

En la consola de Security Hub, el usuario de Azure Graph implicado en una búsqueda de exposición y su información de identificación aparecen en la sección Recursos de los detalles de la búsqueda. Puede recuperar los detalles de los recursos mediante programación mediante la API GetFindingsV2 CSPM de Security Hub.

Después de identificar el recurso involucrado en un resultado de exposición, puede eliminar el recurso si no lo necesita. Eliminar un recurso no esencial puede reducir su perfil de exposición y sus costos. AWS Si el recurso es esencial, siga estos pasos de remediación recomendados para ayudar a mitigar el riesgo. Los temas de remediación se dividen según el tipo de condición.

Un único resultado de exposición puede incluir problemas identificados en varios temas de remediación. También es posible abordar un resultado de exposición y disminuir su nivel de gravedad con solo tratar uno de los temas de remediación. El enfoque de remediación adecuado depende de los requisitos y cargas de trabajo de la organización.

> **Note**
>
> La guía de corrección que se proporciona en este tema puede requerir consultas adicionales en otros recursos de Microsoft Azure.

Contenido

- Características de configuración incorrecta para los usuarios de Azure Graph
  - La función asociada al usuario de Azure Graph tiene una asignación de funciones de acceso administrativo
  - El usuario de Azure Graph no tiene habilitada la MFA

Características de configuración incorrecta para los usuarios de Azure Graph

Estas son las características de los errores de configuración para los usuarios de Azure Graph y las medidas de corrección sugeridas.

La función asociada al usuario de Azure Graph tiene una asignación de funciones de acceso administrativo

El usuario de Azure Graph tiene una asignación de funciones administrativas de control de acceso basado en roles de Azure (Azure RBAC), como`Owner`, `Contributor` o. `User Access Administrator` La asignación suele tener un alcance amplio, como una suscripción o un grupo

de administración. Las asignaciones de funciones administrativas otorgan permisos amplios, de modo que un atacante puede usar una cuenta de usuario comprometida para moverse lateralmente, acceder a los datos o manipular los recursos en todo el entorno. Siguiendo los principios de seguridad estándar, conceda los privilegios mínimos y limite las asignaciones de funciones de administrador con privilegios.

Corrección

Tome una o más de las siguientes medidas para hacer frente a esta exposición:

Revise e identifique las asignaciones de funciones administrativas

En el portal de Azure, revise las asignaciones de funciones del usuario. Busque funciones de administrador con privilegios`Owner`, como`Contributor`, o`User Access Administrator`, y funciones personalizadas que utilicen un comodín (`*`) en sus `Actions` funciones. Para obtener más información, consulte Listar las asignaciones de funciones de Azure en la documentación de Microsoft Azure.

Implementación del acceso a los privilegios mínimos

Elimine las asignaciones de funciones privilegiadas innecesarias y sustitúyalas por la función integrada con menos privilegios, asignada en el ámbito más limitado posible. Prefiera los roles de función laboral a los roles de administrador con privilegios. Mantenga el número de propietarios de suscripciones al mínimo; Microsoft recomienda no más de tres.

Asigne funciones a grupos en lugar de a usuarios individuales. Utilice Microsoft Entra Privileged Identity Management para que las funciones privilegiadas puedan activarse justo a tiempo y en un plazo determinado, en lugar de conceder un acceso permanente. Para obtener más información, consulte las prácticas recomendadas para Azure RBAC en la documentación de Microsoft Azure.

El usuario de Azure Graph no tiene habilitada la MFA

El usuario de Azure Graph puede iniciar sesión de forma interactiva sin la autenticación multifactor (MFA). Sin la MFA, una cuenta solo está protegida por una contraseña, lo que la hace vulnerable a los ataques de suplantación de identidad, ocultación de contraseñas y robo de credenciales. Una única contraseña comprometida es suficiente para que un atacante pueda iniciar sesión. Siguiendo los principios de seguridad estándar, exija la MFA para todos los usuarios que tengan un inicio de sesión interactivo.

Solución: Exija la autenticación multifactorial

Exija la MFA para el usuario mediante una política de acceso condicional de Microsoft Entra. Para obtener una cobertura amplia, habilite los valores predeterminados de seguridad o una política de acceso condicional que exija la autenticación multifactor para todos los usuarios. Priorice una política dedicada para los administradores.

Siempre que sea posible, exige métodos resistentes a la suplantación de identidad (como las claves de seguridad FIDO2, las claves de acceso o Windows Hello for Business) mediante una autenticación de acceso condicional. Evite permitir métodos fraudulentos, como los SMS o la voz. Para obtener más información, consulte Planear una implementación de autenticación multifactorial en la documentación de Microsoft Azure.

Comprender los hallazgos de acceso no utilizados en Security Hub

Security Hub usa IAM Access Analyzer para identificar los permisos, las funciones, las claves de acceso y las contraseñas de IAM no utilizados en su cuenta. Estas conclusiones le ayudan a implementar la mejor práctica de seguridad consistente en el acceso con privilegios mínimos, ya que destacan los principios y permisos de IAM que no se utilizan activamente. Esta capacidad se ofrece a todos los clientes de Security Hub sin coste adicional.

Cómo funciona el análisis de acceso no utilizado

Cuando habilitas Security Hub, el servicio crea automáticamente un IAM Access Analyzer vinculado a un servicio en tu cuenta. Este analizador evalúa todos los principales de IAM (funciones y usuarios) comparándolos con los datos de AWS CloudTrail actividad para determinar cuáles son los principales y los permisos que no se han utilizado en un período retrospectivo de 90 días. El período retrospectivo no se puede configurar.

IAM Access Analyzer vuelve a evaluar todos los hallazgos activos cada 24 horas. Cuando se activa un principal o permiso no utilizado anteriormente, el hallazgo correspondiente se resuelve automáticamente.

El analizador de acceso no utilizado funciona en el este de EE. UU. (Virginia del Norte) porque IAM es un servicio global. Security Hub replica los resultados en todas las regiones en las que haya activado Security Hub. No es necesario que habilite Security Hub en EE. UU. Este (Virginia del Norte) para que el analizador funcione.

Tipos de búsqueda de acceso no utilizados

Security Hub genera cuatro tipos de hallazgos de acceso no utilizados:

Tipo de resultado	Description (Descripción)	Recurso evaluado
Función de IAM no utilizada	Una función de IAM que no se ha asumido en el período retrospectivo de 90 días.	rol de IAM
UnusedIAM UserAccessKey	Una clave de acceso de usuario de IAM que no se ha utilizado para firmar solicitudes de API durante el período retrospectivo de 90 días.	Usuario de IAM
UnusedIAM UserPassword	Una contraseña de usuario de IAM que no se ha utilizado para iniciar sesión en la consola durante el período retrospectivo de 90 días.	Usuario de IAM
UnusedPermission	Acciones específicas de IAM que se otorgan a un rol o usuario pero que no se han invocado en el período retrospectivo de 90 días.	Rol de IAM o usuario de IAM

Service-linked analizador

El analizador de acceso de IAM que crea Security Hub es un analizador vinculado a servicios. Puede verlo en la consola de IAM Access Analyzer, pero no puede modificarlo ni eliminarlo mientras Security Hub esté habilitado.

Al deshabilitar Security Hub en todas las regiones, el analizador vinculado al servicio se elimina automáticamente. Si la eliminación automática falla, puede eliminar el analizador llamando a la operación de la API de IAM Access Analyzer. `DeleteServiceLinkedAnalyzer` Esta operación solo se realiza correctamente después de que Security Hub esté completamente inhabilitado para su cuenta.

El analizador vinculado a servicios es independiente de cualquier analizador gestionado por el cliente que haya creado de forma independiente en IAM Access Analyzer. La creación o eliminación de analizadores gestionados por el cliente no afecta al analizador vinculado al servicio y viceversa.

Visualización de los resultados de acceso no utilizados

Los hallazgos de acceso no utilizados aparecen en la consola de Security Hub junto con otros hallazgos de Security Hub. Puede filtrar los hallazgos por tipo para ver solo los hallazgos de acceso

no utilizados. Los resultados de acceso no utilizados se formatean en el marco del esquema abierto de ciberseguridad (OCSF), el mismo formato que utilizan todos los hallazgos de Security Hub.

En el caso de las UnusedPermission conclusiones, si eliminas algunos permisos no utilizados de la política excesivamente permisiva, pero no todos, Security Hub cierra la conclusión existente y crea una nueva para la política revisada si sigue siendo demasiado permisiva.

También se puede acceder a los datos de acceso no utilizados desde la consola de IAM Access Analyzer. Los datos de acceso no utilizados de la consola de IAM Access Analyzer son de solo lectura y solo están visibles en la región de EE. UU. Este (Virginia del Norte).

El acceso no utilizado aparece en los resultados de exposición

La información de acceso no utilizada puede aparecer como características contextuales en las conclusiones de exposición de Security Hub. Cuando una función de IAM asociada a un recurso tiene permisos no utilizados, el resultado de la exposición los incluye como contexto complementario. Esto le ayuda a comprender el alcance potencial de una vulnerabilidad: un recurso con una función de IAM con privilegios excesivos presenta un riesgo mayor que uno con permisos con privilegios mínimos.

Los siguientes tipos de recursos pueden mostrar características contextuales del acceso no utilizado en sus resultados de exposición:

- Instancias de Amazon Elastic Compute Cloud
- AWS Lambda funciones
- Servicios de Amazon Elastic Container Service
- Clústeres de Amazon Elastic Kubernetes Service
- Usuarios de IAM (directamente)

Para obtener más información sobre los hallazgos de exposición, consulte Resultados de exposición en Security Hub.

Recomendaciones de políticas para los permisos no utilizados

Para obtener UnusedPermission información, Security Hub puede generar recomendaciones de políticas con privilegios mínimos. Estas recomendaciones le muestran una política de reemplazo limitada que conserva solo los permisos que su director realmente usa. Para obtener más

información, consulte Generación de recomendaciones de políticas para los hallazgos de acceso no utilizados.

Precios

El IAM Access Analyzer, vinculado a un servicio, se proporciona a todos los clientes de Security Hub sin costo adicional. No se le cobrará por separado por el analizador ni por los datos de acceso no utilizados.

Generación de recomendaciones de políticas para los hallazgos de acceso no utilizados

En el caso de los permisos no utilizados, Security Hub puede generar recomendaciones de políticas con privilegios mínimos que muestren una política de reemplazo con un alcance limitado. La recomendación evalúa cada política asociada al principal de IAM y genera una política de reemplazo que conserva solo los permisos que el principal ha utilizado realmente. Esta capacidad se proporciona a todos los clientes de Security Hub sin costo adicional.

Cómo funcionan las recomendaciones de políticas

La generación de recomendaciones de políticas es una operación asincrónica. Para generar y recuperar una recomendación:

1. Recupere los permisos no utilizados encontrados en Security Hub mediante la operación de la `GetFindingsV2` API. Observe el `metadata.uid` campo de la búsqueda.
2. Llame `GenerateRecommendedPolicyV2` con el hallazgo`metadata.uid`. Esto inicia la generación de recomendaciones, que normalmente se completa en 20 segundos.
3. Sondea `GetRecommendedPolicyV2` con lo mismo `metadata.uid` hasta que aparezca el `status` campo. `SUCCEEDED`
4. La respuesta contiene uno o más pasos de recomendación. Cada paso especifica uno `recommendedAction` de `CREATE_POLICY` (crear y adjuntar una política de reemplazo con un alcance reducido) o `DETACH_POLICY` (separar la política original con privilegios excesivos). En el caso de `CREATE_POLICY` los pasos, la respuesta incluye tanto el `existingPolicy` JSON como el JSON para que puedas `recommendedPolicy` compararlos.

Debes llamar `GenerateRecommendedPolicyV2` antes de llamar `GetRecommendedPolicyV2` si no se ha generado previamente una recomendación para esa búsqueda.

¿Quién puede generar recomendaciones

Tanto el propietario de la cuenta como los administradores delegados pueden llamar a estas operaciones de API:

- Los propietarios de cuentas pueden generar y ver recomendaciones sobre los permisos no utilizados encontrados en su propia cuenta.
- Los administradores delegados pueden generar y ver recomendaciones sobre los permisos no utilizados de cualquier cuenta de miembro en su organización.

Si no eres un administrador delegado y la búsqueda pertenece a otra cuenta, la operación de la API devuelve un `AccessDeniedException` error.

Ciclo vital de recomendaciones

- Las recomendaciones se almacenan en caché durante 90 días y permanecen disponibles mientras la búsqueda esté activa (no cerrada). Sin embargo, si se llama `GenerateRecommendedPolicyV2` varias veces, se invalida la caché y se inicia un nuevo trabajo que reemplaza la política almacenada en caché. Llame `GenerateRecommendedPolicyV2` solo una vez por búsqueda.
- La recomendación sigue un patrón de separar y adjuntar. No modifica las políticas de IAM existentes. Revisa la política recomendada y la aplica manualmente en la consola de IAM o mediante la API de IAM.
- Si el resultado se resuelve (por ejemplo, porque ahora se utilizan los permisos que antes no se utilizaban), la recomendación ya no estará disponible.

Casos de error

Las operaciones de la API devuelven errores en las siguientes situaciones:

- Se ha resuelto el problema `InvalidInputException` (HTTP 400).
- La búsqueda no es una búsqueda de permisos no utilizados `InvalidInputException` (HTTP 400).
- El principal de IAM se creó mediante el conjunto de permisos del Centro de identidad de IAM. Las políticas relativas a los principales conjuntos de permisos no se pueden modificar directamente. La recomendación devuelve un `FAILED` estado con una explicación.

- La persona que llama no es un administrador delegado y el hallazgo pertenece a otra cuenta `AccessDeniedException` (HTTP 403).
- Aún no se ha generado ninguna recomendación y llamas `GetRecommendedPolicyV2` sin llamar `GenerateRecommendedPolicyV2` primero `ResourceNotFoundException` (HTTP 404).

Uso de la consola

En la consola de Security Hub, puede generar una recomendación de políticas consultando la búsqueda de permisos no utilizados y seleccionando la pestaña Corrección. La consola muestra un indicador de carga mientras se crea la recomendación. Cuando la recomendación esté lista, puedes elegir la opción Vista previa para ver una comparación entre tu política actual y la política sustitutiva con menos privilegios recomendada. Puedes copiar la política recomendada en formato JSON.

Referencia de la API

- GenerateRecommendedPolicyV2— Inicia la generación asincrónica de una recomendación de política de privilegios mínimos para la búsqueda de permisos no utilizados. Toma los hallazgos como entrada. `metadata.uid` Devuelve HTTP 200 con un cuerpo vacío en caso de éxito.
- GetRecommendedPolicyV2— Recupera la recomendación de política generada. Toma los hallazgos `metadata.uid` como entrada. Soporta la paginación con `maxResults` (1—100) y `nextToken` parámetros. Devuelve el estado de la recomendación (`IN_PROGRESS`,`SUCCEEDED`, o`FAILED`), los pasos de la recomendación, el ARN del recurso y cualquier error.

Para obtener documentación detallada sobre la API, consulte la referencia de la API de Security Hub.

Escaneo de red en Security Hub

El escaneo de red es una función opcional de Security Hub que realiza pruebas de accesibilidad de red activas en sus recursos en la nube. Control-plane El análisis evalúa los grupos de seguridad, las listas de control de acceso a la red (NACL) y las tablas de rutas para determinar a qué se puede acceder. El escaneo de red va más allá al detectar lo que es realmente accesible. Examina sus recursos externos a sus cuentas para identificar los puertos abiertos y los servicios en ejecución.

Todos los escaneos se originan en direcciones IP AWS propias y responden a dos preguntas: ¿Se puede acceder a este recurso desde Internet? Si se puede acceder a él, ¿qué se está ejecutando?

Network Scanning publica los resultados como hallazgos independientes de OCSF en Security Hub con pruebas escaneadas.

Tipos de recursos admitidos

Network Scanning admite los siguientes tipos de recursos.

Proveedor de servicios en la nube	Tipo de recurso
AWS	Instancia EC2 (con IP pública)
AWS	IP elástica (EIP)
AWS	Balanceador de carga de red (NLB)
AWS	Balanceador de carga de aplicaciones (ALB)
AWS	Balanceador de carga clásico (CLB)
Azure	Dirección IP pública

> **Note**
>
> El escaneo de red escanea cada tipo de recurso de forma independiente. En el caso de los balanceadores de carga, el escaneo de red resuelve y escanea el nombre DNS. El escaneo de red solo analiza las instancias EC2 individuales que se encuentran detrás de un balanceador de cargas si tienen su propia IP o EIP pública.

Habilite el escaneo de red

Para habilitar el escaneo de red, Security Hub debe estar habilitado en su cuenta. Puede habilitar el escaneo de red mediante una política de configuración o para cuentas individuales.

Cuentas de organización (recomendado): habilite el análisis de red en las cuentas y regiones de su organización creando o editando una política de configuración. Para obtener más información sobre la edición de una política de configuración, consulte Editar una política de configuración. Cuando el

escaneo de red está habilitado mediante una política de configuración, las cuentas de los miembros no pueden desactivar la función.

Cuentas individuales: en el caso de las cuentas que no se administran mediante una política de configuración, puede habilitar el escaneo de red mediante uno de los métodos siguientes.

> **Note**
>
> Al habilitar el análisis de red, autoriza a Security Hub a realizar un análisis de red activo comparándolo con los recursos de sus AWS entornos y entornos de Azure. Esto incluye los intentos de conexión al puerto TCP, la identificación de aplicaciones y protocolos y la recopilación de banners de servicio, encabezados HTTP y metadatos de certificados TLS.

Security Hub console

Para habilitar el escaneo de red

1. Abra la consola de Security Hub en https://console.aws.amazon.com/securityhub/v2/home.
2. En el panel de navegación, elija Configuración general.
3. Busque la sección Escaneo de red.
4. Seleccione Habilitar.
5. Confirme la autorización para continuar con el escaneo de red activo.

Security Hub API

Invoca la `EnableSecurityHubFeatureV2` API con el nombre `NETWORK_SCANNING` de la función.

> **Note**
>
> Al llamar a esta API cuando el escaneo de red ya está habilitado, se obtiene una respuesta de 200. El servicio conserva la `UpdatedAt` marca de tiempo de la activación original.

AWS CLI

Ejecute el siguiente comando para habilitar el escaneo de red:

```
aws securityhub enable-security-hub-feature-v2 --feature-name NETWORK_SCANNING
```

Cómo funciona el escaneo en red

Después de habilitar el escaneo de red, ocurre lo siguiente:

- El escaneo de red escanea los recursos existentes aproximadamente 24 horas después de habilitar la función.
- El escaneo de red analiza los nuevos recursos poco después de que Security Hub reciba la notificación del recurso creado.
- Network Scanning vuelve a analizar los recursos cuando se realizan ciertos cambios en el plano de control que cumplen los requisitos en un recurso apto para el escaneo.
- El escaneo de red vuelve a analizar los recursos activos aproximadamente cada 12 horas para detectar cambios en la accesibilidad.

Es posible que los recursos efímeros o de corta duración no se escaneen antes de que se agoten.

Hallazgos del escaneo de redes

Network Scanning publica los hallazgos en formato Open Cybersecurity Schema Framework (OCSF), utilizando la extensión AWS OCSF, y aparecen junto con otros hallazgos de Security Hub. El escaneo de red determina si un recurso tiene puertos accesibles o no. Si no se encuentra ningún tipo de recurso compatible, Network Scanning aún no ha escaneado el recurso.

Hallazgos sobre los puertos accesibles

Cada resultado representa un único puerto accesible en una combinación específica de recursos y direcciones. La `port_scan_result_list` sección de un hallazgo del OCSF contiene los resultados del análisis. Los siguientes ejemplos muestran la información devuelta por un recurso accesible:

```
"port_scan_result_list": [
    {
      "port_info": {
        "port": 6379,
        "protocol_name": "tcp",
        "protocol_num": 6
```

```
      },
      "status": "Open",
      "status_id": 1,
      "svc_name": "redis"
    }
],
```

```
"port_scan_result_list": [
    {
      "http_response": {
        "code": 200,
        "content_type": "text/html; charset=UTF-8",
        "http_headers": [
          {
            "name": "Server",
            "value": "Apache/2.4.68 (Amazon Linux)"
          },
          {
            "name": "Content-Type",
            "value": "text/html; charset=UTF-8"
          }
        ],
        "latency": 124
      },
      "port_info": {
        "port": 8080,
        "protocol_name": "tcp",
        "protocol_num": 6
      },
      "status": "Open",
      "status_id": 1
    }
  ],
```

Hallazgos informativos sobre la ausencia de puertos abiertos

El análisis de red crea un resultado cuando detecta que no hay puertos abiertos en un recurso. Este hallazgo tiene una gravedad de `Informational` y no requiere ninguna acción. Confirma que Network Scanning ha escaneado el recurso.

La búsqueda informativa permanece abierta en Security Hub hasta que se elimine el recurso o hasta que Network Scanning detecte puertos abiertos en el recurso. Cuando el análisis de red identifica los puertos abiertos en un recurso con un resultado informativo, cierra el hallazgo informativo. A continuación, crea una búsqueda para cada puerto abierto.

La información sobre la ausencia de puertos abiertos abarca los puertos que Network Scanning admite actualmente. Para obtener una lista de los puertos compatibles, consultethe section called "Puertos compatibles".

Búsqueda de eventos del ciclo de vida

En la siguiente tabla se describe el ciclo de vida de un hallazgo de escaneo de red.

Event	¿Qué sucede?
No se detectó ningún puerto abierto	El escaneo de red crea un `Informational` hallazgo que no requiere ninguna acción
Se detectaron puertos abiertos en el recurso con una búsqueda informativa	El escaneo de red cierra la búsqueda informativa y crea una búsqueda para cada puerto abierto
El puerto se detectó por primera vez como accesible	Network Scanning crea y publica un nuevo hallazgo
Aún se puede acceder al puerto al volver a escanear (sin cambios)	El escaneo de red actualiza periódicamente el resultado
Aún se puede acceder al puerto, pero las pruebas han cambiado	Network Scanning vuelve a publicar el hallazgo con pruebas actualizadas
Ya no se puede acceder al puerto	La búsqueda permanece abierta hasta que la próxima vez que se vuelva a escanear confirme que no se puede acceder al puerto
El recurso ha terminado o se ha eliminado	El escaneo de red cierra todos los hallazgos del recurso al establecer el `activity_name` atributo en `Close`
Dirección IP eliminada del recurso	El escaneo de red cierra los hallazgos para esa IP específica

Event	¿Qué sucede?
El escaneo de red está desactivado	El escaneo en red no produce hallazgos nuevos; los hallazgos existentes permanecen hasta que se agotan
Security Hub desactivado	Ya no tiene acceso a los hallazgos

Si se puede acceder a un puerto de forma intermitente, Network Scanning basa los resultados en las pruebas positivas obtenidas en el momento del escaneo. Tras solucionar un problema (por ejemplo, al cerrar una regla de firewall o detener un servicio), Network Scanning cierra la búsqueda en el siguiente análisis.

La desactivación del análisis en red no cierra inmediatamente los resultados. Los hallazgos existentes permanecen visibles hasta que pasan el ciclo de vida normal de búsqueda de Security Hub.

> **Note**
>
> Al adjuntar una dirección IP elástica (EIP) a una instancia de Amazon EC2, Network Scanning obtiene resultados sobre el recurso de EIP. El EIP es el recurso IP de nivel superior que posee la dirección. En el caso de los recursos del balanceador de carga de red (NLB), el nombre del DNS y los EIP adjuntos son puntos de entrada de red distintos, por lo que el escaneo de redes produce resultados distintos para cada uno de ellos.

Escanea las pruebas

Cuando el análisis de red detecta que se puede acceder a un puerto, el resultado incluye pruebas sobre el servicio al que se puede acceder. Se pueden recopilar los siguientes tipos de pruebas:

Banner TCP

Bytes iniciales enviados por el servicio al conectarse, como una cadena de versión SSH.

Metadatos HTTP

Encabezados de respuesta y código de estado HTTP.

Certificado TLS

Nombre común (CN), emisor, fecha de caducidad y estado de autofirma.

Detección de servicio

Aplicación o protocolo identificados que se ejecutan en el puerto.

Excluir los recursos del escaneo

Para excluir un recurso del escaneo de red, añada la clave de etiqueta `SecurityHubNetworkScanExclusion` al recurso. El valor de la etiqueta puede ser cualquier valor o estar vacío.

Debes aplicar la etiqueta al recurso real con la IP pública escaneable:

- En el caso de una EIP adjunta a una instancia EC2, etiquete la EIP, no la instancia EC2.
- En el caso de una instancia EC2 con solo una IP pública (sin EIP), etiquete la instancia EC2.
- En el caso de un balanceador de cargas, etiquete el balanceador de cargas y cualquier objetivo con direcciones IP públicas individuales.

Cuando agregas la etiqueta de exclusión, Network Scanning detiene los análisis futuros y cierra los hallazgos activos de ese recurso. Al eliminar la etiqueta, el recurso vuelve a ser apto para ser escaneado.

Puertos compatibles

El escaneo de red escanea los siguientes puertos TCP conocidos en los recursos elegibles.

```
21, 22, 23, 25, 53, 80, 110, 143, 443, 445, 1433, 3306, 3389, 5432,
5900, 6379, 8080, 8443, 9200, 27017
```

Multi-cloud soporte

El escaneo de red admite las direcciones IP públicas de Azure. Para escanear los recursos de Azure, cree un conector de Security Hub para su entorno de Azure. Para obtener más información sobre la integración con Microsoft Azure, consulte Integrar Security Hub con Microsoft Azure.

El comportamiento, las pruebas y los resultados del análisis de los recursos de Azure son idénticos a AWS los de los recursos. Los hallazgos aparecen junto con AWS los metadatos correspondientes del proveedor de nube y la región.

Disponibilidad por región

El escaneo de red está disponible en AWS las regiones comerciales en las que Security Hub está disponible.

Deshabilite el escaneo de red

Si su organización usa políticas de configuración, el administrador delegado puede deshabilitar el escaneo de redes en cuentas y regiones específicas editando la política de configuración. Para obtener más información sobre la edición de una política de configuración, consulte Editar una política de configuración. Al editar la política, seleccione la función de análisis de red, seleccione Desactivar y, a continuación, especifique las cuentas y las regiones en las que desea desactivar el análisis.

En el caso de las cuentas que no estén administradas por una política de configuración, puede deshabilitar el análisis de red mediante uno de los métodos siguientes.

Security Hub console

Para deshabilitar el escaneo de red

1. Abra la consola de Security Hub en https://console.aws.amazon.com/securityhub/v2/home.
2. En el panel de navegación, elija Configuración general.
3. Busque la sección Escaneo de red.
4. Elija Deshabilitar.
5. Confirme que desea deshabilitar el escaneo de red.

Security Hub API

Invoca la `DisableSecurityHubFeatureV2` API con el nombre `NETWORK_SCANNING` de la función.

AWS CLI

Ejecute el siguiente comando para deshabilitar el escaneo de red:

```
aws securityhub disable-security-hub-feature-v2 --feature-name NETWORK_SCANNING
```

Al deshabilitar el escaneo de red:

- El escaneo de red no activa nuevos escaneos.
- Los hallazgos existentes permanecen visibles hasta que pasan el ciclo de vida normal de búsqueda de Security Hub.
- El escaneo de red completa todos los escaneos que ya están en curso.

Automatizaciones en Security Hub

Security Hub incluye características que modifican automáticamente los resultados y ejecutan acciones sobre ellos según sus especificaciones.

Actualmente, el CSPM de Security Hub admite los siguientes tipos de automatizaciones:

- Reglas de automatización: actualizan y suprimen resultados de forma automática, además de enviar resultados a herramientas de gestión de tickets casi en tiempo real, según los criterios definidos.
- Respuesta y corrección automatizadas: cree EventBridge reglas de Amazon personalizadas que definan las acciones automáticas que se deben tomar en función de hallazgos e información específicos.

Las reglas de automatización son útiles cuando desea actualizar automáticamente los campos de resultados en el marco de esquemas de ciberseguridad abierta (OCSF). Por ejemplo, puede usar una regla de automatización para actualizar el nivel de gravedad de los resultados para los recursos con una etiqueta específica. El uso de la regla de automatización evita tener que actualizar manualmente el nivel de gravedad de cada resultado relacionado con la etiqueta específica. Puede configurar reglas de automatización para crear tickets en herramientas como Jira Cloud y ServiceNow cuando los resultados coinciden con atributos específicos. Los tickets se crean a partir de los hallazgos tan pronto como llegan a Security Hub.

EventBridge Las reglas son útiles cuando quieres tomar medidas fuera de Security Hub para obtener hallazgos específicos o enviar hallazgos específicos a herramientas de terceros para su corrección o investigación adicional. Las reglas se pueden usar para activar las acciones admitidas, como invocar una AWS Lambda función o enviar una notificación a un tema de Amazon Simple Notification Service (Amazon SNS) sobre un hallazgo específico.

Las reglas de automatización entran en vigor antes de que se EventBridge apliquen. Es decir, las reglas de automatización se activan y actualizan un hallazgo EventBridge antes de recibirlo. EventBridge las reglas se aplican entonces al hallazgo actualizado.

Reglas de automatización en Security Hub

Con Security Hub, puede automatizar tareas como actualizar los detalles de resultados y crear tickets para integraciones de terceros.

Reglas de automatización y Regiones de AWS

Las reglas de automatización se pueden crear en una sola configuración Región de AWS y luego aplicarlas en todas las configuraciones Regiones de AWS. Al usar la agregación de regiones, solo puede crear reglas en la región de origen. Al crear reglas en la región de origen, cualquier regla que defina se aplica a todas las regiones vinculadas, a menos que los criterios de la regla excluyan una región vinculada específica. Debes crear una regla de automatización para cualquier región que no sea una región vinculada.

Acciones y criterios de reglas

Las reglas de automatización en Security Hub utilizan criterios para hacer referencia a atributos OCSF en los resultados de Security Hub. Por ejemplo, los filtros compatibles con el `Criteria` parámetro CreateAutomationRuleV2 coinciden con los filtros compatibles con el `Filters` parámetro en la GetFindings versión 2. Esto significa que los filtros utilizados en las reglas de automatización se pueden emplear para obtener resultados. Security Hub admite los siguientes campos OCSF para los criterios de las reglas de automatización.

Campo OCSF	Valor del filtro en la consola	Operadores de filtro	Tipo de campo
`activity_id`	`Activity ID`	`Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)`	`Number`
`activity_name`	`Provider status`	`EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS`	`String`

Campo OCSF	Valor del filtro en la consola	Operadores de filtro	Tipo de campo
class_name	Finding class name	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
cloud.account.name	Finding account name	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
cloud.account.uid	Account ID	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
cloud.provider	Cloud provider	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
cloud.region	Region	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String

Campo OCSF	Valor del filtro en la consola	Operadores de filtro	Tipo de campo
compliance.assessments.category	Assessment category	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
compliance.assessments.meets_criteria	Compliance assessment meets criteria	True, False	Boolean
compliance.assessments.name	Assessment name	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
compliance.control	Security control ID	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
compliance.control_parameters	Control parameter name	EQUALS	Map
compliance.standards	Applicable standards	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String

Campo OCSF	Valor del filtro en la consola	Operadores de filtro	Tipo de campo
compliance.status	Compliance status	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
compliance.status_id	Compliance status ID	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	Number
confidence_score	Confidence	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	Number
finding_info.created_time_dt	Created at	Start, End, DateRange	Date (formatted as 2022-12-01T21:47:39.269Z)
finding_info.desc	Finding description	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
finding_info.first_seen_time_dt	First observed at	Start, End, DateRange	Date (formatted as 2022-12-01T21:47:39.269Z)

Campo OCSF	Valor del filtro en la consola	Operadores de filtro	Tipo de campo
finding_info.last_seen_time_dt	Last observed at	Start, End, DateRange	Date (formatted as 2022-12-01T21:47:39.269Z)
finding_info.modified_time_dt	Updated at	Start, End, DateRange	Date (formatted as 2022-12-01T21:47:39.269Z)
finding_info.related_events.product.uid	Related findings product ID	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
finding_info.related_events.title	Related findings title	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
finding_info.related_events.traits.category	Traits category	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
finding_info.related_events.uid	Related findings ID	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String

Campo OCSF	Valor del filtro en la consola	Operadores de filtro	Tipo de campo
finding_info.related_events_count	Related findings count	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	Number
finding_info.src_url	Source URL	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
finding_info.tags	Finding info tags	EQUALS	Map
finding_info.title	Finding title	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
finding_info.types	Finding type	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
finding_info.uid	Provider finding ID	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String

Campo OCSF	Valor del filtro en la consola	Operadores de filtro	Tipo de campo
metadata.product.feature.uid	Generator ID	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
metadata.product.name	Product name	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
metadata.product.uid	Product ARN	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
metadata.product.vendor_name	Company name	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
remediation.desc	Recommendation text	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String

Campo OCSF	Valor del filtro en la consola	Operadores de filtro	Tipo de campo
remediation.references	Recommendation URL	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
resources.cloud_partition	Resource partition	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
resources.modified_time_dt	Resource last modified time	Start, End, DateRange	Date (formatted as 2022-12-01T21:47:39.269Z)
resources.name	Resource name	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
resources.owner.account.name	Account name	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
resources.owner.account.uid	Account	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String

Campo OCSF	Valor del filtro en la consola	Operadores de filtro	Tipo de campo
resources.owner.org.uid	Organization	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
resources.provider	Cloud provider	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
resources.region	Resource region	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
resources.tags	Resource tags	EQUALS	Map
resources.type	Resource type	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
resources.uid	Resource ID	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String

Campo OCSF	Valor del filtro en la consola	Operadores de filtro	Tipo de campo
vendor_attributes.severity	Provider severity	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
vendor_attributes.severity_id	Provider severity ID	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	Number
vulnerabilities.affected_code.file.path	Affected code file path	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
vulnerabilities.affected_packages.name	Affected package name	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
vulnerabilities.cve.cvss.base_score	CVE CVSS base score	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	Number

Campo OCSF	Valor del filtro en la consola	Operadores de filtro	Tipo de campo
vulnerabilities.cve.epss.score	Epss score	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
vulnerabilities.cve.uid	Vulnerability ID	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
vulnerabilities.fix_coverage	Software vulnerabilities coverage	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
vulnerabilities.is_exploit_available	Software vulnerabilities with exploit available	True, False	Boolean
vulnerabilities.is_fix_available	Software vulnerabilities with fix available	True, False	Boolean
vulnerabilities.related_vulnerabilities	Related vulnerabilities	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String

Para los criterios etiquetados como campos de cadena, el uso de distintos operadores de filtro en el mismo campo afecta la lógica de evaluación. Para obtener más información, consulte StringFilter la referencia de la API de Security Hub.

Cada criterio admite una cantidad máxima de valores que se pueden utilizar para filtrar los resultados que coinciden. Para conocer los límites de cada criterio, consulte OcsfFindingFilters la referencia de la API de Security Hub

Campos OCSF que se pueden actualizar

Los siguientes son los campos OCSF que se pueden actualizar mediante reglas de automatización.

- `Comment`
- `SeverityId`
- `StatusId`

Cómo las reglas de automatización evalúan los resultados

Una regla de automatización evalúa los resultados nuevos y actualizados que Security Hub genera o ingiere después de que se crea la regla.

Las reglas de automatización evalúan los resultados originales proporcionados por el proveedor. Los proveedores pueden aportar resultados nuevos y actualizar resultados existentes mediante su integración con Security Hub. Las reglas no se activan al actualizar los campos de búsqueda después de crear la regla mediante la `BatchUpdateFindingsV2` operación. Si crea una regla de automatización y realiza una actualización `BatchUpdateFindingsV2` que afecten al mismo campo de resultado, la última actualización establecerá el valor de ese campo. Vea el siguiente ejemplo:

Se utiliza `BatchUpdateFindingsV2` para actualizar el campo `Status` de un resultado de `New` a `In Process`. Si llama a `GetFindingsV2`, el campo `Status` ahora tendrá un valor de `In Process`. Se crea una regla de automatización que cambia el campo `Status` del resultado de `New` a `Suppressed` (recuerde que las reglas ignoran las actualizaciones realizadas con `BatchUpdateFindingsV2`). El proveedor de resultados actualiza el resultado y cambia el campo `Status` a `New`. Si llama a `GetFindingsV2`, el campo `Status` ahora tendrá un valor de `Suppressed`, ya que se aplicará la regla de automatización y la regla será la última acción que se realice en el resultado.

Cuando crea o edita una regla en la consola de Security Hub, la consola muestra una vista previa de los resultados que coinciden con los criterios de la regla. Mientras que las reglas de automatización

evalúan los resultados originales enviados por el proveedor de resultados, la vista previa de la consola refleja los resultados del estado final, tal como se mostrarían en respuesta a la operación de la API `GetFindingsV2` (es decir, después de aplicar las acciones de regla u otras actualizaciones al resultado).

Cómo se ordenan las reglas de automatización

A cada regla de automatización se le asigna un orden. Esto determina el orden en que Security Hub aplica sus reglas de automatización y adquiere importancia cuando varias reglas se relacionan con el mismo resultado o campo de resultado.

Cuando varias acciones de reglas se refieren al mismo resultado o campo de resultado, la regla con el valor numérico más alto de orden de reglas se aplica en último lugar y tiene el efecto definitivo.

Al crear una regla en la consola de Security Hub, Security Hub asigna automáticamente el orden de las reglas según el orden de creación de las mismas. A la primera regla que cree se le asigna el orden 1. Cuando exista más de una regla, cada regla nueva recibirá el siguiente valor numérico disponible para el orden.

Al crear una regla mediante una CreateAutomationRuleV2 API o AWS CLI, Security Hub aplica `RuleOrder` primero la regla con el valor numérico más bajo. Luego aplica las reglas subsiguientes en orden ascendente. Si varios resultados tienen el mismo `RuleOrder`, Security Hub aplica primero la regla con un valor anterior para el campo `UpdatedAt` (es decir, la regla que se editó más recientemente se aplica al final).

Puede modificar el orden de las reglas en cualquier momento.

Ejemplo de orden de reglas:

Regla A (el orden de la regla es**1**):

- Criterios de la regla A
  - `ProductName` = `Security Hub CSPM`
  - `Resources.Type` es `S3 Bucket`
  - `Compliance.Status` = `FAILED`
  - `RecordState` es `NEW`
  - `Workflow.Status` = `ACTIVE`
- Acciones de la regla A

- Actualizar `Confidence` a `95`
- Actualizar `Severity` a `CRITICAL`
- Actualizar `Comment` a `This needs attention`

Regla B (el orden de la regla es**2**):

- Criterios de la regla B
  - `AwsAccountId` = `123456789012`
- Acciones de la regla B
  - Actualizar `Severity` a `INFORMATIONAL`

Primero, las acciones de la Regla A se aplican a los resultados de Security Hub que coinciden con los criterios de la Regla A. Luego, las acciones de la Regla B se aplican a los resultados de Security Hub con el ID de cuenta especificado. En este ejemplo, como la regla B se aplica en último lugar, el valor final de `Severity` en los resultados del ID de cuenta especificado es `INFORMATIONAL`. Según la acción de la regla A, el valor final de `Confidence` en los resultados coincidentes es `95`.

Third-party integraciones

Puede usar reglas de automatización para crear tickets para integraciones con Jira Cloud y ServiceNow ITSM. Para obtener más información, consulte Creación de una regla para una integración con terceros.

Situaciones en las que las reglas de automatización no funcionan

Las siguientes son situaciones en las que las reglas de automatización no funcionan:

- La cuenta independiente pasa a ser miembro de una organización con un administrador delegado
- La cuenta de administración de la organización elimina al administrador delegado y designa uno nuevo
- La configuración del agregador para la cuenta de administrador delegado o independiente cambia cuando una región desvinculada pasa a ser una región vinculada

En estos casos, un miembro de una organización puede gestionar las reglas de automatización con operaciones de lista, obtención y eliminación en las AWS CLI API de quirófano.

Cuando una región desvinculada se convierte en una región vinculada, el administrador delegado o la cuenta independiente pueden administrar los recursos de una región vinculada mediante operaciones de lista, obtención y eliminación.

Creación de reglas de automatización en Security Hub

En este tema, se describe cómo crear reglas de automatización. Puede utilizar reglas de automatización para actualizar los detalles de un resultado o crear un ticket para una integración de terceros. Debe crear reglas de automatización de forma individual y en el Región de AWS lugar donde quiera que se apliquen. Sin embargo, si crea una regla de automatización en una región de agregación, se aplica en todas las regiones. De lo contrario, si crea una regla de automatización en una región no vinculada, solo se aplica en esa región.

Creación de una regla que actualiza los detalles de los resultados

El siguiente procedimiento describe cómo crear una regla que actualiza los detalles de los resultados.

1. Inicia sesión en tu AWS cuenta. Abra la consola de Security Hub en https://console.aws.amazon.com/securityhub/v2/home.
2. Desde el panel de navegación, en Administración, elija Automatizaciones.
3. Seleccione Creación de regla.
4. En Detalles, introduzca un nombre para la regla de automatización.
   - (Opcional) Introduzca una descripción para la regla de automatización.
5. En Acciones, elija Actualizar detalles de resultados. Puede buscar criterios y agregar criterios en la barra de búsqueda. Para verificar si algún resultado coincide con los criterios, elija Vista previa de resultados coincidentes.
6. En Actualizar detalles de resultados, elija al menos un detalle de resultado que se actualizará cuando un resultado coincida con los criterios. Puede elegir Gravedad, Estado o Comentario.
7. En Configuración de la regla, seleccione Habilitada o Desactivada. Si selecciona Activado, la regla de automatización se habilita y procesa los nuevos hallazgos. Si selecciona Desactivado, la regla de automatización se desactiva y no procesa ningún hallazgo.
8. (Opcional) En Etiquetas, elija Agregar nueva etiqueta para introducir un par clave-valor que se aplicará a la regla de automatización.
9. Seleccione Creación de regla.

Creación de una regla para una integración con terceros

El siguiente procedimiento describe cómo crear una regla que genera un ticket para una integración con terceros. Para obtener información sobre las integraciones que admite Security Hub CSPM, consulte Third-party Integraciones para Security Hub CSPM.

1. Inicie sesión en su cuenta. AWS Abra la consola de Security Hub en https://console.aws.amazon.com/securityhub/v2/home.
2. Desde el panel de navegación, en Administración, elija Automatizaciones.
3. Seleccione Creación de regla.
4. En Detalles, introduzca un nombre para la regla de automatización.
   - (Opcional) Introduzca una descripción para la regla de automatización.
5. En Acciones, seleccione Crear ticket. Puede buscar criterios y agregar criterios en la barra de búsqueda. Para verificar si algún resultado coincide con los criterios, elija Vista previa de resultados coincidentes.
6. En Crear un ticket, elija una integración de sistemas de tickets de TI en el menú desplegable y, a continuación, seleccione Agregar integración.
7. En Configuración de la regla, seleccione Habilitada o Desactivada. Si selecciona Activado, la regla de automatización se habilita y procesa los nuevos hallazgos. Si selecciona Desactivado, la regla de automatización se desactiva y no procesa ningún hallazgo.
8. (Opcional) En Etiquetas, elija Agregar nueva etiqueta para introducir un par clave-valor que se aplicará a la regla de automatización.
9. Seleccione Crear regla.

Visualización de detalles de las reglas de automatización en Security Hub

En este tema, se describe cómo ver los detalles de las reglas de automatización. Puede ver los siguientes detalles de una regla de automatización:

- Nombre y descripción
- Acciones y criterios
- Estado de la regla y resultados existentes
- Tags

Para ver los detalles de una regla de automatización

1. Inicia sesión en tu AWS cuenta. Abra la consola de Security Hub en https://console.aws.amazon.com/securityhub/v2/home.
2. Desde el panel de navegación, en Administración, elija Automatizaciones. En esta pantalla aparecen todas las reglas de automatización que ha creado.
3. Seleccione la regla de automatización que desea ver. Elija Ver detalles. Como alternativa, puede elegir el nombre de la regla de automatización que desea ver.

Actualización del orden de las reglas en Security Hub

En este tema, se describe cómo actualizar el orden de las reglas de automatización en la consola. Si desea editar los criterios de una regla de automatización, consulte Edición de reglas de automatización en Security Hub.

No puede actualizar el orden de una sola regla de automatización sin actualizar el orden de todas las reglas de automatización. Por ejemplo, tiene cuatro reglas de automatización: Regla A (1), Regla B (2), Regla C (3) y Regla D (4). Desea que la Regla D se aplique primero. Para hacerlo, cambie su número de orden de 4 a 1. Como resultado, la Regla A pasa a ser 2, la Regla B a 3 y la Regla C a 4.

Para actualizar el orden de las reglas de automatización

1. Inicia sesión en tu AWS cuenta. Abra la consola de Security Hub en https://console.aws.amazon.com/securityhub/v2/home.
2. Desde el panel de navegación, en Administración, elija Automatizaciones.
3. Seleccione la regla de automatización que desea editar. En Orden, seleccione el ícono del lápiz junto al número de orden. Use las flechas para definir el nuevo número de orden. Seleccione el ícono ✓ para confirmar. Seleccione el ícono X para cancelar. Como alternativa, puede elegir Cambiar orden para mover la regla de automatización hacia abajo, hacia arriba o al inicio de la lista.

Desactivación de reglas de automatización en Security Hub

En este tema, se describe cómo desactivar reglas de automatización. Cuando se desactiva una regla de automatización, Security Hub deja de aplicarla. Puede deshabilitar las reglas de automatización en cualquier momento y en el Región de AWS lugar donde las creó.

Para desactivar una regla

1. Inicia sesión en tu AWS cuenta. Abra la consola de Security Hub en https://console.aws.amazon.com/securityhub/v2/home.
2. Desde el panel de navegación, en Administración, elija Automatizaciones.
3. Seleccione la regla de automatización que desea desactivar. En Estado, seleccione el ícono del lápiz junto a Habilitada. Abra el menú desplegable y elija Desactivada. Seleccione el ícono ✓ para confirmar. Seleccione el ícono X para cancelar. También puede seleccionar Desactivar desde el menú desplegable Acciones.

Habilitación de una regla de automatización en Security Hub

En este tema, se describe cómo habilitar reglas de automatización. Cuando se habilitan reglas de automatización, Security Hub reanuda la aplicación. Puede activar las reglas de automatización en cualquier momento y en el Región de AWS lugar donde las creó.

Para habilitar una regla

1. Inicia sesión en tu AWS cuenta. Abra la consola de Security Hub en https://console.aws.amazon.com/securityhub/v2/home.
2. Desde el panel de navegación, en Administración, elija Automatizaciones.
3. Seleccione la regla de automatización que desea habilitar. En Estado, seleccione el ícono del lápiz junto a Desactivada. Abra el menú desplegable y elija Habilitada. Seleccione el ícono ✓ para confirmar. Seleccione el ícono X para cancelar. También puede seleccionar Habilitar desde el menú desplegable Acciones.

Duplicación de reglas de automatización en Security Hub

En este tema, se describe cómo duplicar reglas de automatización. La duplicación de reglas de automatización contribuye a ahorrar tiempo si desea evitar crearlas desde cero. Cuando duplica reglas de automatización, puede actualizar los detalles, las acciones, la configuración de la regla y las etiquetas. Puede editar las reglas de automatización en el Región de AWS lugar donde las creó.

Para duplicar una regla

1. Inicie sesión en su AWS cuenta y abra la consola de Security Hub en https://console.aws.amazon.com/securityhub/v2/home.

2. En el panel de navegación, elija Administración y luego Automatizaciones.
3. Seleccione la regla de automatización que desea duplicar. Luego, elija Acciones y, a continuación, Duplicar.
4. Realice y revise los cambios y, después, elija Crear regla.

Edición de reglas de automatización en Security Hub

En este tema, se describe cómo editar reglas de automatización. Puede editar las reglas de automatización en el Región de AWS lugar donde las creó.

Puede editar lo siguiente en las reglas de automatización:

- Nombre y descripción
- Acciones
- Configuración de reglas

No puede editar las etiquetas de las reglas de automatización.

Para editar una regla

1. Inicia sesión en tu AWS cuenta. Abra la consola de Security Hub en https://console.aws.amazon.com/securityhub/v2/home.
2. Desde el panel de navegación, en Administración, elija Automatizaciones.
3. Seleccione la regla de automatización que desea editar. Seleccione Acciones y, a continuación, Editar.
4. Realice los cambios y revíselos.
5. Seleccione Save changes (Guardar cambios).

Eliminación de reglas de automatización en Security Hub

En este tema, se describe cómo eliminar reglas de automatización. Puede eliminar las reglas de automatización en el Región de AWS lugar donde las creó.

Para eliminar una regla

1. Inicie sesión en su AWS cuenta y abra la consola de Security Hub en https://console.aws.amazon.com/securityhub/v2/home.

2. En el panel de navegación, elija Administración y luego Automatizaciones.
3. Seleccione la regla de automatización que desea eliminar. Seleccione Actions y, luego, Delete.
4. Elija Eliminar.

Reglas de automatización en EventBridge

Puedes usar las reglas de automatización de Amazon EventBridge para responder a las conclusiones de Security Hub. Security Hub envía las conclusiones a EventBridge los eventos prácticamente en tiempo real. Puede escribir reglas básicas que indiquen qué acciones automatizadas se deben tomar cuando un evento coincide con una regla. Las acciones que se pueden desencadenar automáticamente incluyen lo siguiente:

- Configurar un destino de API en EventBridge.
- Invocación de comandos de ejecución de Amazon EC2
- Invocación de funciones de Lambda
- Invocación de máquinas de estado de Step Functions
- Notificar un tema de Amazon SNS o una cola de Amazon SQS
- Retransmición de eventos a Kinesis Data Streams
- Enviar un resultado a una herramienta de gestión de tickets, chat, de SIEM o respuesta a incidentes de terceros
- Enviar un evento a un EventBridge bus de otra AWS cuenta

Security Hub envía los hallazgos nuevos y actualizados a un formato EventBridge de eventos. A continuación, configura EventBridge las reglas para responder a cada evento de Security Hub. Para obtener más información, consulte ¿Qué es EventBridge? en la Guía EventBridge del usuario.

> **Note**
>
> Si tiene EventBridge reglas definidas para los hallazgos en Security Hub CSPM, las reglas podrían superponerse con las reglas definidas para Security Hub. Para evitar enviar hallazgos duplicados, evalúe las reglas que ha definido para el CSPM de Security Hub para determinar si coinciden con las reglas que ha definido para Security Hub. Si procede, inhabilite las reglas de CSPM de Security Hub que hayan sido reemplazadas por reglas de Security Hub.

> **Note**
>
> Como práctica recomendada, asegúrese de que los usuarios con permiso para acceder EventBridge utilicen AWS Identity and Access Management políticas que concedan los permisos mínimos requeridos. Para obtener más información, consulte EventBridge y AWS Identity and Access Management en la Guía EventBridge del usuario.

EventBridge tipos de eventos

Security Hub utiliza los siguientes tipos de EventBridge eventos de Amazon para integrarse con ellos EventBridge.

En el EventBridge panel de control de Security Hub, Todos los eventos incluyen todos estos tipos de eventos.

Resultados importados V2

Security Hub envía automáticamente todos los hallazgos nuevos y todas las actualizaciones de los hallazgos existentes a la EventBridge categoría de Findings Imported V2 eventos. Cada evento Findings Imported V2 contiene un único resultado.

Cada hallazgo que se importa y cada hallazgo que se actualiza mediante una `BatchUpdateFindingsV2` solicitud desencadena un Findings Imported V2 evento.

En el caso de las cuentas de administrador, el feed de eventos EventBridge incluye eventos para obtener información tanto de su cuenta como de sus cuentas de miembros.

En una región de agregación, el feed de eventos incluye eventos para los hallazgos de la región de agregación y de las regiones vinculadas. Cross-Region los hallazgos se incluyen en el feed de eventos casi en tiempo real.

Puede definir reglas EventBridge que dirijan automáticamente los hallazgos a un flujo de trabajo de corrección, a una herramienta de terceros o a otro EventBridge objetivo compatible. Las reglas pueden incluir filtros que solo apliquen la regla si el resultado tiene valores de atributo específicos.

Este método le permite enviar automáticamente todos los resultados ,o todos aquellos con determinadas características, a un flujo de trabajo de corrección o respuesta.

> **Note**
>
> Tanto Security Hub como Security Hub CSPM envían los hallazgos a EventBridge Under the source of. `aws.securityhub` Asegúrese de que sus EventBridge reglas utilicen el tipo de detalle específico de Security Hub para evitar la duplicación de notificaciones relacionadas con los hallazgos del CSPM de Security Hub.

EventBridge formatos de eventos

El tipo de evento Findings Imported V2 utiliza el siguiente formato de evento.

Ejemplo

Este formato se usa cuando Security Hub envía un evento a EventBridge.

```
{
   "version":"0",
   "id":"CWE-event-id",
   "detail-type":"Findings Imported V2",
   "source":"aws.securityhub",
   "account":"111122223333",
   "time":"2019-04-11T21:52:17Z",
   "region":"us-west-2",
   "resources":[
      "e51603d1054aad9d9f498d82d6e81acf4cf6bc88140e8ad2273123c73b81084"
   ],
   "detail":{
      "findings": [{
         <finding content>
       }]
   }
}
```

Cada evento envía un único resultado. *`<finding content>`* es el contenido JSON del resultado enviado por el evento.

Para obtener una lista completa de los atributos de los resultados, consulte Resultados de OCSF en el CSPM de Security Hub.

Configuración de reglas para EventBridge

Puedes crear una regla en Amazon EventBridge que defina la acción que se debe realizar cuando se recibe un Findings Imported V2 evento. Findings Imported V2los eventos se activan mediante actualizaciones `BatchUpdateFindingsV2`.

Cada regla contiene un patrón de eventos, que identifica los eventos que activan la regla. El patrón de eventos siempre contiene el origen del evento (`aws.securityhub`) y el tipo de evento (Resultados importados V2). El patrón de eventos también puede especificar filtros para identificar los resultados a los que se aplica la regla.

A continuación, la regla de eventos identifica los objetivos de la regla. Los objetivos son las acciones que se deben tomar cuando se EventBridge recibe un evento de Findings Imported V2 y el resultado coincide con los filtros.

Las instrucciones que se proporcionan aquí utilizan la EventBridge consola. Cuando usas la consola, crea EventBridge automáticamente la política requerida basada en los recursos que te permite EventBridge escribir en Amazon CloudWatch Logs.

También puede utilizar el `PutRule` funcionamiento de la EventBridge API. Sin embargo, si usas la EventBridge API, debes crear la política basada en los recursos. Para obtener información sobre la política requerida, consulte los permisos de CloudWatch registro en la Guía del EventBridge usuario de Amazon.

Formato del patrón de eventos

El formato del patrón para eventos de eventos de Resultados importados V2 es el siguiente:

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Findings Imported V2"
  ],
  "detail": {
    "findings": {
      <attribute filter values>
    }
  }
}
```

- `source` identifica a Security Hub como el servicio que genera el evento.
- `detail-type` identifica el tipo de evento.
- `detail` es opcional y proporciona los valores de filtro para el patrón de eventos. Si el patrón de eventos no contiene un campo `detail`, todos los resultados activan la regla.

Puede filtrar los resultados en función de cualquier atributo del resultado. Para cada atributo, proporciona una matriz separada por comas de uno o más valores.

```
"<attribute name>": [ "<value1>", "<value2>"]
```

Si proporciona más de un valor para un atributo, estos valores se unen mediante `OR`. Un resultado coincide con el filtro para un atributo individual si el resultado tiene cualquiera de los valores enumerados. Por ejemplo, si proporciona `INFORMATIONAL` y `LOW` como valores para `Severity.Label`, entonces el resultado coincide si tiene una etiqueta de gravedad de `INFORMATIONAL` o `LOW`.

Los atributos se unen mediante `AND`. Un resultado coincide si este coincide con los criterios de filtrado para todos los atributos proporcionados.

Cuando proporciones un valor de atributo, este debe reflejar la ubicación de ese atributo dentro de la estructura del marco AWS abierto del esquema de ciberseguridad (OCSF).

En el siguiente ejemplo, el patrón de eventos proporciona valores de filtro para `ProductArn` y `Severity.Label`, por lo que un resultado coincide si lo genera Amazon Inspector y tiene una etiqueta de gravedad de `INFORMATIONAL` o `LOW`.

```
{
    "source": [
        "aws.securityhub"
     ],
    "detail-type": [
        "Findings Imported V2"
    ],
    "detail": {
        "findings": {
            "ProductArn": ["arn:aws:securityhub:us-east-1::product/aws/inspector"],
            "Severity": {
                "Label": ["INFORMATIONAL", "LOW"]
            }
        }
```

```
    }
}
```

Creación de una regla de eventos

Puede usar un patrón de eventos predefinido o un patrón de eventos personalizado para crear una regla. EventBridge Si seleccionas un patrón predefinido, rellena EventBridge automáticamente `source` y`detail-type`. EventBridge también proporciona campos para especificar los valores de filtro para los siguientes atributos de búsqueda:

- `cloud.account.uid`
- `compliance.status`
- `metadata.product.name`
- `resources.uid`
- `severity`
- `status`

Para crear una EventBridge regla (consola)

1. Abre la EventBridge consola de Amazon en https://console.aws.amazon.com/events/.
2. Con los siguientes valores, cree una EventBridge regla que supervise la búsqueda de eventos:
   - En Tipo de regla, seleccione Regla con un patrón de evento.
   - Elija cómo crear el patrón de eventos.

Cómo crear el patrón de eventos con...	Haga lo siguiente...	
Una plantilla	En la sección Patrón de eventos, elija una de las siguientes opciones: • En Origen del evento, seleccione Servicios de AWS . • En Servicio de AWS , elija Security Hub.	

Cómo crear el patrón de eventos con...	Haga lo siguiente...	
	• En Tipo de evento, elija Resultados importados – V2. • (Opcional) Para que la regla sea más específic a, agregue valores de filtro. Por ejemplo, para limitar la regla a resultado s con estados de registro activos, en Estados de registro específicos, seleccione Activo.	

Cómo crear el patrón de eventos con...	Haga lo siguiente...	
Un patrón de eventos personalizado (Utilice un patrón personalizado si desea filtrar los hallazgos en función de los atributos que no aparecen en la EventBridge consola).	• En la sección Patrón de evento, seleccione Patrones personalizados (editor JSON) y luego pegue el siguiente patrón de evento en el área de texto: `{ "source": [ "aws.secu rityhub" ], "detail-type": [ "Findings Imported V2" ], "detail": { "findings": { "<attribut e name> ": [ "<value1>", "<value2>"] } } }` • Actualice el patrón de eventos para incluir el atributo y los valores del atributo que desee utilizar como filtro. Por ejemplo, para aplicar la regla a resultados que tengan una gravedad de `Critical`, use el	

Cómo crear el patrón de eventos con...	Haga lo siguiente...	
	siguiente ejemplo de patrón: `{ "source": ["aws.securityhub"], "detail-type": ["Findings Imported V2"], "detail":{ "findings": { "Severity": ["Critical"] } } }`	

- Para los tipos de destino, elija el AWS servicio y, para Seleccionar un objetivo, elija un objetivo, como un tema o una AWS Lambda función de Amazon SNS. El destino se activa cuando se recibe un evento que coincide con el patrón de eventos definido en la regla.

Para obtener más información sobre la creación de reglas, consulte Creación de EventBridge reglas de Amazon que reaccionen a los eventos en la Guía del EventBridge usuario de Amazon.

> **Note**
>
> Si tiene EventBridge reglas definidas para las conclusiones en el CSPM de Security Hub, las reglas podrían superponerse con las reglas definidas para Security Hub. Para evitar enviar hallazgos duplicados, evalúe las reglas que ha definido para el CSPM de Security Hub para determinar si coinciden con las reglas que ha definido para Security Hub. Si procede, inhabilite las reglas de CSPM de Security Hub que hayan sido reemplazadas por reglas de Security Hub.

Third-party integraciones para Security Hub

Puede mejorar su postura de seguridad con integraciones de terceros para AWS Security Hub. Con esta característica, puede habilitar integraciones que consuman los resultados de Security Hub y así incorporar sus herramientas operativas, de investigación y de respuesta. Actualmente, Security Hub admite integraciones con Jira Cloud y ServiceNow.

Temas

- Integraciones para AWS Centro de seguridad Jira Cloud
- Integraciones para ServiceNow
- Políticas clave de KMS para las integraciones de venta de entradas de Security Hub
- Probar las integraciones de venta de entradas configuradas

Integraciones para AWS Centro de seguridad Jira Cloud

En este tema se describe cómo integrar Security Hub conJira Cloud. Antes de completar cualquiera de los procedimientos de este tema, debe adquirir un plan de suscripción de Jira Cloud. Para obtener información sobre los planes de suscripción, consulte Precios en el sitio web de Atlassian.

Esta integración te permite enviar las conclusiones de Security Hub a Jira Cloud, de forma manual o automática, para que puedas gestionarlas como parte de tus flujos de trabajo operativos. Por ejemplo, puede asignar la responsabilidad de incidencias que requieren investigación y remediación.

Para las cuentas que forman parte de una organización, únicamente el administrador delegado puede configurar una integración. El administrador delegado puede usar manualmente la característica de creación de tickets para cualquier resultado de una cuenta de miembro. Además, el administrador delegado puede usar reglas de automatización para crear tickets de manera automática para cualquier resultado asociado a cuentas de miembro. Al definir una regla de automatización, el administrador delegado puede establecer criterios que incluyan todas las cuentas de miembro o cuentas de miembro específicas. Para obtener información sobre cómo configurar un administrador delegado, consulte Configuración de una cuenta de administrador delegado en Security Hub.

Para las cuentas que no forman parte de una organización, todas las funciones de esta característica están disponibles.

Requisitos previos

Antes de conectar Security Hub con tu Jira Cloud entorno, debes asegurarte de realizar los siguientes pasos de configuración en tu entorno de Jira.

- Instala la aplicación en la nube AWS Security Hub for Jira.
- Ten al menos un proyecto de desarrollo de software gestionado por la empresa.
- Asigne la AWS aplicación a los proyectos de desarrollo de software para los que quiere recibir los hallazgos de Security Hub.

A continuación se enumeran los pasos para cada uno de estos requisitos previos.

1. Instala la AWS Security Hub para Jira Cloud aplicación

Security Hub tiene una aplicación para facilitar su integración con Jira. Esta aplicación instala campos personalizados y un tipo de problema personalizado. Security Hub los usa para completar los atributos específicos de los hallazgos.

1. Inicie sesión en el sitio de Atlassian como administrador.
2. Elija Configuración, y luego elija Aplicaciones.
3. Si se le dirige a la página del marketplace, elija Buscar aplicaciones nuevas. Si se le dirige a la página de aplicaciones, elija Explorar aplicaciones y luego busque AWS Security Hub para Jira Cloud. Después, elija Obtener ahora.

2. Crea un proyecto o verifica los proyectos existentes

Este paso es obligatorio si aún no ha creado un proyecto. Para obtener información sobre cómo crear un proyecto, consulte Creación de un proyecto nuevo en la documentación de Jira Cloud Support.

Requisitos para crear un proyecto

Asegúrese de realizar lo siguiente cuando cree un proyecto nuevo.

- Elija Desarrollo de software como plantilla del proyecto.
- Elige Company-managed el tipo de proyecto.

Requisitos para los proyectos existentes

Todos los proyectos existentes en tu entorno de Jira que estén integrados con Security Hub deben ser del tipo de Company-managed proyecto.

3. Añade tus proyectos al AWS Security Hub para Jira Cloud aplicación

Para que Security Hub pueda enviar correctamente los hallazgos a tu entorno de Jira, cada proyecto que quieras usar con Security Hub debe estar asociado al AWS Security Hub para la Jira Cloud aplicación. La asociación de un proyecto de Jira a la aplicación garantiza que los campos personalizados necesarios para Security Hub estén asociados al proyecto y puedan rellenarse cuando Security Hub envíe las conclusiones al proyecto.

1. Inicie sesión en el sitio de Atlassian como administrador.
2. Elija Configuración, y luego elija Aplicaciones.
3. En la lista de aplicaciones, elija AWS Security Hub para Jira Cloud.
4. Elija la pestaña Configuración del conector.
5. En Proyectos habilitados, elija Agregar proyecto de Jira.
    a. En el menú desplegable, elija Agregar todos o seleccione un proyecto. Repita esta parte del paso si desea agregar más de un proyecto, pero no todos.
    b. Seleccione Save.

Puede verificar qué proyectos se instalaron correctamente en la pestaña Administrador de instalación. También puede verificar configuraciones para campos, pantallas, estados y flujos de trabajo desde la pestaña Administrador de instalación.

Para obtener información adicional sobre Jira Cloud, consulte los Recursos de Jira Cloud en el sitio web de Atlassian.

Recomendaciones

Crea una cuenta de sistema dedicada para tu entorno de Jira

La integración de Security Hub Jira Cloud utiliza una conexión de OAuth asociada a un usuario específico de tu instancia de Jira. Se recomienda crear una cuenta de sistema dedicada para usarla en la conexión OAuth de Security Hub para la conexión por los siguientes motivos:

- Un usuario del sistema dedicado se asegura de que la conexión no esté asociada a un empleado cuyos permisos para acceder al entorno de Jira podrían cambiar con el tiempo, lo que afectaría a la capacidad de Security Hub de integrarse con tu entorno de Jira.

- Cada problema que Security Hub crea en Jira muestra un campo Creado por que contiene el nombre de usuario que se usó para crear la conexión de OAuth. Al usar una cuenta del sistema para la conexión de OAuth, esta cuenta del sistema aparece como la creadora del ticket, lo que permite saber que el hallazgo se creó mediante la integración de Security Hub y no de forma manual por otro usuario de Jira.

Configura una integración entre Security Hub y Jira Cloud

Debe completar el siguiente procedimiento para cada uno de los Jira Cloud proyectos a los que quiera enviar las conclusiones de Security Hub.

> **Note**
>
> Al crear un Jira Cloud conector, se le redirige del conector actual Región de AWS al`"https://3rdp.oauth.console.api.aws"`, para que pueda completar el registro del conector. Después, volverá al lugar en el Región de AWS que se está creando el conector.

Para configurar una integración para Jira Cloud

1. Inicie sesión en su AWS cuenta con sus credenciales y abra la consola de Security Hub en https://console.aws.amazon.com/securityhub/v2/home? region=us-east-1.
2. En el panel de navegación, elija Administración y luego seleccione Integraciones.
3. Elija Añadir Jira Cloud.
4. En Detalles, ingrese un nombre único y descriptivo para la integración y decida si desea incluir una descripción opcional.
5. En el caso de los cifrados, elija cómo quiere cifrar sus credenciales de integración en Security Hub.

   - Usar AWS una clave propia: con esta opción, se usa una clave de servicio propiedad de Security Hub para cifrar los datos de tus credenciales de integración en Security Hub.
   - Elija una clave de KMS diferente (avanzada): con esta opción, elige una AWS KMS key que haya creado y que desea que se utilice para cifrar los datos de sus credenciales de integración en Security Hub. Para obtener información sobre cómo crear una AWS KMS clave, consulte Crear una AWS KMS clave en la Guía para AWS Key Management Service desarrolladores. Si decide usar su propia clave, debe agregar declaraciones de política a la clave de KMS que permitan a Security Hub acceder a la clave. Consulta las políticas AWS

KMS clave para las integraciones de venta de entradas de Security Hub para obtener más información sobre las políticas necesarias.

> **Note**
>
> No podrá modificar estos ajustes una vez que complete esta configuración. Sin embargo, si elige Clave personalizada, puede editar la política de la clave personalizada en cualquier momento.

6. (Opcional) En Etiquetas, cree una etiqueta y agréguela a la integración. Puedes añadir hasta 50 etiquetas.
7. En Autorizaciones, seleccione Crear conector y autorizar. Aparece una ventana emergente en la que debe seleccionar Permitir para completar la autorización. Una vez completada la autorización, aparecerá una casilla de verificación que confirma que la autorización se realizó correctamente.
8. En Configuraciones, ingrese el ID del proyecto de Jira Cloud.
9. Seleccione Completar configuración. Después de completar la configuración, puede ver las integraciones configuradas en la pestaña Integraciones configuradas.

Tras configurar la integración con Jira, puedes probar la conexión para confirmar que todo está configurado correctamente en tu entorno de Jira y en Security Hub. Para obtener más información, consulta Cómo probar las integraciones de venta de entradas configuradas.

Detalles adicionales de la integración con Jira

Consideraciones de límites de velocidad

Jira aplica los límites de velocidad de las API para mantener la estabilidad del servicio y garantizar un uso justo en toda su plataforma. Al usar la integración AWS de Security Hub con Jira, estos límites de frecuencia pueden afectar al procesamiento de las conclusiones de Security Hub, especialmente en entornos que generan un gran volumen de hallazgos. Esto puede retrasar la creación de tickets y, en escenarios con un volumen de búsquedas extremadamente alto, es posible que algunos hallazgos no se procesen en absoluto para convertirlos en tickets de Jira. Para optimizar tu integración, considera la posibilidad de implementar filtros en las reglas de automatización de Security Hub para priorizar la venta de tickets en función de los hallazgos más importantes, supervisar el uso de la API de Jira a través de su consola de administración y planificar tu flujo de trabajo en función de los límites de tarifas específicos de tu nivel de licencia de Jira. En el caso de

las implementaciones críticas para la empresa, ponte en contacto con tu administrador de Jira para revisar las asignaciones de los límites de tarifas.

Para obtener información detallada sobre los límites de velocidad de las API de Jira, consulta la documentación sobre límites de velocidad en el sitio web de la Guía para desarrolladores de Atlassian.

Autenticación y seguridad

La autenticación de la API de Jira requiere una configuración adecuada de OAuth 2.0 para un acceso seguro. Asegúrate de que tu aplicación siga las prácticas recomendadas de seguridad de Atlassian para la integración de las API.

Recursos:

- API REST v3 de Jira: documentación de la API REST v3 de Jira en el sitio web de Atlassian
- Implementación de OAuth 2.0 (3LO): guía de implementación de OAuth 2.0 (3LO) en el sitio web de Atlassian
- Administra las aplicaciones de Jira Cloud: recursos de administración de Jira Cloud en el sitio web de Atlassian https://support.atlassian.com/jira-cloud-administration/resources/
- Gestiona los permisos de Jira: gestiona los permisos de los proyectos en el sitio web de Atlassian

Crear un ticket para un Jira Cloud integración

Después de crear una integración con Jira Cloud, puede crear un ticket para un resultado.

> **Note**
>
> Un resultado siempre permanece asociado a un único ticket durante todo su ciclo de vida. Security Hub envía todas las actualizaciones posteriores de un hallazgo al mismo ticket tras su creación inicial. Si se cambia un conector asociado a una regla de automatización, el conector actualizado solo se usa para los hallazgos nuevos y entrantes que coincidan con los criterios de la regla.

Para crear un ticket para un resultado

1. Inicie sesión en su AWS cuenta con sus credenciales y abra la consola de Security Hub en https://console.aws.amazon.com/securityhub/v2/home? region=us-east-1.

2. En el panel de navegación, en Inventario, elija Resultados.
3. Seleccione un resultado. En el resultado, elija Crear ticket.
4. En Integración, abra el menú desplegable y elija una integración. Esta integración es la misma que creó anteriormente cuando configuró el proyecto de Jira Cloud. Elija la integración a la que desea enviar los resultados.
5. Seleccione Crear.

Visualización de un billete para un Jira Cloud integración

Después de crear un ticket para un resultado, puede abrir el ticket en la instancia de Jira Cloud.

Para ver un hallazgo en su Jira Cloud instancia

1. Inicie sesión en su AWS cuenta con sus credenciales y abra la consola de Security Hub en https://console.aws.amazon.com/securityhub/v2/home? region=us-east-1.
2. En el panel de navegación, en Inventario, elija Resultados.
3. Elija el resultado donde creó el ticket.
4. En el resultado, elija el ID del ticket para ver el ticket en la instancia de Jira Cloud o seleccione Ver JSON.

Integraciones para ServiceNow

En este tema, se describe cómo acceder a la consola de Security Hub para configurar una integración para ServiceNow ITSM. Antes de completar cualquiera de los procedimientos de este tema, debe tener una suscripción a ServiceNow ITSM antes de poder agregar esta integración. Para obtener más información, consulte la página de precios en el sitio web de ServiceNow.

Para las cuentas que forman parte de una organización, únicamente el administrador delegado puede configurar una integración. El administrador delegado puede usar manualmente la característica de creación de tickets para cualquier resultado de una cuenta de miembro. Además, el administrador delegado puede usar reglas de automatización para crear tickets de manera automática para cualquier resultado asociado a cuentas de miembro. Al definir una regla de automatización, el administrador delegado puede establecer criterios que incluyan todas las cuentas de miembro o cuentas de miembro específicas. Para obtener información sobre cómo configurar un administrador delegado, consulte Configuración de una cuenta de administrador delegado en Security Hub.

Para las cuentas que no forman parte de una organización, todas las funciones de esta característica están disponibles.

Requisitos previos: configurar ServiceNow el entorno

Debe completar los siguientes requisitos previos antes de configurar una integración para ServiceNow ITSM. De lo contrario, la integración entre Security Hub ServiceNow ITSM y Security Hub no funcionará.

1. Instalación de la integración de resultados de Security Hub para la Administración de servicios de TI (ITSM)

El siguiente procedimiento describe cómo instalar el complemento de Security Hub.

1. Inicie sesión en la instancia de ServiceNow ITSM y luego abra el navegador de aplicaciones.
2. Navega hasta la ServiceNow tienda.
3. Busque Integración de resultados de Security Hub para la Administración de servicios de TI (ITSM) y luego elija Obtener para instalar la aplicación.

> **Note**
>
> En la configuración de la aplicación de Security Hub, elija la acción que desea ejecutar cuando se envíen nuevos resultados de Security Hub al entorno de ServiceNow ITSM. Puedes elegir No hacer nada, Crear incidente, Crear problema o Crear ambos (incident/problem).

2. Configuración del tipo de concesión de credenciales de cliente para solicitudes OAuth entrantes

Debe configurar este tipo de concesión para solicitudes OAuth entrantes. Para obtener más información, consulte Tipo de concesión de credenciales de cliente para OAuth entrante compatible en la página de soporte de ServiceNow.

3. Cómo crear una aplicación OAuth

Si ya creó una aplicación OAuth, puede omitir este requisito previo. Para obtener información sobre la creación de una aplicación de OAuth, consulte Configurar OAuth en el sitio web. ServiceNow

Requisitos previos: configurar AWS Secrets Manager

Para utilizar la integración de Security Hub con ServiceNow, las credenciales de tu aplicación ServiceNow OAuth deben estar almacenadas en Secrets Manager. Almacenar tus credenciales en Secrets Manager te permite tener el control y la visibilidad del uso de las credenciales y, al mismo tiempo, permite a Security Hub utilizarlas para integrarse con tu ServiceNow instancia. Para almacenar tus credenciales en Secrets Manager, debes usar una AWS KMS clave gestionada por el cliente para proteger los secretos. Esta AWS KMS clave le permite proteger los secretos mientras están guardados en reposo y también permite adjuntar una política a la clave que otorga a Security Hub permisos para acceder a la clave que protege el secreto.

Siga los pasos siguientes para configurar Secrets Manager para sus ServiceNow credenciales.

Paso 1: Adjunte una política a su AWS KMS clave

Para configurar correctamente ServiceNow la integración, primero debes conceder a Security Hub permisos para usar la AWS KMS clave asociada a tus ServiceNow credenciales en Secrets Manager.

Para modificar el AWS KMS política de claves para que Security Hub acceda a sus ServiceNow credenciales

1. Abra la AWS KMS consola en https://console.aws.amazon.com/kms.
2. Para cambiar la AWS región, usa el selector de regiones situado en la esquina superior derecha de la página.
3. Selecciona una AWS KMS clave existente o sigue los pasos para crear una nueva clave en la Guía para AWS KMS desarrolladores.
4. En la sección Key policy (Política de claves), elija Edit (Editar).
5. Si aparece Cambiar a la vista de políticas, selecciónela para mostrar la política clave y, a continuación, elija Editar.
6. Copie el siguiente bloque de políticas a su política de AWS KMS claves para conceder a Security Hub permiso para usar su clave.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
        "Sid": "Enable IAM User Permissions",
        "Effect": "Allow",
```

```
        "Principal": {
            "AWS": "arn:aws:iam::your-account-id:root"
        },
        "Action": "kms:*",
        "Resource": "*"
        },
        {
        "Sid": "Allow Security Hub connector service to decrypt secrets",
        "Effect": "Allow",
        "Principal": {
            "Service": "connector.securityhub.amazonaws.com"
        },
        "Action": "kms:Decrypt",
        "Resource": "*",
        "Condition": {
            "StringEquals": {
            "kms:ViaService": "secretsmanager.your-region.amazonaws.com"
            },
            "StringLike": {
            "kms:EncryptionContext:SecretARN": "arn:aws:secretsmanager:your-
region:your-account-id:secret:ServiceNow*"
            }
        }
        }
    ]
    }
```

7. Edita la política sustituyendo los siguientes valores en el ejemplo de política:
   - *your-account-id*Sustitúyala por el identificador de tu AWS cuenta.
   - *your-region*Sustitúyalo por el de su AWS región (por ejemplo,`us-east-1`).
8. Si ha agregado la instrucción de política antes de la instrucción final, agregue una coma antes de agregar esta instrucción. Asegúrese de que la sintaxis JSON de su política de AWS KMS claves sea válida.
9. Seleccione Save.
10. (Opcional) Copie la clave ARN en un bloc de notas para utilizarla en los pasos posteriores.

Paso 2: Crea el secreto en Secrets Manager

Crea un secreto en Secrets Manager que almacenará tus ServiceNow credenciales. Security Hub accederá a este secreto cuando interactúe con su ServiceNow entorno.

Siga los pasos de la Guía del AWS Secrets Manager usuario para crear un secreto. Después de crear el secreto, copie el ARN secreto, ya que lo necesitará para crear el conector de Security Hub.

Al crear el secreto, asegúrese de configurar lo siguiente:

Tipo de secreto

Otro tipo de secreto

Key/value pares (formato de texto plano)

```
{
    "ClientId": "your-servicenow-client-id",
    "ClientSecret": "your-servicenow-client-secret"
    }
```

> **Note**
>
> Los nombres de los campos deben ser exactos `ClientId` y `ClientSecret` (con distinción entre mayúsculas y minúsculas). Security Hub requiere estos nombres exactos para recuperar las credenciales.

Clave de cifrado

Use la AWS KMS clave que configuró en el paso 1

Política de recursos

Utilice la siguiente política de recursos:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
        "Effect": "Allow",
        "Principal": {
            "Service": "connector.securityhub.amazonaws.com"
        },
        "Action": "secretsmanager:GetSecretValue",
        "Resource": "arn:aws:secretsmanager:your-region:your-account-
id:secret:ServiceNow*",
        "Condition": {
```

```
            "StringEquals": {
            "aws:SourceAccount": "your-account-id",
            "aws:SourceArn": "arn:aws:securityhub:your-region:your-account-id:*"
            }
        }
        }
    ]
    }
```

Ahora que su secreto está configurado, puede crear un conector de Security Hub mediante la API o la AWS consola CreateConnector V2. Deberás proporcionar:

- InstanceName: la URL de tu ServiceNow instancia (por ejemplo,`your-instance.service-now.com`)
- SecretArn: El ARN del secreto que creaste en este procedimiento

Configure una integración para ServiceNow ITSM

Security Hub puede crear incidentes o problemas automáticamente en ServiceNow ITSM.

Para configurar una integración para ServiceNow ITSM

1. Inicie sesión en su AWS cuenta con sus credenciales y abra la consola de Security Hub en? https://console.aws.amazon.com/securityhub/v2/home region=us-east-1.
2. En el panel de navegación, elija Administración y luego seleccione Integraciones.
3. En ServiceNow ITSM, elija Agregar integración.
4. En Detalles, escriba un nombre para la integración y determine si desea incluir una descripción opcional para la integración.
5. En el caso de los cifrados, elija cómo quiere cifrar sus credenciales de integración en Security Hub.
    - Usar AWS una clave propia: con esta opción, se usa una clave de servicio propiedad de Security Hub para cifrar los datos de tus credenciales de integración en Security Hub.
    - Elija una clave de KMS diferente (avanzada): con esta opción, elige una AWS KMS key que haya creado y que desea que se utilice para cifrar los datos de sus credenciales de integración en Security Hub. Para obtener información sobre cómo crear una AWS KMS clave, consulte Crear una AWS KMS clave en la Guía para AWS Key Management Service

desarrolladores. Si decide usar su propia clave, debe agregar declaraciones de política a la clave de KMS que permitan a Security Hub acceder a la clave. Consulta las políticas AWS KMS clave para las integraciones de venta de entradas de Security Hub para obtener más información sobre las políticas necesarias.

> **Note**
>
> No podrá modificar estos ajustes una vez que complete esta configuración. Sin embargo, si elige Clave personalizada, puede editar la política de la clave personalizada en cualquier momento.

6. En el caso de las credenciales, introduce tu ServiceNow ITSM URL y el ARN del AWS Secrets Manager secreto que se generó en la sección de requisitos previos.
7. En Etiquetas, determine si desea crear y agregar una etiqueta opcional a la integración.
8. Seleccione Add Integration. Después de completar la configuración, puede ver las integraciones configuradas en la pestaña Integraciones configuradas.

Tras configurar la integración con ServiceNow, puede probar la conexión para confirmar que todo está configurado correctamente en su ServiceNow entorno y en Security Hub. Para obtener más información, consulte Probar las integraciones de venta de entradas configuradas.

Crear un ticket para un ServiceNow ITSM integración

Después de crear una integración con ServiceNow ITSM, puede crear un ticket para un resultado.

> **Note**
>
> Un resultado siempre permanece asociado a un único ticket durante todo su ciclo de vida. Security Hub envía todas las actualizaciones posteriores de un hallazgo al mismo ticket tras su creación inicial. Si se cambia un conector asociado a una regla de automatización, el conector actualizado solo se usa para los hallazgos nuevos y entrantes que coincidan con los criterios de la regla.

Para crear un ticket para un resultado

1. Inicie sesión en su AWS cuenta con sus credenciales y abra la consola de Security Hub en https://console.aws.amazon.com/securityhub/v2/home? region=us-east-1.
2. En el panel de navegación, en Inventario, elija Resultados.
3. Seleccione un resultado. En el resultado, elija Crear ticket.
4. En Integración, abra el menú desplegable y elija una integración.
5. Seleccione Crear.

Visualización de un billete para un ServiceNow ITSM integración

Después de crear un ticket para un resultado, puede abrir el ticket en la instancia de ServiceNow ITSM.

Para ver un hallazgo en su ServiceNow ITSM instancia

1. Inicie sesión en su AWS cuenta con sus credenciales y abra la consola de Security Hub en? https://console.aws.amazon.com/securityhub/v2/home region=us-east-1.
2. En el panel de navegación, en Inventario, elija Resultados.
3. Elija el resultado donde creó el ticket.
4. En el resultado, elija el ID del ticket para ver el ticket en la instancia de ServiceNow ITSM o seleccione Ver JSON.

Políticas clave de KMS para las integraciones de venta de entradas de Security Hub

Al usar claves de KMS administradas por el cliente con integraciones de venta de entradas de Security Hub, es necesario agregar políticas adicionales a la clave de KMS para permitir que Security Hub interactúe con la clave. Además, es necesario agregar políticas que permitan al director que agrega la clave al conector de Security Hub acceder a la clave.

Política de permisos de Security Hub

La siguiente política describe los permisos que Security Hub necesita para poder acceder y usar la clave de KMS asociada a tu Jira y a tus ServiceNow conectores. Esta política debe agregarse a cada clave de KMS asociada a un conector de Security Hub.

La política contiene los siguientes permisos:

- Permite a Security Hub proteger, acceder temporalmente o actualizar los tokens utilizados para comunicarse con tus integraciones de venta de entradas mediante la clave. Los permisos se restringen a operaciones relacionadas con conectores específicos de Security Hub mediante el bloque de condición que verifica el ARN de origen y el contexto de cifrado.
- Permite a Security Hub leer los metadatos sobre la clave de KMS al permitir la `DescribeKey` operación. Este permiso es necesario para que Security Hub verifique el estado y la configuración de la clave. El acceso se restringe a conectores específicos de Security Hub mediante la condición del ARN de origen.

```
{
    "Sid": "Allow Security Hub access to the customer managed key",
    "Effect": "Allow",
    "Principal": {
        "Service": "connector.securityhub.amazonaws.com"
    },
    "Action": [
        "kms:GenerateDataKey",
        "kms:Decrypt",
        "kms:ReEncrypt*"
    ],
    "Resource": "*",
    "Condition": {
        "ArnLike": {
            "aws:SourceArn": "arn:aws:securityhub:Region:AccountId:connectorv2/*"
        },
        "StringLike": {
            "kms:EncryptionContext:aws:securityhub:connectorV2Arn":
 "arn:aws:securityhub:Region:AccountId:connectorv2/*",
            "kms:EncryptionContext:aws:securityhub:providerName": "CloudProviderName"
        }
    }
},
{
    "Sid": "Allow Security Hub read access to the customer managed key",
    "Effect": "Allow",
    "Principal": {
        "Service": "connector.securityhub.amazonaws.com"
    },
```

```
    "Action": [
        "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
        "ArnLike": {
            "aws:SourceArn": "arn:aws:securityhub:Region:AccountId:connectorv2/*"
        }
    }
}
```

Edite la política sustituyendo los siguientes valores en el ejemplo de política:

- Sustituir *CloudProviderName* `JIRA_CLOUD` por o `SERVICENOW`
- *AccountId*Sustitúyalo por el identificador de la cuenta en el que está creando el conector Security Hub.
- *Region*Sustitúyalo por el de su AWS región (por ejemplo,`us-east-1`).

Acceso de entidad principal de IAM para operaciones de Security Hub

Cualquier principal que asigne claves de KMS administradas por el cliente a un conector de Security Hub debe tener permisos para realizar las operaciones clave (describir, generar, descifrar, volver a cifrar y enumerar los alias) para la clave que se está agregando al conector. Esto se aplica a las API V2 y V2. CreateConnector CreateTicket La siguiente declaración de política debe incluirse como parte de la política para cualquier entidad principal que interactúe con estas API.

```
{
    "Sid": "Allow permissions to access key through Security Hub",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::AccountId:role/RoleName"
    },
    "Action": [
        "kms:GenerateDataKey",
        "kms:Decrypt",
        "kms:ReEncrypt*"
    ],
    "Resource": "*",
```

```
    "Condition": {
        "StringEquals": {
            "kms:ViaService": [
                "securityhub.Region.amazonaws.com"
            ]
        },
        "StringLike": {
            "kms:EncryptionContext:aws:securityhub:providerName": "CloudProviderName"
        }
    }
},
{
    "Sid": "Allow read permissions to access key through Security Hub",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::AccountId:role/RoleName"
    },
    "Action": [
        "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:ViaService": [
                "securityhub.Region.amazonaws.com"
            ]
        }
    }
}
```

Edite la política sustituyendo los siguientes valores en el ejemplo de política:

- *RoleName*Sustitúyalo por el nombre del rol de IAM que realiza llamadas a Security Hub.
- Reemplace *CloudProviderName* por `JIRA_CLOUD` o `SERVICENOW`.
- *AccountId*Sustitúyalo por el ID de la cuenta en la que está creando el conector de Security Hub.
- *Region*Sustitúyalo por el de su AWS región (por ejemplo,`us-east-1`).

Probar las integraciones de venta de entradas configuradas

En el caso de ServiceNow las integraciones y Jira configuradas, puedes probar la conexión para asegurarte de que se ha completado toda la configuración en Security Hub y en tu Jira o entorno. ServiceNow

La función de ticket de prueba crea un ticket con el título de. `TESTING Test CreateTicketV2 Finding` El ticket de prueba contiene datos de muestra, como el identificador de la cuenta y la región de la cuenta en la que se realiza la prueba, los detalles de los recursos de muestra y el ejemplo de AWS Finding JSON.

Probar las integraciones mediante la consola

Siga los pasos siguientes para probar la integración:

1. En el panel de navegación de Security Hub, seleccione Integraciones.
2. En la pestaña Integraciones configuradas, elija la integración que desea probar.
3. En la página de resumen de tu integración, selecciona Crear ticket de prueba.
4. Security Hub muestra un mensaje de éxito y un enlace al ticket de prueba si la prueba se realiza correctamente. Si la prueba no se realiza correctamente, Security Hub muestra un error. Según el mensaje de error, solucione los problemas de configuración en Security Hub o en su Jira ServiceNow entorno.

> **Note**
>
> La función de tickets de prueba tiene como objetivo ayudar a verificar la funcionalidad integral para la configuración de una nueva conexión o cuando se realizan cambios en una conexión existente. Esta función crea un nuevo ticket en tu Jira ServiceNow entorno cada vez que la utilizas y no está destinada a la verificación periódica de tu conexión.

Probando con el AWS CLI

Para probar la integración mediante AWS CLI, utilice el `create-ticket-v2` comando con el `--mode DRYRUN` parámetro:

```
aws securityhub create-ticket-v2 \
```

```
  --mode DRYRUN \
  --region <your-region> \
  --connector-id <your-connector-id> \
  --finding-metadata-uid "TEST_FINDING"
```

Ejemplo

El siguiente ejemplo muestra cómo probar una integración:

```
aws securityhub create-ticket-v2 \
  --mode DRYRUN \
  --region us-east-1 \
  --connector-id "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
  --finding-metadata-uid "TEST_FINDING"
```

Respuesta exitosa

Una respuesta correcta devuelve lo siguiente:

```
{
    "TicketId": "a1b2c3d4e5f6g7h8i9j0k1l2m3n4o5p6",
    "TicketSrcUrl": "https://your-instance.service-now.com/nav_to.do?
uri=x_aws_se_0_finding.do?sys_id=a1b2c3d4e5f6g7h8i9j0k1l2m3n4o5p6"
}
```

La `TicketSrcUrl` respuesta proporciona un enlace directo para ver el ticket de prueba en tu Jira o en tu ServiceNow entorno.

Si la prueba falla, aparece un mensaje de error que indica el problema de configuración que debe solucionarse.

Solución de errores de integración en la nube de Jira

Al probar la integración Jira Cloud desde Security Hub, es posible que aparezcan los siguientes mensajes de error. Estos mensajes de error pueden proporcionar información sobre dónde podría estar el problema de configuración del conector y cómo solucionarlo.

Mensajes de error de integración con Jira Cloud

Error	Mensaje de error	Causa probable y solución
ConflictException	No se puede encontrar el proyecto de Jira	Causa probable: el proyecto del conector es incorrecto o hay credentials/permissions un problema que nos impide acceder al proyecto. Solución probable: añade el proyecto correcto al conector o vuelve a autenticarte en Jira con las credenciales correctas.
ConflictException	No se encontró el tipo de problema de Security Hub	Causa probable: el problema o el tipo de problema de instalación de la aplicación no están asociados al proyecto. Solución probable: realiza el paso previo para instalar la aplicación de Jira en tu entorno de Jira y asociarla al proyecto.

Aplicación MCP (versión preliminar)

Security Hub ofrece una experiencia de agencia con una aplicación de protocolo de contexto modelo (MCP). Con esta aplicación, su agente de IA puede investigar los hallazgos de exposición. También puede diagnosticar un conector de Azure existente o evaluar los requisitos previos del conector de Azure antes de crearlo.

Cada llamada a la herramienta de búsqueda devuelve un resumen en texto para que el agente razone. Cuando está disponible, también devuelve una visualización interactiva para que la compruebes en la misma conversación. Connector Diagnostics muestra un texto estructurado que separa los hallazgos confirmados de las comprobaciones que no se pudieron verificar.

La aplicación MCP es un servidor MCP local que se ejecuta en su máquina y llama directamente a las API de Security Hub con sus credenciales existentes AWS . Connector Diagnostics también

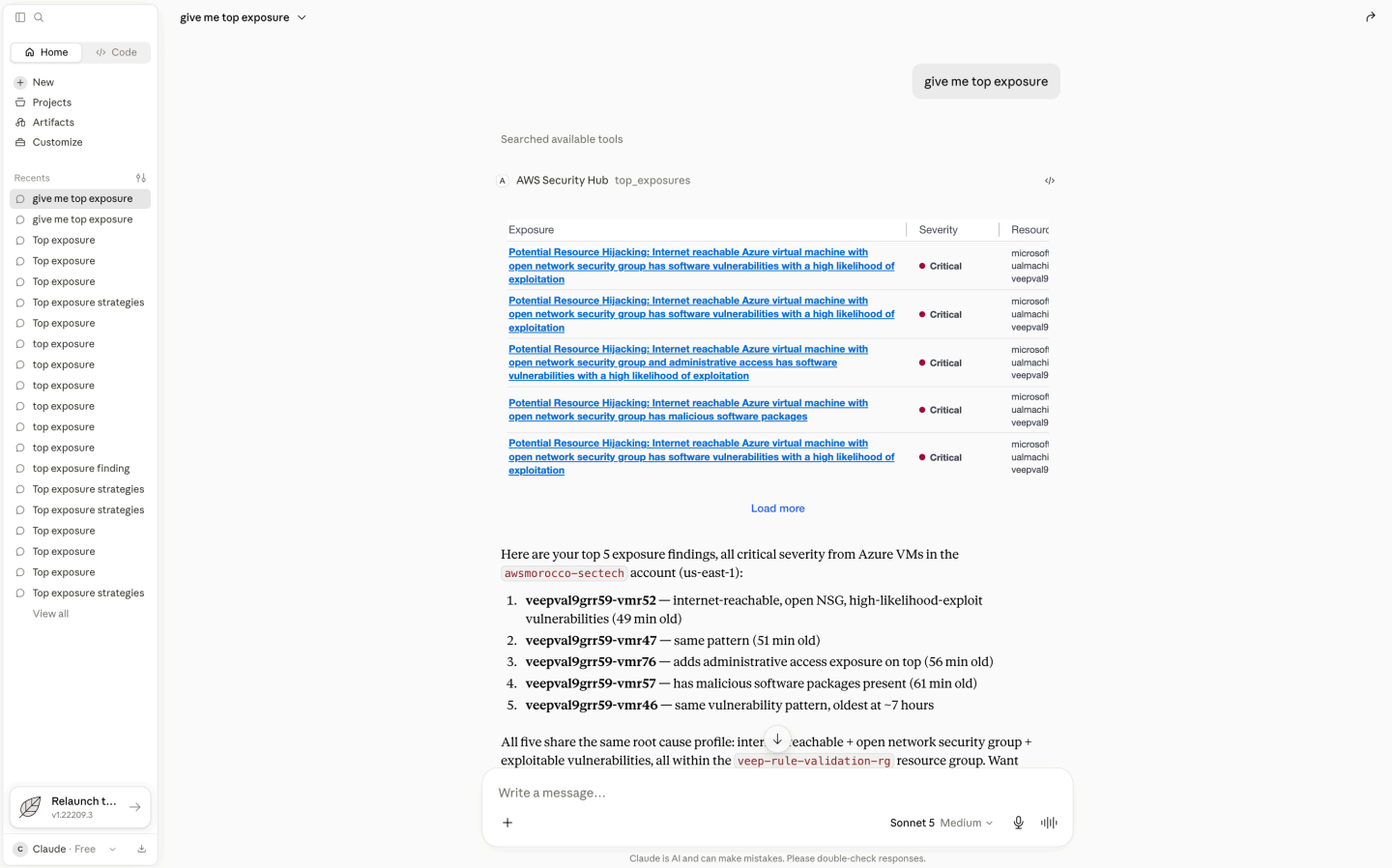
puede ejecutar consultas de la CLI de Azure limitadas y de solo lectura mediante la sesión de la CLI de Azure existente. Todas las herramientas son de solo lectura y no modifican la postura de seguridad ni los recursos del conector. La aplicación MCP está disponible en todas las regiones AWS comerciales en las que Security Hub está disponible.

> **Important**
>
> La versión preliminar de la aplicación Security Hub MCP está en versión preliminar pública.

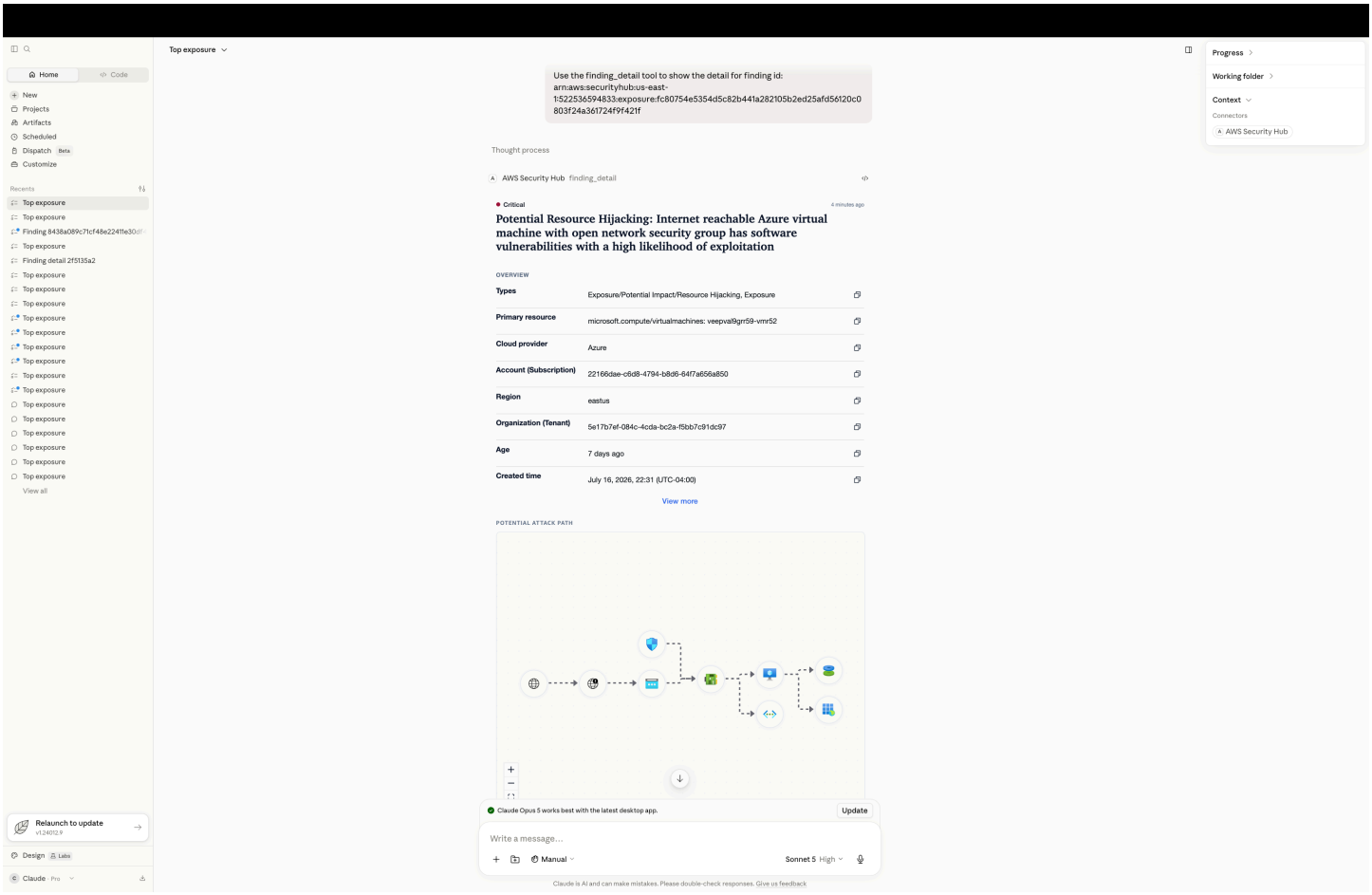
Ejemplos de la aplicación MCP

Los siguientes ejemplos muestran cómo la aplicación MCP representa visualizaciones interactivas en Claude Desktop mientras usted investiga sus exposiciones.

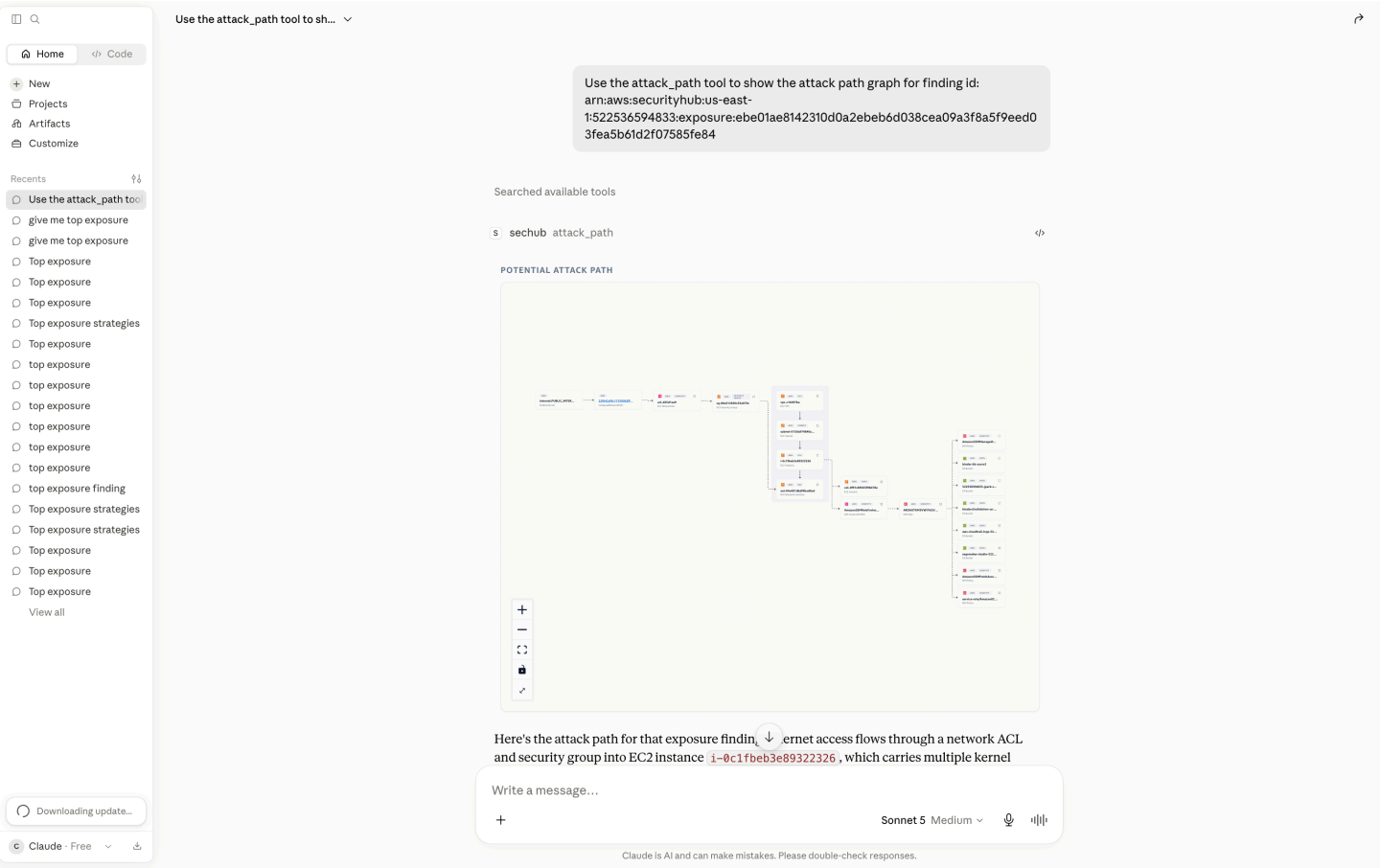
Exposiciones principales: enumera sus hallazgos de exposición más importantes en una tabla interactiva. La siguiente imagen muestra la tabla de exposiciones principales.



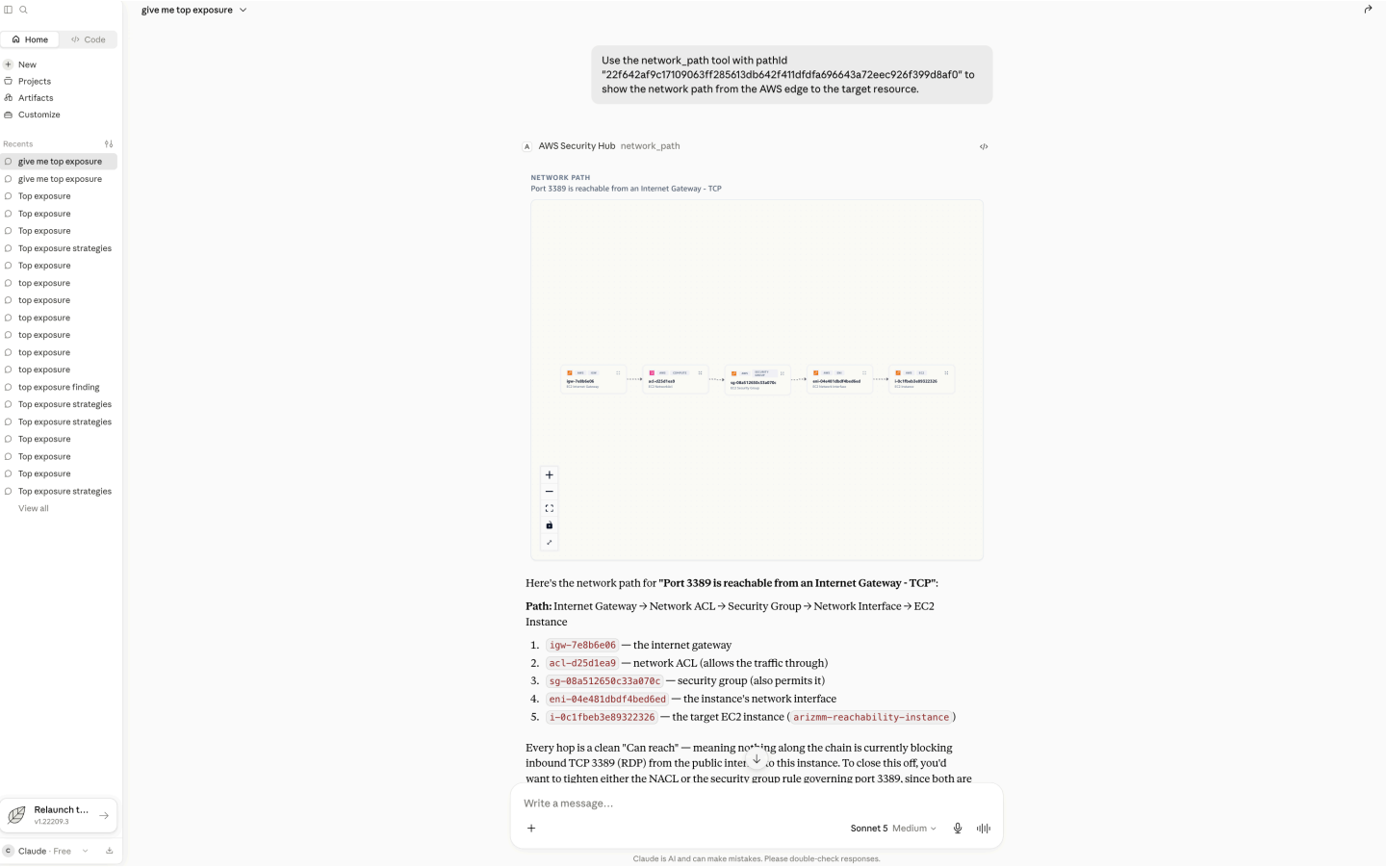
Detalle detallado: consulte la descripción general de un solo hallazgo de exposición, junto con su resumen de características correlacionadas, la ruta de ataque y la guía para solucionarlo. En la imagen siguiente se muestra la vista detallada de la búsqueda.



Ruta de ataque: visualice cómo se puede acceder a una exposición en forma de gráfico interactivo. Los nodos representan recursos, identidades y servicios. Los bordes representan las relaciones entre ellos. La siguiente imagen muestra el gráfico de la trayectoria del ataque.



Ruta de red: explore los saltos de red ordenados desde el AWS extremo hasta el recurso de destino (por ejemplo, de Internet Gateway a NACL, a Security Group, a ENI y a Instance). En la imagen siguiente se muestra la ruta de red.



Diagnóstico del conector: pregunte por qué un conector de Azure existente está degradado o ha fallado. El agente identifica los problemas confirmados, distingue las comprobaciones que no se han podido verificar y recomienda la más mínima reparación sin cambiar el entorno.

Preparación del conector: compruebe los requisitos previos de Azure antes de crear un conector. El agente informa de los requisitos previos que se han cumplido, los que han fallado o los que no se han podido verificar.

Conceptos clave

Detección de exposición: conclusión que correlaciona varias señales (como las vulnerabilidades, los errores de configuración, la accesibilidad de la red y los datos confidenciales) en una vista única de un recurso que está expuesto al riesgo.

Diagnóstico de conectores: tres herramientas de solo lectura para los conectores de Azure. Las herramientas diagnostican un conector existente, evalúan una configuración propuesta y recuperan extractos exactos del script de configuración de Azure compatible. El agente selecciona las herramientas y traduce sus resultados estructurados en una explicación.

Servidor MCP local: programa que se ejecuta en su computadora y actúa como un puente bidireccional seguro entre Claude Desktop y Security Hub. El servidor contiene las herramientas que usa tu agente de IA, incluidas las herramientas que renderizan la interfaz de usuario en Claude Desktop. Utiliza la cadena de AWS credenciales de tu máquina y no contiene credenciales propias.

Aplicación MCP: una aplicación interactiva que se renderiza dentro de Claude Desktop. Cada vista de la aplicación MCP realiza una única función, como mostrar la tabla de exposiciones más altas o un gráfico de la trayectoria de los ataques.

Respuesta dual: una sola llamada a la herramienta de búsqueda arroja dos resultados: un resumen en texto compacto sobre el que el agente razona y una visualización interactiva representada en la misma conversación para que la revise.

Requisitos previos

- Una AWS cuenta con Security Hub activado. Los hallazgos de exposición son necesarios solo para los hallazgos y las herramientas de exposición.
- Claude Desktop instalado. Para ver el instalador, consulte la descarga de Claude Desktop en el sitio web de Claude.
- AWS credenciales configuradas en tu cadena de credenciales de AWS SDK estándar.
- Para el diagnóstico de Azure-side conectores, instale la CLI de Azure. Para autenticarse con el arrendatario del conector `az login --tenant`*`tenant-id`*, ejecute, donde *`tenant-id`* está el ID del arrendatario de Azure que contiene el conector. La aplicación MCP usa la sesión CLI local de Azure resultante. No agregue credenciales de Azure a la configuración de MCP.

> **Note**
>
> Puede ejecutar Connector Diagnostics sin una sesión autenticada de la CLI de Azure. El resultado incluye la evaluación disponible AWS y marca las Azure-dependent comprobaciones como no verificadas. Nunca considera que las pruebas de Azure no disponibles estén en buen estado.

Configuración del servidor MCP

La aplicación MCP se instala en Claude Desktop desde un archivo de paquete. Antes de instalarla, confirme que se `aws sts get-caller-identity` ha realizado correctamente y que `aws`

`configure get region` devuelve una región en su terminal para que el servidor pueda leer sus AWS credenciales y su región.

1. Descargue el paquete de aplicaciones MCP de Security Hub.
2. Abra el `.mcpb` archivo descargado. Claude Desktop inicia un flujo de configuración. Siga las instrucciones para instalar el servidor.
3. Para verificar la conexión, escribe una pregunta en Claude Desktop, como «¿Cuáles son mis principales riesgos de seguridad?» o «Mi conector Azure en us-west-2 está degradado. ¿Puede determinar qué es lo que está mal?» Si recibes un error, consulta las instrucciones del mensaje de error y confirma tus credenciales y tu región.

Uso del diagnóstico del conector

Describa el problema del conector o la configuración propuesta en lenguaje natural. El agente selecciona la herramienta de solo lectura adecuada, interpreta su resultado estructurado y le indica qué comprobaciones se confirmaron y cuáles no.

Diagnostica un conector existente

1. Identifique el conector por su ID de conector o su nombre exacto. Indique también la AWS cuenta y la región que contienen el conector si el agente no puede determinarlos a partir de su solicitud.
2. Haga una pregunta como: «Mi conector de Azure en us-west-2 está degradado. ¿Puedes determinar qué es lo que está mal y decirme qué debo corregir primero?»
3. Revisa los hallazgos confirmados por separado de las comprobaciones que no se verificaron. Cuando la autenticación de Azure no está disponible, el agente limita sus conclusiones a las pruebas AWS complementarias.

Evalúe un conector propuesto

1. Proporcione la AWS cuenta, la AWS región y el ID de inquilino de Azure. Proporcione también de 1 a 10 identificadores de suscripción de Azure que cubrirá el conector propuesto. Indique al agente qué requisitos previos de servicio debe evaluar: la gestión del estado de seguridad en la nube (CSPM), el escaneo de máquinas virtuales de Inspector o la detección de amenazas. Estas selecciones abarcan las comprobaciones de disponibilidad. No son ajustes de creación de conectores.

2. Haga una pregunta como la siguiente: «Antes de crear mi conector de Azure, compruebe si están listos los requisitos previos para estas suscripciones».
3. Revise las comprobaciones aprobadas, fallidas y no verificadas. Un resultado de preparación correcto significa que se han superado los requisitos previos comprobados. No significa que exista un conector, que esté funcionando o que se haya recuperado.

Recupera las instrucciones de configuración

Si un resultado hace referencia a un paso de incorporación, pídele al agente que muestre ese paso. Por ejemplo, pregunte «Muéstrame el paso 6 del script de configuración del conector de Azure compatible». Para ver el script completo, consulte Configurar Microsoft Azure para que se integre con Security Hub. La herramienta devuelve un extracto exacto, pero no lo ejecuta. Ejecute todo el script compatible, ya que sus pasos comparten funciones de configuración y de ayuda.

> **Note**
>
> Connector Diagnostics nunca repara ni cambia los recursos. La corrección es una guía para una acción independiente que usted controla. El diagnóstico informa de la recuperación solo cuando hay pruebas recientes en tiempo de ejecución que lo demuestren.

Herramientas disponibles

`top_exposures`— Enumera sus hallazgos de exposición más urgentes en forma de tabla interactiva. Utilice primero esta herramienta porque las herramientas de búsqueda previa requieren un identificador de búsqueda de esta lista.

`finding_detail`— Muestra la descripción general de un hallazgo, incluido el resumen de las características de búsqueda correlacionadas.

`finding_overview`— Devuelve un resumen textual de un hallazgo por ID de búsqueda.

`correlated_finding_detail`— Enumera los hallazgos relacionados con una exposición para un solo rasgo, como la vulnerabilidad, la mala configuración o la accesibilidad.

`attack_path`— Crea el gráfico de la trayectoria del ataque para un hallazgo.

`network_path`— Amplía la ruta de red de un hallazgo en saltos ordenados desde el AWS borde hasta el recurso objetivo.

`recommendation`— Devuelve una guía para corregir un hallazgo, incluidos los enlaces a la documentación.

`resource_detail`— Devuelve la configuración de un AWS recurso mediante un identificador corto (por ejemplo,`i-1234`) o un ARN.

`diagnose_connector`— Diagnostica un conector de Azure existente mediante el estado de Security Hub y las pruebas limitadas de la CLI de Azure, cuando estén disponibles. Muestra los hallazgos confirmados, el alcance de los afectados, las directrices de corrección y la actualización de los datos. También contiene una lista de las comprobaciones que no se han podido verificar.

`assess_connector_readiness`— Evalúa el AWS lado y los Azure-side requisitos previos de un conector de Azure propuesto antes de crearlo. No crea un conector.

`get_connector_setup_instructions`— Devuelve extractos exactos del script de incorporación de Azure empaquetado y compatible. No ejecuta el script.

Supervisión del uso y los costos en Security Hub

La página de uso lo ayuda a comprender y administrar los costos de ejecutar Security Hub en toda la organización. En esta página, puede ver sus costos actuales, ver los costos mensuales proyectados, explorar el uso por capacidad o por cuenta y encontrar estrategias para optimizar sus gastos.

¿Quién puede acceder a la página de uso

La página de uso está disponible en cualquier cuenta que tenga activado Security Hub. Para acceder a ella, abra la consola de Security Hub y seleccione Uso en la sección Configuración del panel de navegación.

> **Important**
>
> Si su cuenta es una cuenta de miembro de una AWS organización y no se ha designado a un administrador delegado de Security Hub, los datos de uso no están disponibles. Para ver los datos de uso, la cuenta de administración de su organización debe designar un administrador delegado. Para obtener más información, consulte the section called “Designación de un administrador delegado”.

La experiencia varía según el tipo de cuenta:

- Cuenta de administración o administrador delegado: verás la página de uso completa con un resumen de los costos de la organización, el uso por capacidad, el uso por cuenta y las estrategias de optimización de costos.
- Cuenta de miembro o cuenta independiente: verá un resumen de los costos de la cuenta con el uso por capacidad únicamente para su cuenta. La pestaña Por cuenta no está disponible porque estás viendo una sola cuenta.

Resumen de costos de la organización y la cuenta

> **Note**
>
> La sección de resumen de costos de la organización solo está visible desde la cuenta de administrador delegado o desde la cuenta de administración. En su lugar, las cuentas de miembros y las cuentas independientes muestran un resumen de los costos de la cuenta.

Cuando abres la página de uso desde una cuenta de administración o administrador delegado, la sección Resumen de los costos de la organización muestra un resumen detallado de los costos de Security Hub de tu organización para el ciclo de facturación actual. Esta sección incluye lo siguiente:

- Datos actualizados por última vez: la fecha en la que Security Hub actualizó por última vez los datos de uso de su organización. Security Hub actualiza estos datos periódicamente. Si los datos tienen más de 24 horas cuando visita la página de uso, Security Hub activa automáticamente una actualización. La actualización se completa en unas pocas horas, según el tamaño de la organización. Mientras se actualizan los datos, aparece una alerta con un mensaje que indica que los datos estarán disponibles en breve.
- Costos actuales: el importe total en el que ha incurrido su organización para usar Security Hub desde el inicio del ciclo de facturación actual hasta la fecha en que se actualizaron los datos por última vez.
- Costos mensuales proyectados (30 días): un costo mensual estimado basado en los últimos 7 días de uso, extrapolado a un ciclo de facturación completo de 30 días. Esta proyección incluye el uso de la prueba gratuita y de pago para ofrecerte una estimación realista de tus costos mensuales. Los costos proyectados no tienen en cuenta los descuentos (EDP) con AWS los que hayas negociado. Si tus costos proyectados parecen ser más bajos que tus costos actuales, eso significa que tu consumo ha ido disminuyendo y, teniendo en cuenta el uso de los últimos 7 días, la factura de 30 días será más baja que la del ciclo de facturación actual.

Vista de capacidad

La vista de capacidad muestra los costos y el uso en toda la organización, organizados por capacidad de seguridad. Las capacidades se organizan en tres grupos ampliables. Puede expandir o reducir cada grupo para ver los tipos de uso individuales que contiene. Cada tipo de uso se asigna directamente al tipo de uso correspondiente en AWS Cost Explorer.

Plan básico de Security Hub: supervisa las instancias de EC2, las imágenes de contenedores de ECR, las funciones de Lambda, los usuarios de IAM y las funciones de IAM. Incluye el análisis de riesgos y exposición, la gestión de vulnerabilidades (con la tecnología de Amazon Inspector), la gestión de la postura de seguridad (con la tecnología de Security Hub CSPM) y la respuesta de seguridad. Todas estas funciones están incluidas en el plan Essentials a un precio único por recurso; no es necesario que habilites o pagues por separado Amazon Inspector o AWS Security Hub CSPM, y no tendrás que pagar el doble por el uso del servicio subyacente.

Análisis de amenazas: incluye los eventos CloudTrail de administración y los eventos de datos, la actividad de la red y otros registros. Estas capacidades abarcan la detección de amenazas con la tecnología de Amazon GuardDuty.

Capacidades adicionales: incluye el escaneo de código de las funciones de Lambda. Se trata de una mejora opcional con tecnología de Amazon Inspector para analizar el código de las aplicaciones de funciones de Lambda en busca de vulnerabilidades de seguridad.

Para obtener más información sobre los precios de cada capacidad, consulte los precios https://aws.amazon.com/security-hub/pricing/ de Security Hub.

La tabla de esta vista incluye las siguientes columnas para cada tipo de uso:

- Uso actual: el volumen total de uso de este tipo de uso desde el inicio del ciclo de facturación hasta la fecha en que se actualizaron los datos por última vez, en todas las cuentas y en todas las regiones.
- Uso gratuito: el volumen de uso total de este tipo de uso en las cuentas que se encuentran actualmente en la prueba gratuita. Los valores de uso gratuito aparecen en verde.
- Costos actuales: el coste total de este tipo de uso desde el inicio del ciclo de facturación hasta la fecha en que se actualizaron los datos por última vez, en todas las cuentas y en todas las regiones.
- Valor de la prueba gratuita: el costo en el que habría incurrido por este tipo de uso si las cuentas que actualmente están en la prueba gratuita no estuvieran en la prueba. Esto le ayuda a comprender el valor de la prueba gratuita.

- Costos mensuales proyectados (30 días): el costo mensual estimado de este tipo de uso, extrapolado a partir de los últimos 7 días de uso en todas las cuentas y en todas las regiones. Esto incluye el uso de la prueba gratuita y de pago para obtener un costo mensual estimado.

Vista de la cuenta

> **Note**
>
> La vista de la cuenta solo está disponible desde la cuenta de administrador delegado o la cuenta de administración.

Elija la vista de cuenta para ver los costos organizados por cuentas de miembros individuales en todas las regiones. Esta vista le ayuda a identificar qué cuentas generan los mayores costos.

La tabla muestra cada cuenta con las siguientes columnas:

- Cuenta: el Cuenta de AWS ID, que se muestra como un enlace en el que se puede hacer clic. Al elegir una cuenta, se abre un panel de desglose detallado.
- Costos actuales: el coste total de esta cuenta desde el inicio del ciclo de facturación hasta la fecha en que se actualizaron los datos por última vez, en todas las regiones.
- Valor de la prueba gratuita: el costo en el que habría incurrido esta cuenta si no hubiera estado en la prueba gratuita.
- Costos mensuales proyectados (30 días): un costo mensual estimado de esta cuenta, extrapolado de los últimos 7 días de uso en todas las regiones a un ciclo de facturación completo de 30 días. La proyección incluye el uso de la prueba gratuita y de pago para ofrecer una estimación representativa de tus costos mensuales. Los costos proyectados no tienen en cuenta ningún descuento con el que hayas negociado AWS (EDP).

  Si Security Hub se activó en esta cuenta en los últimos 7 días, la proyección se basa en el número de días transcurridos desde la activación. Transcurridos 7 días, la proyección utiliza la totalidad de los últimos 7 días de uso. La página de uso no detecta actualmente cuándo se ha desactivado Security Hub en una cuenta. Si Security Hub se ha desactivado recientemente en una o más cuentas, esas cuentas seguirán apareciendo en la proyección hasta que se acabe su uso. Una vez realizados estos cambios, espere 7 días para que la proyección refleje el estado actualizado de su organización.

Vista detallada de la cuenta

Al elegir una cuenta de la lista, se abre un panel de detalles en la parte derecha de la página. Este panel muestra el mismo desglose por niveles de capacidad que en la vista de capacidades, pero se filtra para esa cuenta específica. Puedes ver el uso actual, el uso gratuito, los costos actuales, el valor de la prueba gratuita y los costos mensuales proyectados para cada tipo de uso de esa cuenta, en todas las regiones.

Estrategias de optimización de costos

Elige estrategias de optimización de costos en la página de uso para acceder a una página específica con formas prácticas de administrar tus costos y, al mismo tiempo, mantener la cobertura de seguridad.

Cada estrategia se presenta como una opción independiente que puede evaluar y aplicar en función de las necesidades de su organización. Las opciones sin concesiones de seguridad se enumeran en primer lugar. Después de aplicar cualquier estrategia, los cambios suelen tardar entre 24 y 48 horas en reflejarse en la facturación.

Recursos relacionados

- Precios de Security Hub
- AWS Guía del usuario de Cost Explorer

Deshabilitación de Security Hub

Desactivar Security Hub para una sola cuenta

Si su cuenta no forma parte de una organización, puede deshabilitar Security Hub en la consola de Security Hub en cualquier momento o usar la DisableSecurityHubV2 API. Cuando inhabilitas Security Hub, deja de recopilar los hallazgos de los motores de detección y, además, pierdes el acceso a los hallazgos, integraciones y configuraciones existentes.

Si inhabilitas Security Hub para tu cuenta en todas las regiones, Security Hub también elimina el IAM Access Analyzer vinculado al servicio que se creó cuando habilitaste el servicio. Si la eliminación automática falla, puedes eliminar el analizador llamando a la operación de la API de IAM Access Analyzer. `DeleteServiceLinkedAnalyzer` Esta operación solo se realiza correctamente después de que Security Hub esté completamente inhabilitado para su cuenta. Si inhabilitas Security Hub en

una sola región pero permaneces activado en otras regiones, el analizador de acceso no utilizado seguirá ejecutándose y los resultados se seguirán replicando en las demás regiones habilitadas.

Para deshabilitar Security Hub

1. Inicie sesión en su AWS cuenta con sus credenciales y abra la consola de Security Hub en. https://console.aws.amazon.com/securityhub/v2/home
2. En el panel de navegación, seleccione General.
3. En Security Hub, selecciona Desactivar. En la ventana emergente**`Disable`**, escribe y elige Desactivar.

Deshabilitar Security Hub en una organización

Si es el administrador delegado de una AWS organización, tiene dos opciones para deshabilitar Security Hub en las cuentas de los miembros.

Opción 1: deshabilitar Security Hub con motores de detección

Puedes aprovechar la política y la implementación de Security Hub (funciones esenciales y adicionales) del catálogo de políticas de tu cuenta de administrador delegado para inhabilitar Security Hub junto con Amazon Inspector en unidades organizativas, cuentas o regiones específicas.

Para inhabilitar Security Hub y Amazon Inspector en las cuentas de los miembros, utiliza una política

1. Inicia sesión con tu AWS cuenta con tus credenciales de administrador delegado. Abra la consola de Security Hub en https://console.aws.amazon.com/securityhub/v2/home.
2. En el panel de navegación, seleccione Administración y, a continuación, seleccione Configuraciones.
3. Elija Security Hub (funciones esenciales y adicionales) en el catálogo de configuración.
4. En la página Configurar Security Hub, en la sección de detalles, introduzca un nombre y una descripción para la política (por ejemplo, «Política de desactivación de Security Hub»).
5. En la sección Selección de cuentas, seleccione una de las siguientes opciones. Selecciona Todas las unidades organizativas y cuentas si quieres aplicar la desactivación a todas las unidades organizativas y cuentas. Selecciona Unidades organizativas y cuentas específicas si quieres aplicar la inhabilitación a unidades organizativas y cuentas específicas. Si eliges esta opción, usa la barra de búsqueda o el árbol de estructura organizativa para especificar las unidades organizativas y cuentas de destino.

6. En la sección Regiones, selecciona Deshabilitar todas las regiones para deshabilitar Security Hub en todas las regiones. Si lo desea, elija si desea deshabilitar automáticamente las nuevas regiones. Seleccione Especificar regiones para elegir qué regiones específicas quiere deshabilitar.
7. (Opcional) Para ver la configuración avanzada, consulta la guía de AWS Organizations.
8. (Opcional) En el caso de las etiquetas de recursos, añada etiquetas como pares clave-valor para poder identificar fácilmente la configuración.
9. Elija Siguiente.
10. Revise los cambios y luego seleccione Aplicar. Las cuentas de destino se configuran según la política. El estado de configuración de su política aparece en la parte superior de la página de políticas.

Deshabilitar Amazon GuardDuty y AWS CSPM de Security Hub

En el GuardDuty caso de las capacidades de CSPM de Security Hub, debe inhabilitarlas manualmente desde las respectivas cuentas de administrador delegado. GuardDuty y Security Hub CSPM utilizan implementaciones (acciones únicas) en lugar de políticas, por lo que la desactivación debe realizarse manualmente desde sus respectivas consolas.

Opción 2: deshabilitar Security Hub únicamente

Si ya tienes una política de Security Hub y quieres inhabilitar Security Hub únicamente, sin que ello afecte a Amazon Inspector ni al CSPM de Security Hub, sigue estos pasos. GuardDuty

Para inhabilitar Security Hub solo en las cuentas de los miembros

1. Inicia sesión con tu AWS cuenta con tus credenciales de administrador delegado. Abra la consola de Security Hub en https://console.aws.amazon.com/securityhub/v2/home.
2. En el panel de navegación, seleccione Administración y, a continuación, seleccione Configuraciones.
3. Elija cualquiera de sus políticas de Security Hub en las políticas configuradas.
4. Elija Editar política y, en la sección Selección de cuentas, seleccione una de las siguientes opciones. Selecciona Todas las unidades organizativas y cuentas si quieres aplicar la inhabilitación a todas las unidades organizativas y cuentas. Selecciona Unidades organizativas y cuentas específicas si quieres aplicar la inhabilitación a unidades organizativas y cuentas específicas. Si eliges esta opción, usa la barra de búsqueda o el árbol de estructura organizativa para especificar las unidades organizativas y cuentas de destino.

5. En la sección Regiones, selecciona Deshabilitar todas las regiones para deshabilitar Security Hub en todas las regiones. Si lo desea, elija si desea deshabilitar automáticamente las nuevas regiones. Seleccione Especificar regiones para elegir qué regiones específicas quiere deshabilitar.
6. (Opcional) Para ver la configuración avanzada, consulta la guía de AWS las organizaciones.
7. (Opcional) En el caso de las etiquetas de recursos, añada etiquetas como pares clave-valor para poder identificar fácilmente la configuración.
8. Elija Siguiente.
9. Revise los cambios y luego seleccione Aplicar. Las cuentas de destino se configuran según la política. El estado de configuración de su política aparece en la parte superior de la página de configuraciones.

Impacto en otros servicios de seguridad

La desactivación de Security Hub mediante una política de Security Hub no afecta a las configuraciones de Security Hub GuardDuty, CSPM y Amazon Inspector.

Si necesitas inhabilitar Amazon Inspector solo en las cuentas de los miembros, puedes usar la política de gestión de vulnerabilidades del catálogo de configuración de Security Hub. Diríjase a la página de configuración de Security Hub, seleccione la gestión de vulnerabilidades de Amazon Inspector y cree una política de inhabilitación siguiendo los pasos similares a los del procedimiento de desactivación de Security Hub anterior.

Seguridad enAWSSecurity Hub

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de una arquitectura de centro de datos y red diseñada para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre usted AWS y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la AWS nube. AWStambién le proporciona servicios que puede utilizar de forma segura. Third-partylos auditores prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los programas de AWS cumplimiento. Para obtener más información

sobre los programas de conformidad que se aplican a Security Hub, consulte AWSServicios incluidos en el ámbito de aplicación por programa de conformidad.

- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. También es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y la normativa aplicables.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida al utilizar Security Hub. En los siguientes temas le mostramos cómo configurar Security Hub para satisfacer sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros AWS servicios que le ayudan a supervisar y proteger los recursos de Security Hub.

Temas

- Protección de datos enAWSSecurity Hub
- AWS Administración de identidades y accesos para Security Hub
- Validación de conformidad para AWS Centro de seguridad
- Resiliencia en AWS Centro de seguridad
- Seguridad de infraestructura en AWS Centro de seguridad
- AWS Puntos finales de VPC de interfaz y centro de seguridad (AWS PrivateLink)

Protección de datos enAWSSecurity Hub

El modelo de se aplica a la protección de datos en AWS Security Hub. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta todos losNube de AWS. Eres responsable de mantener el control sobre el contenido alojado en esta infraestructura. También eres responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulte las Preguntas frecuentes sobre privacidad de datos y los . Para obtener más información sobre la protección de datos en Europa, consulte el Centro del Reglamento General de Protección de Datos (RGPD).

Para fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure usuarios individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utiliza la autenticación multifactor (MFA) en cada cuenta.
- Se utiliza SSL/TLS para comunicarse con AWS los recursos. Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios conAWS CloudTrail. Para obtener información sobre el uso de CloudTrail senderos para capturar AWS actividades, consulte Cómo trabajar con CloudTrail senderos en la Guía del AWS CloudTrail usuario.
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminadosServicios de AWS.
- Utiliza servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger la información confidencial almacenada en Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-3 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-3.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabajas con Security Hub u otro dispositivo Servicios de AWS mediante la consola, la API o AWS los SDK. AWS CLI Cualquier dato que introduzca en etiquetas o campos de formato libre utilizados para los nombres se pueden emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya información de credenciales en la URL a fin de validar la solicitud para ese servidor.

Security Hub es una oferta de servicio para varios clientes. Para ayudar a proteger sus datos, Security Hub cifra los datos en reposo y los datos en tránsito entre los servicios de los componentes.

Desactivación del uso de los datos para mejorar el servicio

> **Note**
>
> Esta página de documentación solo se aplica al AWS Security Hub mejorado lanzado el 2 de diciembre de 2025. Si es cliente del Security Hub original (ahora AWS AWS Security Hub CSPM), el uso de datos que se describe a continuación solo se aplicará una vez que haya habilitado el AWS Security Hub mejorado.

Puedes optar por que tus datos (definidos como «contenido de Security Hub» en las condiciones de servicio de Security Hub) no se utilicen para desarrollar y mejorar AWS Security Hub y otros servicios de AWS seguridad mediante la política de exclusión de la AWS organización. Puede optar por excluirse incluso si Security Hub no recopila actualmente ningún contenido de este tipo. Para más información sobre cómo excluirse, consulte Políticas de exclusión de servicios de IA en la Guía del usuario de AWS Organizations .

> **Note**
>
> Para poder utilizar la política de exclusión voluntaria, las AWS organizaciones deben administrar sus AWS cuentas de forma centralizada. Si aún no has creado una organización para tus AWS cuentas, consulta Cómo crear y administrar una organización en la Guía del AWS Organizations usuario.

La exclusión tiene los siguientes efectos:

- Security Hub eliminará el contenido que recopiló y almacenó para mejorar el servicio antes de que te des de baja (si lo hubiera).
- Tras darse de baja, Security Hub ya no recopilará ni almacenará este Contenido para mejorar el servicio.

En la siguiente sección, se explica cómo Security Hub gestionará su contenido para mejorar el servicio.

AWS Uso de datos de Security Hub

Actualmente, AWS Security Hub no recopila ni almacena ningún contenido de Security Hub con fines de mejora del servicio. Sin embargo, en el futuro, Security Hub puede recopilar y utilizar los hallazgos de seguridad de terceros que usted agregue a Security Hub y a otras formas de contenido de Security Hub (que Security Hub reciba de usted o de los servicios de terceros con el fin de proporcionar capacidades de Security Hub) para mejorar Security Hub y otras capacidades de los servicios de AWS seguridad.

Tu confianza, privacidad y la seguridad de tu Contenido son nuestra máxima prioridad. Si Security Hub comienza a recopilar contenido de Security Hub para mejorar el servicio en el futuro, esta página se actualizará para reflejar esos cambios y proporcionar detalles sobre los datos que se recopilan y cómo se utilizan. Puede excluirse de esta recopilación de contenido de Security Hub en

cualquier momento mediante la política de exclusión voluntaria de la AWS organización descrita anteriormente. Para obtener más información sobre las prácticas AWS de privacidad de datos, consulte las Preguntas frecuentes sobre privacidad de datos.

Referencias

Para obtener información sobre procedimientos de exclusión similares en otros servicios de AWS seguridad, consulte:

- En la Guía del GuardDuty usuario de Amazon, puede optar por no utilizar sus datos para mejorar el servicio.
- Optar por no utilizar sus datos para mejorar el servicio en la guía del usuario de Amazon Security Lake.

AWS Administración de identidades y accesos para Security Hub

AWS Identity and Access Management (IAM) ayuda al administrador Servicio de AWS a controlar de forma segura el acceso a AWS los recursos. Los administradores de IAM controlan quién puede estar autenticado (ha iniciado sesión) y autorizado (tiene permisos) para utilizar recursos de Security Hub. IAM es un Servicio de AWS servicio que puede utilizar sin coste adicional.

Temas

- Público
- Autenticación con identidades
- Administración del acceso con políticas
- Cómo funciona Security Hub con IAM
- Identity-based ejemplos de políticas para AWS Security Hub CSPM
- Service-linked roles para AWS Centro de seguridad
- AWSpolíticas gestionadas para Security Hub
- Resolución de problemas AWS Identidad y acceso a Security Hub

Público

La forma en que usas AWS Identity and Access Management (IAM) difiere según tu función:

- Usuario del servicio: solicite permisos al administrador si no puede acceder a las características (consulte Resolución de problemas AWS Identidad y acceso a Security Hub).
- Administrador del servicio: determine el acceso de los usuarios y envíe las solicitudes de permiso (consulte Cómo funciona Security Hub con IAM).
- Administrador de IAM: escribe las políticas para administrar el acceso (consulte Identity-based ejemplos de políticas para AWS Security Hub CSPM).

Autenticación con identidades

La autenticación es la forma en que inicias sesión AWS con tus credenciales de identidad. Debe autenticarse como usuario de Usuario raíz de la cuenta de AWS IAM o asumiendo una función de IAM.

Puedes iniciar sesión como una identidad federada con credenciales de una fuente de identidad, como AWS IAM Identity Center (el centro de identidad de IAM), la autenticación de inicio de sesión único o las credenciales. Google/Facebook Para obtener más información sobre el inicio de sesión, consulte Cómo iniciar sesión en la Cuenta de AWS en la Guía del usuario de AWS Sign-In .

Para el acceso programático, AWS proporciona un SDK y una CLI para firmar criptográficamente las solicitudes. Para obtener más información, consulte AWS Signature Version 4 para solicitudes de API en la Guía del usuario de IAM.

Cuenta de AWS usuario raíz

Cuando creas una Cuenta de AWS, comienzas con una identidad de inicio de sesión denominada usuario Cuenta de AWS raíz que tiene acceso total a todos los recursos. Servicios de AWS Se recomiendaencarecidamente que no utilice el usuario raíz para las tareas diarias. Para ver las tareas que requieren credenciales de usuario raíz, consulte Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Identidad federada

Como práctica recomendada, exija a los usuarios humanos que utilicen la federación con un proveedor de identidad para acceder Servicios de AWS mediante credenciales temporales.

Una identidad federada es un usuario de su directorio empresarial, proveedor de identidad web o Directory Service que accede Servicios de AWS mediante credenciales de una fuente de identidad. Las identidades federadas asumen roles que proporcionan credenciales temporales.

Para una administración centralizada del acceso, utilice. AWS IAM Identity Center Para obtener más información, consulte ¿Qué es el Centro de identidades de IAM? en la Guía del usuario de AWS IAM Identity Center .

Usuarios y grupos de IAM

Un usuario de IAM es una identidad con permisos específicos para una sola persona o aplicación. Como práctica recomendada, utilice credenciales temporales en lugar de usuarios de IAM con credenciales de larga duración. Para obtener más información, consulte Exigir a los usuarios humanos que utilicen la federación con un proveedor de identidad para acceder AWS mediante credenciales temporales en la Guía del usuario de IAM.

Un grupo de IAM especifica un conjunto de usuarios de IAM y facilita la administración de los permisos para grupos grandes de usuarios. Para obtener más información, consulte Casos de uso para usuarios de IAM en la Guía del usuario de IAM.

Roles de IAM

Un Rol de IAM es una identidad con permisos específicos que proporciona credenciales temporales. Puede asumir un rol cambiando de un rol de usuario a uno de IAM (consola) o llamando a una AWS CLI operación de AWS API. Para obtener más información, consulte Métodos para asumir un rol en la Guía del usuario de IAM.

Los roles de IAM son útiles para el acceso de usuario federado, los permisos de usuario de IAM temporales, el acceso entre cuentas, el acceso entre servicios y las aplicaciones que se ejecutan en Amazon EC2. Para obtener más información, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Administración del acceso con políticas

Puedes controlar el acceso AWS creando políticas y adjuntándolas a AWS identidades o recursos. Una política define los permisos cuando se asocian a una identidad o un recurso. AWS evalúa estas políticas cuando un director hace una solicitud. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre los documentos de políticas de JSON, consulte Información general de políticas de JSON en la Guía del usuario de IAM.

Mediante las políticas, los administradores especifican quién tiene acceso a qué, definiendo qué entidad principal puede realizar acciones sobre qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Un administrador de IAM crea políticas de IAM y las agrega a roles, que los usuarios pueden asumir posteriormente. Las políticas de IAM definen permisos independientemente del método que se utilice para realizar la operación.

Identity-based políticas

Identity-based las políticas son documentos de política de permisos de JSON que se adjuntan a una identidad (usuario, grupo o rol). Estas políticas controlan qué acciones pueden realizar las identidades, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en la identidad, consulte Definición de permisos de IAM personalizados con políticas administradas por el cliente en la Guía del usuario de IAM.

Identity-based las políticas pueden ser políticas en línea (integradas directamente en una sola identidad) o políticas administradas (políticas independientes asociadas a varias identidades). Para obtener información sobre cómo elegir entre políticas administradas e insertadas, consulte Selección entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Resource-based políticas

Resource-based las políticas son documentos de políticas JSON que se adjuntan a un recurso. Los ejemplos incluyen las Políticas de confianza de roles de IAM y las Políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Debe especificar una entidad principal en una política basada en recursos.

Resource-based las políticas son políticas en línea que se encuentran en ese servicio. No puede usar políticas AWS administradas de IAM en una política basada en recursos.

Otros tipos de políticas

AWS admite tipos de políticas adicionales que pueden establecer los permisos máximos que otorgan los tipos de políticas más comunes:

- Límites de permisos: establecen los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM. Para obtener más información, consulte Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.
- Políticas de control de servicios (SCP): especifican los permisos máximos para una organización o unidad organizativa en AWS Organizations. Para obtener más información, consulte Políticas de control de servicios en la Guía del usuario de AWS Organizations .

- Políticas de control de recursos (RCP): definen los permisos máximos disponibles para los recursos de las cuentas. Para obtener más información, consulte Políticas de control de recursos (RCP) en la Guía del usuario de AWS Organizations .
- Políticas de sesión: políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal para un rol o un usuario federado. Para obtener más información, consulte Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo se AWS determina si se permite una solicitud cuando se trata de varios tipos de políticas, consulte la lógica de evaluación de políticas en la guía del usuario de IAM.

Cómo funciona Security Hub con IAM

Antes de usar AWS Identity and Access Management (IAM) para administrar el acceso a AWS Security Hub, descubre qué funciones de IAM están disponibles para usar con Security Hub.

Funciones de IAM con las que puedes usar AWS Centro de seguridad

Característica de IAM	Soporte de Security Hub
Identity-based políticas	Sí
Resource-based políticas	No
Acciones de políticas	Sí
Recursos de políticas	No
Claves de condición de política	Sí
Listas de control de acceso (ACL)	No
Attribute-based control de acceso (ABAC): etiquetas en las políticas	Sí
Credenciales temporales	Sí

Característica de IAM	Soporte de Security Hub
Sesiones de acceso directo (FAS)	Sí
Roles de servicio	No
Service-linked roles	Sí

Para obtener una visión general de cómo Security Hub y otros Servicios de AWS funcionan con la mayoría de las funciones de IAM, consulte la sección sobre cómo Servicios de AWS funciona con IAM en la Guía del usuario de IAM.

Identity-based políticas de Security Hub

Compatibilidad con las políticas basadas en identidad: sí

Identity-based las políticas son documentos de política de permisos de JSON que puedes adjuntar a una identidad, como un usuario, un grupo de usuarios o un rol de IAM. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en la identidad, consulte Definición de permisos de IAM personalizados con políticas administradas por el cliente en la Guía del usuario de IAM.

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. Para obtener más información sobre los elementos que puede utilizar en una política de JSON, consulte Referencia de los elementos de la política de JSON de IAM en la Guía del usuario de IAM.

Security Hub es compatible con las políticas basadas en identidad. Para obtener más información, consulte Identity-based ejemplos de políticas para AWS Security Hub CSPM.

Resource-based políticas de Security Hub

Admite políticas basadas en recursos: no

Resource-based las políticas son documentos de políticas JSON que se adjuntan a un recurso. Los ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad

principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política basada en recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Para habilitar el acceso entre cuentas, puede especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. Para obtener más información, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Security Hub no admite políticas basadas en recursos. No puede adjuntar una política de IAM directamente a un recurso de Security Hub.

Acciones de la política para Security Hub

Compatibilidad con las acciones de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Las acciones de las políticas de Security Hub utilizan el siguiente prefijo antes de la acción:

```
securityhub:
```

Por ejemplo, para conceder a un usuario permiso para habilitar Security Hub, que es una acción que corresponde a la operación `EnableSecurityHubV2` de la API de Security Hub, debe incluir la acción `securityhub:EnableSecurityHubV2` en su política. Las instrucciones de la política deben incluir un elemento `Action` o un elemento `NotAction`. Security Hub define su propio conjunto de acciones que describen las tareas que se pueden realizar con este servicio.

```
"Action": "securityhub:EnableSecurityHubV2"
```

Para especificar varias acciones en una única instrucción, sepárelas con comas. Por ejemplo:

```
"Action": [
      "securityhub:EnableSecurityHubV2",
      "securityhub:CreateAutomationRuleV2"
```

También puede utilizar caracteres comodín para especificar varias acciones (*). Por ejemplo, para especificar todas las acciones que comiencen con la palabra `Get`, incluya la siguiente acción:

```
"Action": "securityhub:Get*"
```

Sin embargo, recomendamos que las políticas se creen según el principio de privilegios mínimos. En otras palabras, debe crear políticas que incluyan solo los permisos necesarios para realizar una tarea específica.

Para obtener una lista de las acciones de Security Hub, consulte Acciones definidas por AWS Security Hub en la referencia de autorización del servicio. Para ver ejemplos de políticas que especifican acciones de Security Hub, consulte Identity-based ejemplos de políticas para AWS Security Hub CSPM.

Recursos de políticas para Security Hub

Compatibilidad con recursos de políticas: no

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). En el caso de las acciones que no admiten permisos por recurso, utilice un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

```
"Resource": "*"
```

Security Hub define los siguientes tipos de recursos:

- Hub
- Producto
- Agregador de resultados, también denominado agregador entre regiones
- Regla de automatización

Puede especificar estos tipos de recursos en políticas utilizando los ARN.

Para obtener una lista de los tipos de recursos de Security Hub y la sintaxis ARN de cada uno, consulte Recursos definidos por AWS Security Hub en la Referencia de autorización de servicios.

Para saber qué acciones puede especificar para cada tipo de recurso, consulte Acciones definidas por AWS Security Hub en la Referencia de autorización de servicios. Para ver ejemplos de políticas que especifican recursos, consulte Identity-based ejemplos de políticas para AWS Security Hub CSPM.

Claves de condición de política de Security Hub

Compatibilidad con claves de condición de políticas específicas del servicio: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` especifica cuándo se ejecutan las instrucciones en función de criterios definidos. Puede crear expresiones condicionales que utilizan operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud. Para ver todas las claves de condiciones AWS globales, consulte las claves de contexto de condiciones AWS globales en la guía del usuario de IAM.

Para obtener una lista de las claves de estado de Security Hub, consulte las claves de estado de AWS Security Hub en la referencia de autorización de servicio. Para saber con qué acciones y recursos puede usar una clave de condición, consulte Acciones definidas por AWS Security Hub. Para ver ejemplos de políticas que utilizan claves de condición, consulte Identity-based ejemplos de políticas para AWS Security Hub CSPM.

Listas de control de acceso (ACL) en Security Hub

Compatibilidad con ACL: no

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

Security Hub no admite las ACL, lo que significa que no puede adjuntar una ACL a un recurso de Security Hub.

Attribute-based control de acceso (ABAC) con Security Hub

Admite ABAC (etiquetas en las políticas): sí

Attribute-based el control de acceso (ABAC) es una estrategia de autorización que define los permisos en función de atributos denominados etiquetas. Puede adjuntar etiquetas a las entidades y

AWS los recursos de IAM y, a continuación, diseñar políticas de ABAC para permitir las operaciones cuando la etiqueta del principal coincida con la etiqueta del recurso.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información sobre ABAC, consulte Definición de permisos con la autorización de ABAC en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulte Uso del control de acceso basado en atributos (ABAC) en la Guía del usuario de IAM.

Puede adjuntar etiquetas a los recursos de Security Hub. También puede controlar el acceso a los recursos proporcionando información sobre las etiquetas en el elemento `Condition` de una política.

Para obtener información acerca del etiquetado de recursos de Security Hub, consulte Etiquetado de recursos de Security Hub. Para obtener un ejemplo de política basada en identidad que controla el acceso a un recurso basado en etiquetas, consulte Identity-based ejemplos de políticas para AWS Security Hub CSPM.

Uso de credenciales de seguridad temporales con Security Hub

Compatibilidad con credenciales temporales: sí

Las credenciales temporales proporcionan acceso a corto plazo a AWS los recursos y se crean automáticamente al usar la federación o al cambiar de rol. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para obtener más información, consulte Credenciales de seguridad temporales en IAM y Servicios de AWS que funcionan con IAM en la Guía del usuario de IAM.

Puede utilizar credenciales temporales para iniciar sesión con federación, asumir un rol de IAM o asumir un rol de acceso entre cuentas. Las credenciales de seguridad temporales se obtienen llamando a operaciones de AWS STS API como AssumeRole o GetFederationToken.

Security Hub admite el uso de credenciales temporales.

Sesiones de acceso directo en Security Hub

Admite sesiones de acceso directo (FAS): sí

Las sesiones de acceso directo (FAS) utilizan los permisos de la persona principal que llama a una Servicio de AWS, junto con la solicitud Servicio de AWS para realizar solicitudes a los servicios posteriores. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Sesiones de acceso directo.

Por ejemplo, Security Hub convierte las solicitudes de FAS en fase descendente Servicios de AWS al integrar Security Hub con una cuenta de administrador de Security Hub delegada para una organización en Organizations AWS Organizations y al designar la cuenta de administrador delegada de Security Hub.

En lo que respecta a otras tareas, Security Hub permite al rol vinculado a un servicio llevar a cabo acciones en su nombre. Para obtener más información sobre este rol, consulte Service-linked roles para AWS Centro de seguridad.

Roles de servicios de Security Hub

Security Hub no asume ni usa funciones de servicio. Security Hub utiliza un rol vinculado al servicio para llevar a cabo acciones en su nombre. Para obtener más información sobre este rol, consulte Service-linked roles para AWS Centro de seguridad.

> **Warning**
>
> El cambio de los permisos de un rol de servicio podría provocar problemas operativos con el uso de Security Hub. Edite los roles de servicio solo cuando Security Hub proporcione orientación para hacerlo.

Service-linked funciones de Security Hub

Compatible con roles vinculados al servicio: sí

Un rol vinculado a un servicio es un tipo de rol de servicio que está vinculado a un. Servicio de AWS El servicio puede asumir la función de realizar una acción en su nombre. Service-linked las funciones aparecen en su nombre Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Security Hub permite al rol vinculado a un servicio llevar a cabo acciones en su nombre. Para obtener más información sobre este rol, consulte Service-linked roles para AWS Centro de seguridad.

Identity-based ejemplos de políticas para AWS Security Hub CSPM

De forma predeterminada, los usuarios y los roles no tienen permiso para crear o modificar los recursos de CSPM de Security Hub. Tampoco pueden realizar tareas mediante la Consola de administración de AWS API AWS CLI o AWS . Un administrador debe crear políticas de IAM que concedan permisos a los usuarios y a los roles para realizar operaciones de la API concretas en los recursos especificados que necesiten. El administrador debe adjuntar esas políticas a los usuarios o grupos que necesiten esos permisos.

Para obtener información acerca de cómo crear una política basada en identidad de IAM con estos documentos de políticas JSON de ejemplo, consulte Creación de políticas en la pestaña JSON en la Guía del usuario de IAM.

Temas

- Prácticas recomendadas relativas a políticas
- Uso de la consola CSPM de Security Hub
- Ejemplo: Permitir que los usuarios vean sus propios permisos
- Ejemplo: Permitir a los usuarios ver los resultados
- Ejemplo: Permitir a los usuarios crear y administrar reglas de automatización

Prácticas recomendadas relativas a políticas

Identity-based las políticas determinan si alguien puede crear, acceder o eliminar los recursos de Security Hub de su cuenta. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos en muchos casos de uso comunes. Están disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por los AWS clientes que sean específicas para sus casos de uso. Con el fin de obtener más información, consulte las políticas administradas por AWS o las políticas administradas por AWS para funciones de tarea en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos

como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulte Políticas y permisos en IAM en la Guía del usuario de IAM.

- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder acceso a las acciones de servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo CloudFormation. Para obtener más información, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utiliza el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte Validación de políticas con el Analizador de acceso de IAM en la Guía del usuario de IAM.
- Exigir la autenticación multifactor (MFA): si tienes una situación en la que se requieren usuarios de IAM o un usuario raíz Cuenta de AWS, activa la MFA para aumentar la seguridad. Para exigir la MFA cuando se invoquen las operaciones de la API, añada condiciones de MFA a sus políticas. Para más información, consulte Acceso seguro a la API con MFA en la Guía del usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.

Uso de la consola CSPM de Security Hub

Para acceder a la AWS Security Hub CSPM consola, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle enumerar y ver detalles sobre los recursos de CSPM de Security Hub que tiene. Cuenta de AWS Si crea una política basada en la identidad que sea más restrictiva que los permisos mínimos requeridos, la consola no funcionará según lo previsto para las entidades (usuarios o roles) que tengan esa política.

No es necesario conceder permisos mínimos de consola a los usuarios que solo llamen a la API AWS CLI o a la AWS API. En su lugar, permita el acceso únicamente a las acciones que coincidan con la operación de API que intentan realizar.

Para garantizar que esos usuarios y roles puedan usar la consola CSPM de Security Hub, adjunte también la siguiente política AWS administrada a la entidad. Para obtener más información, consulte Agregar de permisos a un usuario en la Guía del usuario de IAM:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "securityhub:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "securityhub.amazonaws.com"
                }
            }
        }
    ]
}
```

Ejemplo: Permitir que los usuarios vean sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a los usuarios de IAM ver las políticas administradas e insertadas que se asocian a la identidad de sus usuarios. Esta política incluye permisos para completar esta acción en la consola o mediante programación mediante la API or. AWS CLI AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
```

```
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Ejemplo: Permitir a los usuarios ver los resultados

En este ejemplo se muestra cómo se puede crear una política de IAM que permita a un usuario ver las conclusiones del CSPM de Security Hub.

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ReviewFindings",
            "Effect": "Allow",
            "Action": [
                "securityhub:GetFindingsV2"
            ],
            "Resource": "*"
        }
    ]
```

```
}
```

Ejemplo: Permitir a los usuarios crear y administrar reglas de automatización

En este ejemplo se muestra cómo puede crear una política de IAM que permita a un usuario crear, ver, actualizar y eliminar las reglas de automatización de CSPM de Security Hub. Para que esta política de IAM funcione, el usuario debe ser un administrador de CSPM de Security Hub. Para limitar los permisos (por ejemplo, para permitir que un usuario solo vea las reglas de automatización), puede eliminar los permisos de creación, actualización y eliminación.

```
{
            "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "CreateAndUpdateAutomationRules",
            "Effect": "Allow",
            "Action": [
                "securityhub:CreateAutomationRuleV2",
            ],
            "Resource": "*"
        },
        {
            "Sid": "ViewAutomationRules",
            "Effect": "Allow",
            "Action": [
                "securityhub:ListAutomationRulesV2",
                "securityhub:GetAutomationRuleV2"
            ],
            "Resource": "*"
        },
        {
            "Sid": "DeleteAutomationRules",
            "Effect": "Allow",
            "Action": [
                "securityhub:DeleteAutomationRuleV2"
            ],
            "Resource": "*"
        }
    ]
}
```

Service-linked roles para AWS Centro de seguridad

AWS Security Hub usa un rol vinculado a un servicio AWS Identity and Access Management (IAM) denominado. `AWSServiceRoleForSecurityHubV2` Esta función vinculada a un servicio es una función de IAM que está vinculada directamente a Security Hub. Está predefinida por Security Hub e incluye todos los permisos que Security Hub necesita para llamar a otros AWS recursos Servicios de AWS y supervisarlos en su nombre. Security Hub utiliza esta función vinculada a un servicio en todos los lugares en los Regiones de AWS que Security Hub está disponible.

Una función vinculada a un servicio facilita la configuración de Security Hub, ya que no es necesario agregar manualmente los permisos necesarios. Security Hub define los permisos de su rol vinculado al servicio y, salvo que se especifique lo contrario, solo Security Hub puede asumir el rol. Los permisos definidos incluyen la política de confianza y la política de permisos, y no puedes adjuntar esa política de permisos a ninguna otra entidad de IAM.

Para revisar los detalles del rol vinculado al servicio, puede usar la consola de Security Hub. En el panel de navegación, elija General en Configuración. Luego, en la sección Permisos del servicio, elija Ver permisos del servicio.

Puede eliminar el rol vinculado al servicio de Security Hub solo después de deshabilitar Security Hub en todas las regiones en las que esté habilitado. Esto protege sus recursos de Security Hub, ya que no puede eliminar inadvertidamente los permisos de acceso a ellos.

Para obtener información sobre otros servicios que admiten funciones vinculadas a servicios, consulte los AWS servicios que funcionan con IAM en la guía del usuario de IAM y localice los servicios que tienen la palabra Sí en la columna de funciones. Service-linked Seleccione una opción Sí con una conexión para revisar la documentación acerca del rol vinculado a un servicio en cuestión.

Temas

- Service-linked permisos de rol para Security Hub
- Creación de un rol vinculado a un servicio de Security Hub
- Edición de un rol vinculado a un servicio de Security Hub
- Eliminación de un rol vinculado a un servicio de Security Hub

Service-linked permisos de rol para Security Hub

Security Hub usa el rol vinculado a un servicio denominado `AWSServiceRoleForSecurityHubV2`. Es un rol vinculado a un servicio necesario para que AWS Security Hub acceda a sus recursos. Esta función vinculada a un servicio permite a Security Hub realizar tareas como recibir información de otros usuarios Servicios de AWS y configurar la AWS Config infraestructura necesaria para ejecutar las comprobaciones de seguridad de los controles. El rol vinculado a servicios `AWSServiceRoleForSecurityHubV2` confía en el servicio `securityhub.amazonaws.com` para asumir el rol.

El rol vinculado al servicio `AWSServiceRoleForSecurityHubV2` utiliza la política administrada de `AWSSecurityHubV2ServiceRolePolicy`.

Debe conceder permisos para permitir a una identidad de IAM (como un rol, grupo o usuario) crear, editar o eliminar un rol vinculado a un servicio. Para que el rol vinculado al servicio `AWSServiceRoleForSecurityHubV2` se cree correctamente, la identidad de IAM que usa para acceder a Security Hub debe tener los permisos necesarios. Para conceder los permisos necesarios, asocie la siguiente política a la identidad de IAM.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "securityhub:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "securityhub.amazonaws.com"
                }
            }
        }
    ]
```

```
}
```

Creación de un rol vinculado a un servicio de Security Hub

El rol vinculado al servicio de `AWSServiceRoleForSecurityHubV2` se crea automáticamente cuando habilita Security Hub por primera vez o cuando habilita Security Hub en una región donde no lo había habilitado antes. También puede crear manualmente el rol vinculado al servicio de `AWSServiceRoleForSecurityHubV2` por medio de la consola de IAM, la CLI de IAM o la API de IAM. Para obtener más información acerca de cómo crear un rol manualmente, consulte Crear un rol vinculado a un servicio en la Guía del usuario de IAM.

> **Important**
>
> La función vinculada a un servicio que se crea para una cuenta de administrador de Security Hub no se aplica a las cuentas de miembros de Security Hub asociadas.

Edición de un rol vinculado a un servicio de Security Hub

Security Hub no permite editar el rol vinculado al `AWSServiceRoleForSecurityHubV2` servicio. Después de crear un rol vinculado a un servicio, no podrá cambiar el nombre del rol, ya que varias entidades podrían hacer referencia al mismo. Sin embargo, puede editar la descripción del rol mediante IAM. Para obtener más información, consulte Edición de un rol vinculado a un servicio en la Guía del usuario de IAM.

Eliminación de un rol vinculado a un servicio de Security Hub

Si ya no necesita usar una función o un servicio que requiera un rol vinculado a un servicio, elimínelo. De esta forma, no tendrá una entidad sin usar que no se supervise o mantenga activamente.

Al deshabilitar Security Hub, Security Hub no elimina automáticamente la función `AWSServiceRoleForSecurityHubV2` vinculada al servicio. Si vuelve a habilitar Security Hub, el servicio puede entonces comenzar a usar nuevamente el rol vinculado al servicio existente. Si ya no necesita usar Security Hub, puede eliminar manualmente el rol vinculado al servicio.

> **Important**
>
> Antes de eliminar la función `AWSServiceRoleForSecurityHubV2` vinculada a un servicio, primero debe deshabilitar Security Hub en todas las regiones en las que esté habilitada. Para obtener más información, consulte Deshabilitación de Security Hub. Si Security Hub no está desactivado al intentar eliminar el rol vinculado al servicio, la eliminación no se realizará correctamente.

Para eliminar el rol vinculado al servicio de `AWSServiceRoleForSecurityHubV2`, puede usar la consola de IAM, la CLI de IAM o la API de IAM. Para obtener más información, consulte Eliminación de un rol vinculado a un servicio en la Guía del usuario de IAM.

AWSpolíticas gestionadas para Security Hub

Una política AWS administrada es una política independiente creada y administrada porAWS. AWSLas políticas administradas están diseñadas para proporcionar permisos para muchos casos de uso comunes, de modo que pueda empezar a asignar permisos a usuarios, grupos y funciones.

Ten en cuenta que es posible que las políticas AWS administradas no otorguen permisos con privilegios mínimos para tus casos de uso específicos, ya que están disponibles para que los usen todos los AWS clientes. Se recomienda definir políticas administradas por el cliente específicas para sus casos de uso a fin de reducir aún más los permisos.

No puedes cambiar los permisos definidos en AWS las políticas administradas. Si AWS actualiza los permisos definidos en una política AWS administrada, la actualización afecta a todas las identidades principales (usuarios, grupos y roles) a las que está asociada la política. AWSes más probable que actualice una política AWS administrada cuando Servicio de AWS se lance una nueva o cuando estén disponibles nuevas operaciones de API para los servicios existentes.

Para obtener más información, consulte Políticas administradas por AWS en la Guía del usuario de IAM.

AWSpolítica gestionada: AWSSecurityHubFullAccess

Puede asociar la política `AWSSecurityHubFullAccess` a las identidades de IAM.

Esta política otorga permisos administrativos que brindan a una entidad principal acceso completo a todas las acciones de Security Hub. Esta política debe adjuntarse a una entidad principal antes de que habiliten Security Hub manualmente para sus cuentas. Por ejemplo, las entidades principales

con estos permisos pueden tanto ver como actualizar el estado de los resultados. También pueden configurar resultados de información personalizados, habilitar integraciones, y habilitar o deshabilitar estándares y controles. Las entidades principales de una cuenta de administrador también pueden administrar cuentas miembro.

Detalles de los permisos

Esta política incluye los permisos siguientes:

- `securityhub`: concede a las entidades principales acceso completo a todas las acciones de Security Hub.
- `guardduty`— Permite a los directores obtener información sobre el estado de las cuentas en Amazon GuardDuty.
- `iam`— Permite a los directores crear un rol vinculado a un servicio para Security Hub.
- `inspector`: permite a las entidades principales obtener información acerca del estado de las cuentas de Amazon Inspector.
- `pricing`— Permite a los directores obtener una lista de precios y productos. Servicios de AWS

Para revisar los permisos de esta política, consulte AWSSecurityHubFullAccess en la Guía de referencia de la política administrada de AWS.

AWSpolítica gestionada: AWSSecurityHubReadOnlyAccess

Puede asociar la política `AWSSecurityHubReadOnlyAccess` a las identidades de IAM.

Esta política otorga permisos de solo lectura que permiten a los usuarios ver información en Security Hub. Las entidades principales con esta política adjunta no pueden realizar ninguna actualización en Security Hub. Por ejemplo, las entidades principales con estos permisos pueden ver la lista de resultados asociados a su cuenta, pero no pueden cambiar el estado de un resultado. Pueden ver los resultados de las informaciones, pero no pueden crear ni configurar informaciones personalizadas. No pueden configurar controles ni integraciones de productos.

Detalles de los permisos

Esta política incluye los permisos siguientes:

- `securityhub`: permite a los usuarios realizar acciones que devuelven una lista de elementos o detalles sobre un elemento. Esto incluye las operaciones de la API que comienzan con `Get`, `List` o `Describe`.

Para revisar los permisos de esta política, consulte AWSSecurityHubReadOnlyAccess en la Guía de referencia de la política administrada de AWS.

AWSpolítica gestionada: AWSSecurityHubOrganizationsAccess

Puede asociar la política `AWSSecurityHubOrganizationsAccess` a las identidades de IAM.

Esta política otorga permisos administrativos para habilitar y administrar Security Hub para una organización enAWS Organizations. Los permisos de esta política permiten a la cuenta de administración de la organización designar la cuenta de administrador delegado para Security Hub. También permiten que la cuenta de administrador delegado habilite las cuentas de la organización como cuentas de miembro.

Esta política solo proporciona permisos paraAWS Organizations. La cuenta de administración de la organización y la cuenta de administrador delegado también requieren permisos para las acciones asociadas. Estos permisos se pueden conceder mediante la política administrada de `AWSSecurityHubFullAccess`.

Detalles de los permisos

Esta política incluye los permisos siguientes:

- `organizations:ListAccounts`: permite a las entidades principales recuperar la lista de cuentas que pertenecen a una organización.
- `organizations:DescribeOrganization`: permite a las entidades principales recuperar información sobre la organización.
- `organizations:ListRoots`: permite a las entidades principales enumerar la raíz de una organización.
- `organizations:ListDelegatedAdministrators`: permite a las entidades principales enumerar el administrador delegado de una organización.
- `organizations:ListAWSServiceAccessForOrganization`— Permite a los directores enumerar lo Servicios de AWS que usa una organización.
- `organizations:ListOrganizationalUnitsForParent`: permite a las entidades principales enumerar las unidades organizativas (OU) secundarias de una unidad organizativa principal.
- `organizations:ListAccountsForParent`: permite a las entidades principales enumerar las cuentas secundarias de una unidad organizativa principal.
- `organizations:ListParents`: enumera las unidades raíz u organizativas (UO) que sirven como unidad principal inmediata de la UO secundaria o cuenta especificada.

- `organizations:DescribeAccount`: permite a las entidades principales recuperar información de sobre una cuenta en una organización.
- `organizations:DescribeOrganizationalUnit`: permite a las entidades principales recuperar información sobre una unidad organizativa de la organización.
- `organizations:ListPolicies`: recupera la lista de todas las políticas de una organización de un tipo especificado.
- `organizations:ListPoliciesForTarget`: enumera las políticas que están asociadas directamente con la raíz de destino, la unidad organizativa (UO) o la cuenta especificada.
- `organizations:ListTargetsForPolicy`: enumera todas las raíces, las unidades organizativas (UO) y las cuentas a las que está asociada la política especificada.
- `organizations:EnableAWSServiceAccess`: permite que las entidades principales habiliten la integración con Organizations.
- `organizations:RegisterDelegatedAdministrator`: permite que las entidades principales designen la cuenta de administrador delegado.
- `organizations:DeregisterDelegatedAdministrator`: permite que las entidades principales eliminen la cuenta de administrador delegado.
- `organizations:DescribePolicy`: recupera información sobre una política.
- `organizations:DescribeEffectivePolicy`: devuelve el contenido de la política en vigor para el tipo de política y la cuenta especificados.
- `organizations:CreatePolicy`— Crea una política de un tipo específico que se puede adjuntar a una cuenta raíz, a una unidad organizativa (OU) o a una AWS cuenta individual.
- `organizations:UpdatePolicy`: actualiza una política existente con un nombre nuevo, una descripción nueva o contenido nuevo.
- `organizations:DeletePolicy`: elimina la política especificada de la organización.
- `organizations:AttachPolicy`: asocia una política a una raíz, una unidad organizativa (UO) o una cuenta individual.
- `organizations:DetachPolicy`: desasocia una política de una raíz de destino, una unidad organizativa (UO) o una cuenta.
- `organizations:EnablePolicyType`: habilita un tipo de política en una raíz.
- `organizations:DisablePolicyType`: deshabilita un tipo de política organizacional en una raíz.
- `organizations:TagResource`: agrega uno o más etiquetas a un recurso especificado.

- `organizations:UntagResource`: elimina cualquier etiqueta con las claves especificadas de un recurso indicado.
- `organizations:ListTagsForResource`: enumera las etiquetas asociadas a un recurso especificado.

Para revisar los permisos de esta política, consulte AWSSecurityHubOrganizationsAccess en la Guía de referencia de la política administrada de AWS.

AWSpolítica gestionada: AWSSecurityHubV2ServiceRolePolicy

Esta política permite a Security Hub gestionar AWS Config las reglas y los recursos del Security Hub para su organización y en su nombre. Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede adjuntar esta política a las identidades de IAM. Para obtener más información, consulte the section called “Service-linked roles”.

Detalles de los permisos

Esta política incluye los permisos siguientes:

- `access-analyzer`— Cree y elimine analizadores de acceso de IAM vinculados a servicios cuando los clientes habiliten o deshabiliten Security Hub, enumere los analizadores para comprobar que el estado del analizador es coherente con el estado de activación y genere y recupere recomendaciones de políticas para los hallazgos de acceso no utilizados.
- `cloudwatch`— Recupere datos de métricas para respaldar las capacidades de medición de los recursos de Security Hub y las métricas de estado de Connector.
- `config`— Administre grabadores de configuración vinculados a servicios y grabadores de configuración vinculados a servicios de terceros para los recursos de Security Hub, incluida la compatibilidad con los grabadores Config globales. Enumere los grabadores de configuración y obtenga información sobre los conectores para admitir integraciones en la nube de terceros.
- `ecr`— Recupere información sobre las imágenes y los repositorios de Amazon Elastic Container Registry para respaldar las capacidades de medición.
- `iam`— Cree las siguientes funciones vinculadas a servicios: AWS Config IAM Access Analyzer en la cuenta del cliente y Amazon Inspector para el escaneo de terceros. Recupere la información de la cuenta para respaldar las capacidades de medición. Recupere las políticas de IAM existentes para que los clientes puedan ver una comparación entre su política actual y la que se recomienda reemplazar con menos privilegios.

- `inspector2`— Cree, actualice, elimine y enumere los conectores de Amazon Inspector y las configuraciones de escaneo de conectores para admitir integraciones en la nube de terceros.
- `lambda`— Recupere AWS Lambda la información de las funciones para respaldar las capacidades de medición.
- `organizations`: recuperar información de cuentas y unidades organizativas (OU) de una organización.
- `securityhub`: administrar la configuración de Security Hub. Cree, actualice y elimine conectores de Security Hub para admitir integraciones en la nube de terceros.
- `sts`— Obtenga tokens de identidad web para la federación de identidades salientes a fin de respaldar las integraciones en la nube de terceros.
- `tag`: recuperar información sobre las etiquetas de recursos.

Para revisar los permisos de esta política, consulte AWSSecurityHubV2ServiceRolePolicy en la Guía de referencia de la política administrada de AWS.

Security Hub se actualiza aAWSpolíticas administradas

La siguiente tabla proporciona detalles sobre las actualizaciones de las políticas AWS administradas para AWS Security Hub desde que este servicio comenzó a rastrear estos cambios. Para recibir alertas automáticas sobre actualizaciones en las políticas, suscríbase al canal RSS en la página del Historial de documentos de Security Hub.

Cambio	Descripción	Fecha
AWSSecurityHubV2ServiceRolePolicy: política actualizada	Security Hub actualizó la política para admitir integraciones de terceros. La actualización añade los siguientes permisos: gestionar grabadores de configuración de terceros, crear y gestionar los conectores de Security Hub y Amazon Inspector, recuperar las métricas de estado de	30 de junio de 2026

Cambio	Descripción	Fecha
	Connector CloudWatch, crear el rol vinculado al servicio Amazon Inspector para el escaneo de terceros y obtener tokens de identidad web para la federación.	
AWSSecurityHubV2ServiceRolePolicy: política actualizada	Security Hub actualizó la política para añadir permisos de IAM Access Analyzer. La actualización permite a Security Hub crear y gestionar analizadores gestionados por el servicio, enumerar los analizadores para comprobar que la configuración del analizador es coherente con el estado de habilitación, generar y recuperar recomendaciones de políticas para los hallazgos de acceso no utilizados y recuperar las políticas de IAM para mostrar las recomenda ciones.	10 de mayo de 2026
AWSSecurityHubOrganizationsAccess: política actualizada	Security Hub actualizó la política para añadir permisos que describan las políticas de recursos que admitan las funciones de Security Hub. Security Hub se encuentra en versión preliminar y está sujeto a cambios.	12 de noviembre de 2025

Cambio	Descripción	Fecha
AWSSecurityHubFullAccess: política actualizada	Security Hub actualizó la política para añadir funciones relacionadas con la administr ación GuardDuty, Amazon Inspector y la administración de cuentas para admitir las funciones de Security Hub. Security Hub se encuentra en versión preliminar y está sujeto a cambios.	17 de noviembre de 2025
AWSSecurityHubV2Se rviceRolePolicy: política actualizada	Security Hub actualizó la política para añadir capacidad es de medición para Amazon Elastic Container Registry (Amazon CloudWatch) y AWS Identity and Access Management para admitir las funciones de Security Hub. AWS Lambda La actualiza ción también agregó soporte para AWS Config grabadore s globales. Security Hub se encuentra en versión prelimina r y está sujeto a cambios.	5 de noviembre de 2025
AWSSecurityHubOrga nizationsAccess: actualización de una política actual	Security Hub agregó nuevos permisos a la política. Estos permisos permiten que la administración de la organizac ión habilite y administre Security Hub y el CSPM de Security Hub para una organización.	17 de junio de 2025

Cambio	Descripción	Fecha
AWSSecurityHubFullAccess: actualización de una política actual	El CSPM de Security Hub agregó nuevos permisos que permiten a las entidades principales crear un rol vinculado al servicio para Security Hub.	17 de junio de 2025
AWSSecurityHubV2ServiceRolePolicy: política nueva	Security Hub agregó una nueva política que permite a Security Hub administrar AWS Config las reglas y los recursos del Security Hub para la organización de un cliente y en su nombre. Security Hub se encuentra en versión preliminar y está sujeto a cambios.	17 de junio de 2025
AWSSecurityHubFullAccess— Actualización de una política existente	Security Hub CSPM actualizó la política para obtener información detallada sobre los precios Servicios de AWS y los productos.	24 de abril de 2024
AWSSecurityHubReadOnlyAccess— Actualización de una política existente	El CSPM de Security Hub actualizó esta política administrada mediante la adición de un campo `Sid`.	22 de febrero de 2024

Cambio	Descripción	Fecha
AWSSecurityHubFullAccess— Actualización a una política existente	Security Hub CSPM actualizó la política para poder determinar si Amazon GuardDuty y Amazon Inspector están habilitados en una cuenta. Esto ayuda a los clientes a reunir información relacionada con la seguridad de múltiples fuentes. Servicios de AWS	16 de noviembre de 2023
AWSSecurityHubOrganizationsAccess— Actualización a una política existente	El CSPM de Security Hub ha actualizado la política para conceder permisos adicionales a fin de permitir acceso de solo lectura a las funcionalidades de administrador delegado de AWS Organizations. Esto incluye detalles como la raíz, las unidades organizativas (OU), las cuentas, la estructura de la organización y el acceso a servicios.	16 de noviembre de 2023
AWSSecurityHubOrganizationsAccess— Nueva política	El CSPM de Security Hub agregó una nueva política que otorga los permisos necesarios para la integración del CSPM de Security Hub con Organizations.	15 de marzo de 2021

Cambio	Descripción	Fecha
El CSPM de Security Hub comenzó a hacer un seguimiento de los cambios	Security Hub CSPM comenzó a realizar un seguimiento de los cambios en sus políticas AWS gestionadas.	15 de marzo de 2021

Resolución de problemas AWS Identidad y acceso a Security Hub

Usa la siguiente información para ayudarte a diagnosticar y solucionar los problemas comunes que puedes encontrar al trabajar con AWS Security Hub e IAM.

Temas

- No tengo autorización para realizar una acción en Security Hub
- No estoy autorizado a ejecutar iam: PassRole
- Quiero tener acceso programático a Security Hub
- Soy administrador y deseo permitir que otros obtengan acceso a Security Hub
- Quiero permitir la entrada de personas ajenas a mi Cuenta de AWS para acceder a mis recursos de Security Hub

No tengo autorización para realizar una acción en Security Hub

Si Consola de administración de AWS le indica que no está autorizado a realizar una acción, debe ponerse en contacto con su administrador para obtener ayuda. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

El siguiente ejemplo de error se produce cuando el usuario `mateojackson` intenta usar la consola para ver los detalles de una *`widget`* pero no tiene `securityhub:`*`GetWidget`* permisos.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 securityhub:GetWidget on resource: my-example-widget
```

En este caso, Mateo pide a su administrador que actualice sus políticas de forma que pueda obtener acceso al recurso *`my-example-widget`* mediante la acción `securityhub:`*`GetWidget`*.

No estoy autorizado a ejecutar iam: PassRole

Si recibe un error que indica que no tiene autorización para realizar la acción `iam:PassRole`, se deben actualizar las políticas a fin de permitirle pasar un rol a Security Hub.

Algunas Servicios de AWS permiten transferir una función existente a ese servicio en lugar de crear una nueva función de servicio o una función vinculada a un servicio. Para ello, debe tener permisos para transferir el rol al servicio.

En el siguiente ejemplo, el error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en Security Hub. Sin embargo, la acción requiere que el servicio cuente con permisos que otorguen un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con su AWS administrador. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero tener acceso programático a Security Hub

Los usuarios necesitan acceso mediante programación si quieren interactuar con personas AWS ajenas a. Consola de administración de AWS La forma de conceder el acceso programático depende del tipo de usuario al que acceda. AWS

Para conceder acceso programático a los usuarios, elija una de las siguientes opciones.

¿Qué usuario necesita acceso programático?	Para	Mediante
IAM	(Recomendado) Usa las credenciales de la consola como credenciales temporales para firmar las solicitudes programáticas a los AWS CLI AWS SDK o las API. AWS	Siga las instrucciones de la interfaz que desea utilizar: • Para ello AWS CLI, consulte Inicio de sesión para el desarrollo AWS local en la

¿Qué usuario necesita acceso programático?	Para	Mediante
		Guía del AWS Command Line Interface usuario. • Para AWS los SDK, consulte Iniciar sesión para el desarrollo AWS local en la Guía de referencia AWS sobre los SDK y las herramientas.
Identidad del personal (Usuarios administrados en el IAM Identity Center)	Usa credenciales temporales para firmar las solicitudes programáticas a los AWS SDK o AWS CLI las API. AWS	Siga las instrucciones de la interfaz que desea utilizar: • Para ello AWS CLI, consulte Configuración AWS CLI para su uso AWS IAM Identity Center en la Guía del AWS Command Line Interface usuario. • Para ver AWS los SDK, las herramientas y las AWS API, consulte la autenticación del IAM Identity Center en la guía de referencia de AWS SDK y herramientas.
IAM	Utilice credenciales temporales para firmar las solicitudes programáticas a los AWS SDK o las AWS CLI API. AWS	Siga las instrucciones que aparecen en la Guía del usuario de IAM, que se indican en la sección Uso de credenciales temporales con los AWS recursos.

¿Qué usuario necesita acceso programático?	Para	Mediante
IAM	(No recomendado) Utilice credenciales a largo plazo para firmar las solicitud es programáticas a los AWS CLI AWS SDK o las API. AWS	Siga las instrucciones de la interfaz que desea utilizar: • Para ello AWS CLI, consulte Autenticación mediante credenciales de usuario de IAM en la Guía del usuario. AWS Command Line Interface • Para ver AWS los SDK y las herramientas, consulte Autenticar con credencia les de larga duración en la Guía de referencia sobre los AWS SDK y las herramien tas. • Para obtener informaci ón AWS sobre las API, consulte Administrar las claves de acceso para los usuarios de IAM en la Guía del usuario de IAM.

Soy administrador y deseo permitir que otros obtengan acceso a Security Hub

Para dar acceso, agregue permisos a los usuarios, grupos o roles:

- Usuarios y grupos en: AWS IAM Identity Center

  Cree un conjunto de permisos. Siga las instrucciones de Creación de un conjunto de permisos en la Guía del usuario de AWS IAM Identity Center .

- Usuarios gestionados en IAM a través de un proveedor de identidades:

Cree un rol para la federación de identidades. Siga las instrucciones descritas en Creación de un rol para un proveedor de identidad de terceros (federación) en la Guía del usuario de IAM.

- Usuarios de IAM:
  - Cree un rol que el usuario pueda aceptar. Siga las instrucciones descritas en Creación de un rol para un usuario de IAM en la Guía del usuario de IAM.
  - (No recomendado) Adjunte una política directamente a un usuario o agregue un usuario a un grupo de usuarios. Siga las instrucciones descritas en Adición de permisos a un usuario (consola) de la Guía del usuario de IAM.

Quiero permitir la entrada de personas ajenas a mi Cuenta de AWS para acceder a mis recursos de Security Hub

Se puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Se puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que admitan las políticas basadas en recursos o las listas de control de acceso (ACL), puede utilizar dichas políticas para conceder a las personas acceso a sus recursos.

Para obtener más información, consulte lo siguiente:

- Para obtener información sobre la compatibilidad de Security Hub con estas características, consulte Cómo funciona Security Hub con IAM.
- Para obtener información sobre cómo proporcionar acceso a los recursos de tu Cuentas de AWS propiedad, consulta Cómo proporcionar acceso a un usuario de IAM en otro Cuenta de AWS de tu propiedad en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta Cómo proporcionar acceso a los que Cuentas de AWS pertenecen a terceros en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulte Proporcionar acceso a usuarios autenticados externamente (identidad federada) en la Guía del usuario de IAM.
- Para conocer sobre la diferencia entre las políticas basadas en roles y en recursos para el acceso entre cuentas, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Validación de conformidad para AWS Centro de seguridad

Nuestra nueva experiencia AWS de registro no está diseñada para cargas de trabajo reguladas. Si utilizas nuestra nueva experiencia de AWS registro, pero quieres utilizarla AWS para cargas de trabajo reguladas, puedes suscribirte a una versión AWS (avanzada) o activar funciones avanzadas para tu entorno. AWS

Para saber si una Servicio de AWS está dentro del ámbito de un programa de cumplimiento específico, consulte Servicios de AWS la sección Alcance por programa de cumplimiento y seleccione el programa de cumplimiento que le interese. Para obtener información general, consulte Programas AWS de cumplimiento Programas .

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descargar informes en AWS Artifact .

Su responsabilidad de cumplimiento al usarlos Servicios de AWS viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y normativas aplicables. Para obtener más información sobre su responsabilidad de cumplimiento al usarlos Servicios de AWS, consulte la documentación AWS de seguridad.

Resiliencia en AWS Centro de seguridad

La infraestructura AWS global se basa en zonas Regiones de AWS de disponibilidad. Las regiones proporcionan varias zonas de disponibilidad físicamente independientes y aisladas que se encuentran conectadas mediante redes con un alto nivel de rendimiento y redundancia, además de baja demora. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre las zonas sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de uno o varios centros de datos.

Para obtener más información sobre Regiones de AWS las zonas de disponibilidad, consulte Infraestructura AWS global.

Seguridad de infraestructura en AWS Centro de seguridad

Como servicio gestionado, AWS Security Hub está protegido por la seguridad de red AWS global. Para obtener información sobre los servicios de AWS seguridad y cómo AWS protege la infraestructura, consulta AWS Cloud Security. Para diseñar su AWS entorno utilizando las mejores

prácticas de seguridad de la infraestructura, consulte Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Las llamadas a la API AWS publicadas se utilizan para acceder a Security Hub a través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Conjuntos de cifrado con un secreto directo perfecto (PFS), como el DHE (efímero) o el ECDHE (efímero de curva elíptica Diffie-Hellman). Diffie-Hellman La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

AWS Puntos finales de VPC de interfaz y centro de seguridad (AWS PrivateLink)

Puede establecer una conexión privada entre su VPC y AWS Security Hub creando un punto final de VPC de interfaz. Los puntos de conexión de interfaz cuentan con tecnología de AWS PrivateLink que le permite acceder de forma privada a las API de Security Hub sin una puerta de enlace de Internet, un dispositivo NAT, una conexión de VPN o una conexión de AWS Direct Connect. Las instancias de su VPC no necesitan direcciones IP públicas para comunicarse con las API de Security Hub. El tráfico entre la VPC y Security Hub no sale de la red de Amazon.

Cada punto de conexión de la interfaz está representado por una o más interfaces de red elásticas en las subredes. Para obtener más información, consulte Acceder a un punto final de VPC y Servicio de AWS utilizar una interfaz en la Guía de Amazon Virtual Private Cloud.

Consideraciones para los puntos de conexión de VPC de Security Hub

Antes de configurar un punto de conexión de VPC de interfaz para Security Hub, asegúrese de revisar los requisitos previos y otra información en la Guía de Amazon Virtual Private Cloud.

Security Hub admite la realización de llamadas a todas las acciones de la API desde su VPC.

Creación de un punto de conexión de VPC de la interfaz para Security Hub

Puede crear un punto de enlace de VPC para el servicio Security Hub mediante la consola de Amazon VPC o el AWS Command Line Interface ().AWS CLI Para obtener más información, consulte Cómo crear un punto de conexión de VPC en la Guía de Amazon Virtual Private Cloud.

Cree un punto de conexión de VPC para Security Hub mediante el siguiente nombre de servicio:

`com.amazonaws.region.securityhub`

¿Dónde *region* está el código de región aplicable? Región de AWS

Si habilita DNS privado para el punto de conexión, podrá realizar solicitudes de la API a Security Hub mediante su nombre DNS predeterminado para la región; por ejemplo, `securityhub.us-east-1.amazonaws.com` para la región Este de EE. UU (Norte de Virginia).

Creación de una política de punto de conexión de VPC para Security Hub

Puede adjuntar una política de punto de conexión al punto de conexión de VPC que controla el acceso a Security Hub. La política especifica la siguiente información:

- La entidad principal que puede realizar acciones.
- Las acciones que se pueden realizar.
- Los recursos en los que se pueden llevar a cabo las acciones.

Para obtener más información, consulte Control del acceso a puntos de conexión de VPC mediante políticas de punto de conexión en la Guía de Amazon Virtual Private Cloud.

Ejemplo: política de punto de conexión de VPC para acciones de Security Hub

El siguiente es un ejemplo de un resultado típico de una política de punto de conexión para Security Hub. Cuando se asocia con un punto de conexión, esta política concede acceso a las acciones de Security Hub mostradas para todas las entidades principales en todos los recursos.

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "securityhub:getFindings",
            "securityhub:getEnabledStandards",
            "securityhub:getInsights"
         ],
         "Resource":"*"
      }
   ]
}
```

Subredes compartidas

No puede crear, describir, modificar ni eliminar puntos de conexión de VPC en subredes que se compartan con usted. No obstante, puede usar los puntos de conexión de VPC en las subredes que se compartan con usted. Para obtener información sobre el uso compartido de VPC, consulte Uso compartido de las subredes de la VPC con otras cuentas en la Guía de Amazon Virtual Private Cloud.

Registro de llamadas a la API de Security Hub con CloudTrail

está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en Security Hub. CloudTrail captura las llamadas a la API de Security Hub como eventos. Las llamadas capturadas incluyen llamadas desde la consola de Security Hub y las llamadas desde el código a las operaciones de la API de Security Hub. Si crea un registro, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos para Security Hub. Si no configuras un registro, puedes seguir viendo los eventos más recientes en la CloudTrail consola, en el Historial de eventos. Con la información que se CloudTrail recopila, puede determinar la solicitud que se hizo a Security Hub, la dirección IP desde la que se realizó la solicitud, quién la hizo, cuándo se hizo y detalles adicionales.

Para obtener más información sobre CloudTrail cómo configurarla y habilitarla, consulte la Guía del AWS CloudTrail usuario.

Información sobre Security Hub en CloudTrail

CloudTrail está activado Cuenta de AWS cuando creas la cuenta. Cuando se produce una actividad de eventos admitida en Security Hub, esa actividad se registra en un CloudTrail evento junto con otros eventos de AWS servicio en el historial de eventos. Se puede ver, buscar y descargar los últimos eventos de la cuenta de . Para obtener más información, consulte Visualización de eventos con el historial de CloudTrail eventos.

Para mantener un registro continuo de los eventos de su cuenta, incluidos los eventos de Security Hub, cree un registro de seguimiento. Un registro permite CloudTrail enviar los archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando se crea un registro de seguimiento en la consola, este se aplica a todas las regiones de AWS . El registro registra los eventos de todas las regiones de la AWS partición y envía los archivos de registro al bucket de Amazon S3 que usted especifique. Además, puede configurar otros AWS servicios para analizar más a fondo los datos de

eventos recopilados en los CloudTrail registros y actuar en función de ellos. Para más información, consulte los siguientes temas:

- Introducción a la creación de registros de seguimiento
- CloudTrail servicios e integraciones compatibles
- Configurar las notificaciones de Amazon SNS para CloudTrail
- Recibir archivos de CloudTrail registro de varias regiones y Recibir archivos de CloudTrail registro de varias cuentas

Security Hub permite registrar todas las acciones de la API de Security Hub como eventos en CloudTrail los registros. Para ver una lista de operaciones de Security Hub, consulte la Referencia de la API de Security Hub.

Cuando se registra la actividad de las siguientes acciones CloudTrail, el valor de `responseElements` se establece en`null`. Esto garantiza que la información confidencial no se incluya en CloudTrail los registros.

- `GetFindingsV2`

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con credenciales de usuario raíz o de usuario AWS Identity and Access Management (IAM)
- si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado
- Si la solicitud la hizo otro servicio AWS

Para obtener más información, consulte el elemento userIdentity de CloudTrail .

Ejemplo: entradas del archivo de registros de Security Hub

Un registro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que usted especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una única solicitud de cualquier fuente e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud,

etc. CloudTrail los archivos de registro no son un registro ordenado de las llamadas a la API pública, por lo que no aparecen en ningún orden específico.

El siguiente ejemplo muestra una entrada de CloudTrail registro que demuestra la `CreateAutomationRuleV2` acción. En este ejemplo, `TestAutomationRule` se crea una regla de automatización denominada. Los `Account ID` atributos `Severity` y se especifican como criterios. Cuando la regla coincide, `Severity` se actualiza a Alta. Para obtener más información sobre las reglas de automatización, consulte[Reglas de automatización en Security Hub](#).

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROA123456789EXAMPLE:Admin",
        "arn": "arn:aws:sts::555555555555:assumed-role/Admin",
        "accountId": "555555555555",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROA123456789EXAMPLE",
                "arn": "aarn:aws:iam::555555555555:role/Admin",
                "accountId": "555555555555",
                "userName": "Admin"
            },
            "attributes": {
                "creationDate": "2025-11-15T18:49:13Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2025-11-15T18:51:17Z",
    "eventSource": "securityhub.amazonaws.com",
    "eventName": "CreateAutomationRuleV2",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.50",
    "userAgent": "aws-cli/1.11.76 Python/2.7.10 Darwin/17.7.0 botocore/1.5.39",
    "requestParameters": {
        "Description": "Test Automation Rule",
        "Actions": [
            {
                "Type": "FINDING_FIELDS_UPDATE",
                "FindingFieldsUpdate": {
```

```
                    "SeverityId": 4
                }
            }
        ],
        "RuleStatus": "ENABLED",
        "Criteria": {
            "OcsfFindingCriteria": {
                "CompositeFilters": [
                    {
                        "Operator": "OR",
                        "StringFilters": [
                            {
                                "FieldName": "severity",
                                "Filter": {
                                    "Value": "Medium",
                                    "Comparison": "EQUALS"
                                }
                            }
                        ]
                    },
                    {
                        "Operator": "OR",
                        "StringFilters": [
                            {
                                "FieldName": "cloud.account.uid",
                                "Filter": {
                                    "Value": "111122223333",
                                    "Comparison": "EQUALS"
                                }
                            }
                        ]
                    }
                ],
                "CompositeOperator": "AND"
            }
        },
        "ClientToken": "a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa",
        "RuleOrder": 61,
        "RuleName": "TestAutomationRule",
        "Tags": {}
    },
    "responseElements": {
        "RuleArn": "arn:aws:securityhub:us-west-2:555555555555:automation-rulev2/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
```

```
        "RuleId": "c8bc6f90-29e9-4eb7-919f-b145e44eb8ec"
    },
    "requestID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "eventID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "555555555555",
    "eventCategory": "Management"
}
```

Introducción a AWS CSPM de Security Hub

AWS La gestión de la postura de seguridad en la nube de AWS Security Hub (Security Hub CSPM) le proporciona una visión completa del estado de su seguridad y le ayuda a evaluar su AWS entorno en AWS relación con los estándares y las mejores prácticas del sector de la seguridad.

AWS Security Hub CSPM recopila datos de seguridad de productos de terceros compatibles y compatibles Cuentas de AWS Servicios de AWS, y le ayuda a analizar sus tendencias de seguridad e identificar los problemas de seguridad más prioritarios.

Para ayudar a administrar el estado de seguridad de la organización, el CSPM de Security Hub admite varios estándares de seguridad. Entre ellos se incluyen el estándar AWS Fundational Security Best Practices (FSBP), desarrollado por AWS, y marcos de cumplimiento externos, como el Center for Internet Security (CIS), el Payment Card Industry Data Security Standard (PCI DSS) y el National Institute of Standards and Technology (NIST). Cada estándar incluye varios controles de seguridad, cada uno de los cuales representa una práctica de seguridad recomendada. El CSPM de Security Hub ejecuta comprobaciones basadas en controles de seguridad y genera resultados de control que ayudan a evaluar el cumplimiento con las prácticas recomendadas de seguridad.

Además de generar conclusiones de control, Security Hub CSPM también recibe las conclusiones de otros productos Servicios de AWS—como Amazon, Amazon Inspector y Amazon GuardDuty Macie— y de otros productos compatibles de terceros. De este modo, podrá ver varios problemas relacionados con la seguridad en un único panel. También puede enviar los resultados del CSPM de Security Hub a otros Servicios de AWS y productos de terceros compatibles.

El CSPM de Security Hub ofrece características de automatización que ayudan a clasificar y remediar problemas de seguridad. Por ejemplo, puede usar reglas de automatización para actualizar automáticamente resultados críticos cuando un control de seguridad falla. También puedes aprovechar la integración con Amazon EventBridge para activar respuestas automáticas a hallazgos específicos.

Temas

- Beneficios del CSPM de Security Hub
- Acceso al CSPM de Security Hub
- Servicios relacionados
- Prueba gratuita y precios del CSPM de Security Hub
- Terminología y conceptos del CSPM de Security Hub

- Habilitación del CSPM de Security Hub
- Administración de cuentas de administrador y de miembro en el CSPM de Security Hub
- Descripción de la agregación entre regiones en el CSPM de Security Hub
- Descripción de los estándares de seguridad en el CSPM de Security Hub
- Comprensión de los controles de seguridad en el CSPM de Security Hub
- Comprensión de las integraciones en el CSPM de Security Hub
- Integración de Security Hub CSPM con Microsoft Azure
- Creación y actualización de resultados en el CSPM de Security Hub
- Visualización de productos de información en el CSPM de Security Hub
- Modificación automática de los resultados del CSPM de Security Hub y adopción de medidas al respecto
- Uso del panel en el CSPM de Security Hub
- Límites regionales del CSPM de Security Hub
- Creación de recursos CSPM de Security Hub con CloudFormation
- Suscripción a los anuncios del CSPM de Security Hub con Amazon SNS
- Cómo desactivar el CSPM de Security Hub
- Seguridad en AWS Security Hub CSPM
- Registrar llamadas a la API de Security Hub con CloudTrail

Beneficios del CSPM de Security Hub

Estas son algunas de las formas clave en las que Security Hub CSPM le ayuda a supervisar el cumplimiento y la seguridad en todo su entorno. AWS

Reducción del esfuerzo para recopilar y priorizar los resultados

El CSPM de Security Hub reduce el esfuerzo de recopilar y priorizar los hallazgos de seguridad en las cuentas de los productos integrados Servicios de AWS y de socios. AWS El CSPM de Security Hub procesa la búsqueda de datos mediante el formato de búsqueda AWS de seguridad (ASFF), un formato de búsqueda estándar. Esto elimina la necesidad de administrar los resultados de numerosas fuentes en varios formatos. El CSPM de Security Hub también correlaciona resultados de distintos proveedores para ayudar a identificar y priorizar los más relevantes.

Controles de seguridad automáticos respecto a las prácticas recomendadas y a los estándares

Security Hub CSPM ejecuta automáticamente comprobaciones continuas de configuración y seguridad a nivel de cuenta según las mejores prácticas y los estándares del sector. AWS El CSPM de Security Hub usa los resultados de estas comprobaciones para calcular las puntuaciones de seguridad e identificar las cuentas y los recursos que requieren atención.

Vista consolidada de los resultados en cuentas y proveedores

El CSPM de Security Hub consolida los resultados de seguridad de las cuentas y de los productos de proveedores compatibles, y muestra los resultados en la consola del CSPM de Security Hub. También puede recuperar los hallazgos a través de la API o los SDK de CSPM de Security Hub. AWS CLI Con una visión integral del estado actual de su seguridad, puede detectar tendencias, identificar posibles problemas y tomar las medidas de corrección necesarias.

Capacidad para automatizar la actualización y corrección de resultados

Puede crear reglas de automatización que modifiquen o supriman resultados en función de los criterios que haya definido. El CSPM de Security Hub también admite la integración con Amazon. EventBridge Para automatizar la corrección de resultados específicos, puede definir acciones personalizadas que se deben llevar a cabo cuando se genera un resultado. Por ejemplo, puede configurar acciones personalizadas para enviar resultados a un sistema de tickets o a un sistema de corrección automático.

Acceso al CSPM de Security Hub

Security Hub CSPM está disponible en la mayoría. Regiones de AWS Para obtener una lista de las regiones donde el CSPM de Security Hub está disponible actualmente, consulte Puntos de conexión y cuotas del CSPM de AWS Security Hub en la Referencia general de AWS. Para obtener información sobre la administración Regiones de AWS de su cuenta Cuenta de AWS, consulte Especificar qué Regiones de AWS cuenta puede usar en la guía de AWS Account Management referencia.

En cada región, puede acceder y utilizar el CSPM de Security Hub de cualquiera de las siguientes formas:

Consola del CSPM de Security Hub

Consola de administración de AWS Es una interfaz basada en un navegador que puede usar para crear y administrar AWS recursos. Como parte de esa consola, la consola del CSPM de

Security Hub proporciona acceso a la cuenta, datos y recursos del CSPM de Security Hub. Puede realizar tareas del CSPM de Security Hub mediante la consola del CSPM de Security Hub: ver resultados, crear reglas de automatización, crear una región de agregación y otras acciones.

API del CSPM de Security Hub

La API del CSPM de Security Hub proporciona acceso mediante programación a la cuenta, los datos y los recursos del CSPM de Security Hub. Con la API, puede enviar solicitudes HTTPS directamente al CSPM de Security Hub. Para obtener información sobre la API, consulte Referencia de la API de AWS Security Hub.

AWS CLI

Con él AWS CLI, puede ejecutar comandos en la línea de comandos de su sistema para realizar tareas de CSPM de Security Hub. En algunos casos, el uso de la línea de comandos puede ser más rápido y cómodo que usar la consola. La línea de comandos también es útil si desea crear scripts que realicen tareas. Para obtener información sobre la instalación y el uso del AWS CLI, consulte la Guía del AWS Command Line Interface usuario.

AWS SDKs

AWS proporciona SDK que constan de bibliotecas y código de muestra para varios lenguajes de programación y plataformas, por ejemplo, Java, Go, Python, C++ y.NET. Los SDK proporcionan un acceso práctico y programático a Security Hub, CSPM y a otros en el idioma que prefiera. Servicios de AWS También permiten realizar tareas como firmar solicitudes criptográficamente, administrar errores y reintentar solicitudes automáticamente. Para obtener información sobre la instalación y el uso de los AWS SDK, consulte Tools to Build On. AWS

> **Important**
>
> El CSPM de Security Hub solo detecta y consolida resultados generados después de habilitar el CSPM de Security Hub. No detecta ni consolida de manera retroactiva los resultados generados antes de habilitar el CSPM de Security Hub.
> El CSPM de Security Hub solo recibe y procesa resultados en la región donde lo haya habilitado en la cuenta.
> Para cumplir plenamente con las comprobaciones de seguridad de CIS AWS Foundations Benchmark, debe habilitar el CSPM de Security Hub en todas las regiones compatibles. AWS

Servicios relacionados

Para proteger aún más su AWS entorno, considere la posibilidad de usar otros Servicios de AWS en combinación con Security Hub CSPM. Algunos Servicios de AWS envían sus hallazgos al CSPM de Security Hub, y el CSPM de Security Hub normaliza los hallazgos en un formato estándar. Algunas también Servicios de AWS pueden recibir las conclusiones del CSPM de Security Hub.

Para obtener una lista de otras personas Servicios de AWS que envían o reciben las conclusiones del CSPM de Security Hub, consulte. Servicio de AWS integraciones con Security Hub CSPM

El CSPM de Security Hub usa reglas vinculadas a servicios desde para ejecutar las comprobaciones de seguridad de la mayoría de AWS Config los controles. Los controles se refieren a recursos específicos y específicos. Servicios de AWS AWS Para obtener una lista de los controles del CSPM de Security Hub, consulte Referencia de controles para el CSPM de Security Hub. Debe habilitar AWS Config y registrar los recursos en Security Hub CSPM AWS Config para generar la mayoría de los resultados de control. Para obtener más información, consulte Consideraciones antes de habilitar y configurar AWS Config.

Prueba gratuita y precios del CSPM de Security Hub

Cuando habilita Security Hub CSPM Cuenta de AWS por primera vez, esa cuenta se inscribe automáticamente en una prueba gratuita de 30 días de Security Hub CSPM.

Cuando usa Security Hub CSPM durante la prueba gratuita, se le cobra por el uso de otros servicios con los que interactúa Security Hub CSPM, como los artículos. AWS Config No se le cobrará nada por AWS Config las reglas que se activen únicamente según los estándares de seguridad de Security Hub CSPM.

No se cobra por usar el CSPM de Security Hub hasta que finaliza el periodo de prueba gratuito.

Visualización de los detalles de uso

Security Hub CSPM proporciona información de uso, incluida la cantidad de comprobaciones y comprobaciones de seguridad procesadas por su cuenta. Los detalles de uso también incluyen el tiempo restante de la prueba gratuita. Esta información puede ayudarlo a comprender el uso de Security Hub CSPM una vez que finalice la prueba gratuita. La información de uso también está disponible una vez finalizada la prueba gratuita.

Cómo mostrar la información de uso (consola)

1. Abra la consola AWS CSPM de Security Hub en. https://console.aws.amazon.com/securityhub/
2. En el panel de navegación, elija Uso en Configuración.

La información de uso es solo para la cuenta actual y la región actuales. En una región de agregación, la información de uso no incluye las regiones vinculadas. Para obtener más información acerca de las regiones vinculadas, consulte the section called “Tipos de datos que se agregan”.

Para ver los detalles de los costos de tu cuenta, usa la consola AWS de facturación.

Información sobre precios

Para obtener más información sobre cómo el CSPM de Security Hub cobra por los resultados ingeridos y por las comprobaciones de seguridad, consulte Precios del CSPM de Security Hub.

Terminología y conceptos del CSPM de Security Hub

En AWS Security Hub CSPM, nos basamos en AWS conceptos y terminología comunes y utilizamos estos términos adicionales.

Cuenta

Una cuenta estándar de Amazon Web Services (AWS) que contiene sus AWS recursos. Puede iniciar sesión AWS con su cuenta y activar Security Hub CSPM.

Una cuenta puede invitar a otras cuentas a habilitar el CSPM de Security Hub y a asociarse a ella dentro del CSPM de Security Hub. La aceptación de una invitación de suscripción es opcional. Si las invitaciones se aceptan, la cuenta se convierte en la cuenta de administrador, mientras que las cuentas añadidas se convierten en cuentas miembro. Las cuentas de administrador pueden ver los resultados de sus cuentas miembro.

Si está inscrito AWS Organizations, su organización designa una cuenta de administrador de CSPM de Security Hub para la organización. La cuenta de administrador del CSPM de Security Hub puede habilitar otras cuentas de la organización como cuentas de miembro.

Una cuenta no puede ser cuenta de administrador y cuenta miembro al mismo tiempo. Una cuenta solo puede tener una cuenta de administrador.

Para obtener más información, consulte Administración de cuentas de administrador y de miembro en el CSPM de Security Hub.

Cuenta de administrador

Una cuenta del CSPM de Security Hub a la que se le concede acceso para ver los resultados de las cuentas de miembro asociadas.

Una cuenta se convierte en cuenta de administrador de las siguientes formas:

- La cuenta invita a otras cuentas a asociarse a ella en el CSPM de Security Hub. Cuando esas cuentas aceptan la invitación, pasan a ser cuentas miembro y la cuenta que las ha invitado se convierte en su cuenta de administrador.
- Una cuenta de administración de la organización designa la cuenta como cuenta de administrador del CSPM de Security Hub. La cuenta de administrador del CSPM de Security Hub puede habilitar cualquier cuenta de la organización como cuenta de miembro y también puede invitar a otras cuentas para que se conviertan en cuentas de miembro.

Una cuenta solo puede tener una cuenta de administrador. Una cuenta no puede ser cuenta de administrador y cuenta miembro al mismo tiempo.

Región de agregación

La configuración de una región de agregación le permite ver los resultados de seguridad de varias Regiones de AWS en un solo panel.

La región de agregación es la región desde la que se visualizan y administran los resultados. Los resultados se agregan a la región de agregación desde las regiones vinculadas. Las actualizaciones de los resultados se reproducen en todas las regiones.

En la región de agregación, las páginas de Estándares de seguridad, Información y Resultados contienen datos de todas las regiones vinculadas.

Para obtener más información, consulte the section called “Agregar datos en las regiones”.

Resultado archivado

Un resultado cuyo estado de registro (`RecordState`) es `ARCHIVED`. Archivar un resultado indica que el proveedor del mismo cree que dicho resultado ya no es relevante. El estado de registro es distinto del estado del flujo de trabajo, que realiza un seguimiento del estado de la investigación de un resultado.

Los proveedores de resultados pueden usar la operación BatchImportFindings de la API del CSPM de Security Hub para archivar los resultados que creen. El CSPM de Security Hub archiva

de forma automática los resultados de controles que cumplan ciertos criterios. Para obtener más información, consulte Generación, actualización y archivado de resultados de control.

En la consola del CSPM de Security Hub, los filtros predeterminados excluyen los resultados archivados de las listas y tablas de resultados. Puede actualizar la configuración para incluir los resultados archivados. Si recupera resultados mediante la operación GetFindings de la API del CSPM de Security Hub, la operación recupera tanto los resultados archivados como los activos. Para excluir resultados archivados, puede filtrar los resultados. Por ejemplo:

```
"RecordState": [
    {
        "Comparison": "EQUALS",
        "Value": "ARCHIVED"
    }
],
```

AWS Formato de búsqueda de seguridad (ASFF)

Un formato estandarizado para el contenido de los resultados que el CSPM de Security Hub agrega o genera. El formato AWS de búsqueda de seguridad le permite usar el CSPM de Security Hub para ver y analizar los hallazgos que generan los servicios de AWS seguridad, las soluciones de terceros o el propio CSPM de Security Hub al ejecutar las comprobaciones de seguridad. Para obtener más información, consulte AWS Formato de búsqueda de seguridad (ASFF).

Controlar

Una salvaguardia o contramedida prescrita para un sistema de información o una organización diseñada para proteger la confidencialidad, integridad y disponibilidad de su información y para cumplir un conjunto de requisitos de seguridad definidos. Un estándar de seguridad está asociado a un conjunto de controles.

El término control de seguridad se refiere a los controles que tienen un ID y un título de control únicos en todos los estándares. El término control estándar se refiere a los controles que tienen ID y títulos de control específicos del estándar. Actualmente, el CSPM de Security Hub admite controles estándar únicamente en las regiones de China y AWS GovCloud (US) Regions. Los controles de seguridad son compatibles en todas las demás regiones.

Acción personalizada

Un mecanismo CSPM de Security Hub para enviar los hallazgos seleccionados a. EventBridge Se crea una acción personalizada en el CSPM de Security Hub. A continuación, se vincula a una

EventBridge regla. La regla define una acción específica que se debe realizar cuando se recibe un resultado asociado al ID de la acción personalizada. Las acciones personalizadas se pueden utilizar, por ejemplo, para enviar un resultado específico o un pequeño conjunto de resultados a un flujo de trabajo de respuesta o corrección. Para obtener más información, consulte the section called “Crear una acción personalizada”.

Cuenta de administrador delegado (Organizations)

En AWS Organizations, la cuenta de administrador delegado de un servicio puede administrar el uso de un servicio para la organización.

En el CSPM de Security Hub, la cuenta de administrador del CSPM de Security Hub también es la cuenta de administrador delegado para el CSPM de Security Hub. Cuando la cuenta de administración de la organización designa por primera vez una cuenta como administrador del CSPM de Security Hub, el CSPM de Security Hub solicita a Organizations que convierta esa cuenta en el administrador delegado.

La cuenta de administración de la organización debe elegir la cuenta de administrador delegado como la cuenta de administrador del CSPM de Security Hub en todas las regiones.

Resultado

El registro observable de un control de seguridad o una detección relacionada con la seguridad. El CSPM de Security Hub genera y actualiza resultados de control después de completar las comprobaciones de seguridad. A estos se les denomina resultados de control. Los hallazgos también pueden provenir de integraciones con productos de otros Servicios de AWS fabricantes o de terceros.

Para obtener más información, consulte the section called “Hallazgos”.

Cross-Region agregación

La agregación de resultados, información, estados de conformidad de los controles y puntuaciones de seguridad de las regiones vinculadas a una región de agregación. A continuación, puede ver todos los datos de la región de agregación y actualizar los resultados y la información de la región de agregación.

Para obtener más información, consulte the section called “Agregar datos en las regiones”.

Ingesta de resultados

La importación de los hallazgos a Security Hub CSPM desde otros AWS servicios y desde proveedores asociados externos.

Los eventos de ingesta de resultados incluyen tanto resultados nuevos como actualizaciones de resultados existentes.

Información

Una recopilación de resultados relacionados definida por una instrucción de agregación y filtros opcionales. Una información identifica un área de seguridad que requiere atención e intervención. El CSPM de Security Hub ofrece varias informaciones (predeterminadas) administradas que no se pueden modificar. También puede crear información personalizada sobre el CSPM de Security Hub para hacer un seguimiento de los problemas de seguridad que son exclusivos de su AWS entorno y uso. Para obtener más información, consulte the section called “Información”.

Región vinculada

Al habilitar la agregación entre regiones, una región vinculada es una región que agrega resultados, información, estados de conformidad de controles y puntuaciones de seguridad a la región de agregación.

En una región vinculada, las páginas de Resultados e información contienen únicamente resultados de esa región.

Para obtener más información, consulte the section called “Agregar datos en las regiones”.

Cuenta miembro

Una cuenta que ha concedido permiso a una cuenta de administrador para ver sus resultados y tomar medidas al respecto.

Una cuenta se convierte en cuenta miembro de las siguientes formas:

- La cuenta acepta una invitación de otra cuenta.
- En el caso de una cuenta de la organización, la cuenta de administrador del CSPM de Security Hub la habilita como cuenta de miembro.

Requisitos relacionados

Un conjunto de requisitos reglamentarios o del sector asignados a un control.

Regla

Un conjunto de criterios automatizados que se utiliza para evaluar si se cumple un control. Cuando se evalúa una regla, puede superarse o devolver un error. Si la evaluación no puede determinar si la regla se supera o devuelve un error, la regla se encuentra en un estado de advertencia. Si la regla no se puede evaluar, está en un estado no disponible.

Control de seguridad

Una evaluación en un momento dado específico de una regla frente a un único recurso que da lugar a un estado `PASSED`, `FAILED`, `WARNING` o `NOT_AVAILABLE`. La ejecución de un control de seguridad produce un resultado.

Cuenta de administrador del CSPM de Security Hub

Una cuenta de la organización que administra la membresía de una organización al CSPM de Security Hub.

La cuenta de administración de la organización designa la cuenta de administrador del CSPM de Security Hub de cada región. La cuenta de administración de la organización debe elegir la misma cuenta de administrador del CSPM de Security Hub en todas las regiones.

La cuenta de administrador del CSPM de Security Hub también es la cuenta de administrador delegado del CSPM de Security Hub en Organizations.

La cuenta de administrador del CSPM de Security Hub puede habilitar cualquier cuenta de la organización como cuenta de miembro. La cuenta de administrador del CSPM de Security Hub también puede invitar a otras cuentas a convertirse en cuentas de miembro.

Estándar de seguridad

Una instrucción publicada sobre un tema que especifica las características, normalmente medibles y en forma de controles, que deben cumplirse o lograrse para fines de conformidad. Los estándares de seguridad pueden basarse en marcos normativos, prácticas recomendadas o políticas internas de la empresa. Un control puede estar asociado a uno o más estándares compatibles en el CSPM de Security Hub. Para obtener más información sobre los estándares de seguridad en el CSPM de Security Hub, consulte Descripción de los estándares de seguridad en el CSPM de Security Hub.

Gravedad

La gravedad asignada a un control del CSPM de Security Hub indica el nivel de importancia que tiene ese control. La gravedad de un control puede ser Crítica, Alta, Media, Baja o Informativa. La gravedad asignada a los resultados del control es igual a la gravedad del propio control. Para obtener información sobre cómo el CSPM de Security Hub determina la gravedad de un control, consulte Niveles de gravedad correspondientes a los resultados de control.

Estado del flujo de trabajo

El estado de una investigación sobre un resultado. Para realizar un seguimiento de esto, se utiliza el atributo `Workflow.Status`.

El estado del flujo de trabajo es inicialmente `NEW`. Si ha notificado al propietario del recurso que tome medidas sobre el resultado, puede establecer el estado del flujo de trabajo en `NOTIFIED`. Si el resultado no es un problema y no requiere ninguna acción, establezca el estado del flujo de trabajo en `SUPPRESSED`. Después de revisar y corregir un resultado, establezca el estado del flujo de trabajo en `RESOLVED`.

De forma predeterminada, la mayoría de las listas de resultados solo incluyen resultados con un estado de flujo de trabajo de `NEW` o `NOTIFIED`. Las listas de resultados para los controles también incluyen resultados `RESOLVED`.

Para la operación de GetFindings, puede incluir un filtro para el estado del flujo de trabajo.

```
"WorkflowStatus": [
    {
        "Comparison": "EQUALS",
        "Value": "RESOLVED"
    }
],
```

La consola del CSPM de Security Hub proporciona una opción para establecer el estado del flujo de trabajo de los resultados. Los clientes (o herramientas SOAR, de SIEM, de venta de tickets, de administración de incidentes que trabajan en nombre de un cliente para actualizar resultados de los proveedores de resultados) también pueden utilizar BatchUpdateFindings para actualizar el estado del flujo de trabajo.

Habilitación del CSPM de Security Hub

Hay dos maneras de habilitar el CSPM AWS de Security Hub: integrándolo o manualmente. AWS Organizations

Se recomienda encarecidamente la integración con Organizations para entornos con varias cuentas y regiones. Si tiene una cuenta independiente, es necesario configurar el CSPM de Security Hub manualmente.

Verificación de los permisos necesarios

Después de registrarse en Amazon Web Services (AWS), debe habilitar el CSPM de Security Hub para usar sus capacidades y características. Para habilitar el CSPM de Security Hub, primero debe configurar permisos que permitan acceder a la consola y a las operaciones de la API del CSPM de Security Hub. Para ello, usted o su AWS administrador pueden usar AWS Identity and Access Management (IAM) para adjuntar la política AWS gestionada llamada `AWSSecurityHubFullAccess` a su identidad de IAM.

Para habilitar y administrar el CSPM de Security Hub a través de la integración con las organizaciones, también debes adjuntar la AWS política administrada denominada. `AWSSecurityHubOrganizationsAccess`

Para obtener más información, consulte AWS políticas administradas para Security Hub.

Habilitación del CSPM de Security Hub con la integración de Organizations

Para empezar a usar Security Hub CSPM con AWS Organizations, la cuenta de AWS Organizations administración de la organización designa una cuenta como la cuenta de administrador de CSPM de Security Hub delegada para la organización. El CSPM de Security Hub se habilita automáticamente en la cuenta de administrador delegada en la región actual.

Seleccione el método que prefiera y siga los pasos para designar el administrador delegado.

Security Hub CSPM console

Para designar al administrador delegado del CSPM de Security Hub durante el proceso de incorporación

1. Abra la consola CSPM de AWS Security Hub en. https://console.aws.amazon.com/securityhub/
2. Seleccione Ir al CSPM de Security Hub. Se le solicitará que inicie sesión en la cuenta de administración de Organizations.
3. En la página Designar administrador delegado, en la sección Cuenta de administrador delegado, especifique la cuenta de administrador delegado. Se recomienda que elija el mismo administrador delegado que haya configurado para otros servicios de seguridad y conformidad de AWS .
4. Elija Establecer administrador delegado.

Security Hub CSPM API

Invoque la API `EnableOrganizationAdminAccount` desde la cuenta de administración de Organizations. Proporcione el ID de Cuenta de AWS de la cuenta del administrador delegado del CSPM de Security Hub.

AWS CLI

Ejecute el comando `enable-organization-admin-account` desde la cuenta de administración de Organizations. Proporcione el ID de Cuenta de AWS de la cuenta del administrador delegado del CSPM de Security Hub.

Comando de ejemplo:

```
aws securityhub enable-organization-admin-account --admin-account-id 777788889999
```

Para obtener más información acerca de la integración con Organizations, consulte Integración de Security Hub CSPM conAWS Organizations.

Configuración centralizada

Cuando integra el CSPM de Security Hub con Organizations, tiene la opción de usar una característica llamada configuración centralizada para configurar y administrar el CSPM de Security Hub para la organización. Se recomienda encarecidamente utilizar la configuración centralizada porque permite que el administrador personalice la cobertura de seguridad de la organización. Cuando corresponde, el administrador delegado puede permitir que la cuenta de un miembro configure sus propios ajustes de cobertura de seguridad.

La configuración centralizada permite que el administrador delegado configure el CSPM de Security Hub en las cuentas, las unidades organizativas y las Regiones de AWS. El administrador delegado configura el CSPM de Security Hub mediante la creación de políticas de configuración. Dentro de una política de configuración, puede especificar la siguiente configuración:

- Si se habilita o desactiva el CSPM de Security Hub
- Los estándares de seguridad que se habilitan y deshabilitan
- Los controles de seguridad que se habilitan y deshabilitan
- Si se deben personalizar los parámetros de los controles seleccionados

Como administrador delegado, puede crear una política de configuración única para toda la organización o diferentes políticas de configuración para las distintas cuentas y unidades organizativas. Por ejemplo, las cuentas de prueba y las cuentas de producción pueden utilizar políticas de configuración diferentes.

Las cuentas de los miembros y las unidades organizativas que utilizan una política de configuración se administran de forma centralizada y solo las puede configurar el administrador delegado. El administrador delegado puede designar cuentas y unidades organizativas específicas de un miembro como autoadministrables para que el miembro pueda configurar sus propios ajustes de forma individual. Region-by-Region

Si no utiliza la configuración centralizada, debe configurar el CSPM de Security Hub, en gran medida, de forma independiente en cada cuenta y región. Esto se denomina configuración local. En la configuración local, el administrador delegado puede habilitar automáticamente el CSPM de Security Hub y un conjunto limitado de estándares de seguridad en las nuevas cuentas de la organización dentro de la región actual. La configuración local no se aplica a las cuentas de la organización existentes ni a otras regiones que no sean la actual. La configuración local tampoco admite el uso de políticas de configuración.

Habilitación manual del CSPM de Security Hub

Debe habilitar Security Hub CSPM manualmente si tiene una cuenta independiente o si no está integrada con ella. AWS Organizations Las cuentas independientes no se pueden integrar AWS Organizations y deben habilitarse manualmente.

Al habilitar el CSPM de Security Hub manualmente, designa una cuenta de administrador de este servicio e invita a otras cuentas a convertirse en cuentas de miembro. La relación entre administrador y miembros se establece cuando una potencial cuenta de miembro acepta la invitación.

Elija el método que prefiera y siga estos pasos para habilitar el CSPM de Security Hub. Al habilitar el CSPM de Security Hub desde la consola, también tiene la opción de habilitar los estándares de seguridad admitidos.

Security Hub CSPM console

1. Abra la consola AWS CSPM de Security Hub en. https://console.aws.amazon.com/securityhub/
2. Al abrir la consola del CSPM de Security Hub por primera vez, seleccione Ir al CSPM de Security Hub.

3. En la página de bienvenida, la sección Estándares de seguridad enumera los estándares de seguridad que el CSPM de Security Hub admite.

   Seleccione la casilla de verificación de un estándar para habilitarlo y quite la selección de la casilla para deshabilitarlo.

   Puede habilitar o deshabilitar un estándar o sus controles individuales en cualquier momento. Para obtener más información sobre cómo administrar los estándares de seguridad, consulte Descripción de los estándares de seguridad en el CSPM de Security Hub.

4. Seleccione Habilitar Security Hub.

Security Hub CSPM API

Invoque la API `EnableSecurityHub`. Al habilitar el CSPM de Security Hub desde la API, se habilitan automáticamente los siguientes estándares de seguridad predeterminados:

- AWS Mejores prácticas fundamentales de seguridad
- Aspectos básicos de Benchmark v1.2.0 del Centro para la Seguridad de Internet (CIS) AWS

Si no deseas habilitar estos estándares, establece `EnableDefaultStandards` como `false`.

También puede usar el parámetro `Tags` para asignar valores de etiqueta al recurso del hub.

AWS CLI

Ejecute el comando `enable-security-hub`. Para habilitar los estándares predeterminados, incluya `--enable-default-standards`. Para no habilitar los estándares predeterminados, incluya `--no-enable-default-standards`. Los estándares de seguridad predeterminados son los siguientes:

- AWS Mejores prácticas fundamentales de seguridad
- Aspectos básicos de Benchmark v1.2.0 del Centro para la Seguridad de Internet (CIS) AWS

```
aws securityhub enable-security-hub [--tags <tag values>] [--enable-default-
standards | --no-enable-default-standards]
```

Ejemplo

```
aws securityhub enable-security-hub --enable-default-standards --tags
 '{"Department": "Security"}'
```

Multi-account script de habilitación

> **Note**
>
> En lugar de este script, se recomienda utilizar la configuración centralizada para habilitar y configurar el CSPM de Security Hub en varias cuentas y regiones.

El script de activación de múltiples cuentas de Security Hub CSPM GitHub le permite habilitar Security Hub CSPM en todas las cuentas y regiones. El script también automatiza el proceso de envío de invitaciones a las cuentas miembro y de activación de AWS Config.

El script habilita automáticamente el registro de AWS Config recursos para todos los recursos, incluidos los recursos globales, en todas las regiones. No limita el registro de recursos globales a una única región. Para optimizar costos, recomendamos registrar los recursos globales únicamente en una sola región. Si utiliza configuración centralizada o agregación entre Regiones, esta debe ser la región de origen. Para obtener más información, consulte Registrar recursos en AWS Config.

Existe un script correspondiente que permite desactivar el CSPM de Security Hub en las cuentas y regiones.

Próximos pasos: gestión de la posición e integraciones

Después de habilitar el CSPM de Security Hub, recomendamos habilitar estándares y controles de seguridad para supervisar la posición de seguridad. Después de habilitar los controles, Security Hub CSPM comienza a realizar comprobaciones de seguridad y a generar resultados de control que le ayudan a detectar errores de configuración en su entorno. AWS Para recibir los resultados de los controles, debe habilitar y configurar el CSPM AWS Config de Security Hub. Para obtener más información, consulte Activación y configuración AWS Config para Security Hub CSPM.

Tras habilitar el CSPM de Security Hub, también puede aprovechar las integraciones entre el CSPM de Security Hub Servicios de AWS y otras soluciones de terceros para ver sus resultados en el CSPM de Security Hub. El CSPM de Security Hub consolida resultados provenientes de distintos orígenes y los ingiere en un formato coherente. Para obtener más información, consulte Comprensión de las integraciones en el CSPM de Security Hub.

Activación y configuración AWS Config para Security Hub CSPM

AWS Security Hub CSPM utiliza AWS Config reglas para ejecutar comprobaciones de seguridad y generar resultados para la mayoría de los controles. AWS Config proporciona una vista detallada de la configuración de los AWS recursos de su. Cuenta de AWS Utiliza reglas para definir una configuración de referencia para los recursos y un registrador de configuración para detectar si un recurso incumple las condiciones de una regla.

Algunas reglas, denominadas reglas AWS Config administradas, están predefinidas y desarrolladas por AWS Config. Otras reglas son AWS Config reglas personalizadas que desarrolla Security Hub CSPM. AWS Config las reglas que Security Hub CSPM utiliza para los controles se denominan reglas vinculadas a servicios. Service-linked las reglas permiten Servicios de AWS , como Security Hub CSPM, crear AWS Config reglas en su cuenta.

Si tiene habilitados tanto AWS Security Hub CSPM como Security Hub, Security Hub CSPM crea automáticamente un grabador de configuración vinculado a servicios para evaluar sus controles de seguridad. No necesita activarlos ni configurarlos manualmente. AWS Config Para obtener más información, consulte Uso del grabador de configuración vinculado a un servicio.

Si tiene el Security Hub CSPM activado sin Security Hub, debe habilitar AWS Config y activar manualmente el registro de recursos. Para obtener más información, consulte Configuración manual AWS Config.

AWS Config Los requisitos previos descritos en esta página se aplican únicamente a los estándares de AWS seguridad, como AWS Foundational Security Best Practices y CIS AWS Foundations Benchmark. Los estándares multinube, como CIS Azure Foundations Benchmark v4.0.0, no requieren que habilite la AWS Config grabación ni configure una grabadora de configuración. El conector multicloud CSPM de Security Hub configura automáticamente una grabadora vinculada a un servicio para evaluar los recursos externos de la nube. El único requisito previo para los estándares multinube es un conector CSPM de Security Hub para el proveedor de nube externo.

Temas

- Uso del grabador de configuración vinculado a un servicio
- Configuración manual AWS Config
- Entender el control Config.1
- Generación de reglas vinculadas al servicio

Uso del grabador de configuración vinculado a un servicio

Cuando tiene habilitados tanto AWS Security Hub CSPM como Security Hub, Security Hub CSPM crea y administra automáticamente un grabador de configuración vinculado a servicios en todas sus cuentas y regiones. No es necesario que lo habilite o configure manualmente. AWS Config

El nombre de esta grabadora de configuración es`AWSConfigurationRecorderForSecurityHubCSPM`. Security Hub CSPM crea un grabador de configuración vinculado al servicio correspondiente para cada cuenta y región en la que estén habilitados tanto el Security Hub CSPM como el Security Hub. Al habilitar el CSPM de Security Hub para los nuevos Cuenta de AWS s y Región de AWS s, Security Hub CSPM crea automáticamente el grabador de configuración vinculado al servicio.

Security Hub (CSPM) administra la configuración de recursos del grabador de configuración vinculado al servicio, lo que garantiza que la grabación esté habilitada para todos los recursos que están vinculados a los controles compatibles con Security Hub. Para obtener una lista de los recursos necesarios, consulte. ObligatorioAWS Configrecursos para hallazgos de control

Cuando Security Hub CSPM crea este grabador de configuración vinculado a un servicio, Security Hub no utiliza el grabador de configuración administrado por el cliente en. AWS Config

Para obtener más información sobre los grabadores de configuración, consulte Trabajar con el grabador de configuración en la Guía para desarrolladores.AWS Config

Configuración manual AWS Config

Los siguientes pasos se aplican cuando el Security Hub CSPM está activado sin Security Hub. En este caso, debe habilitar AWS Config en su cuenta y activar el registro de recursos para los tipos de recursos que evalúen sus controles habilitados. Una vez hecho esto, Security Hub CSPM crea las AWS Config reglas adecuadas y comienza a ejecutar comprobaciones de seguridad para generar hallazgos.

Consideraciones antes de habilitar y configurar AWS Config

Para recibir los resultados de control en Security Hub CSPM, AWS Config debe estar habilitado en su cuenta en todos los Región de AWS lugares en los que Security Hub CSPM esté habilitado. Si utiliza el CSPM de Security Hub en un entorno de varias cuentas, AWS Config debe estar habilitado en cada región tanto para la cuenta de administrador como para todas las cuentas de miembro.

Le recomendamos encarecidamente que active el registro de recursos AWS Config antes de activar los estándares y controles CSPM de Security Hub. Esto ayuda a garantizar que los resultados de control sean precisos.

Para activar el registro de recursos AWS Config, debe tener permisos suficientes para registrar los recursos en la función AWS Identity and Access Management (IAM) asociada a la grabadora de configuración. Además, asegúrese de que ninguna política o AWS Organizations política de IAM le AWS Config impida tener permiso para registrar sus recursos. Los controles CSPM de Security Hub evalúan las configuraciones de los recursos directamente y no tienen en cuenta AWS Organizations las políticas. Para obtener más información sobre el registro de AWS Config , consulte Utilización del registrador de configuración en la Guía para desarrolladores de AWS Config .

Si habilita un estándar en Security Hub CSPM pero no lo ha habilitado AWS Config, Security Hub CSPM intentará crear AWS Config reglas vinculadas a servicios de acuerdo con la siguiente programación:

- El día en que habilite el estándar.
- El día después de habilitar el estándar.
- Tres días después de habilitar el estándar.
- Siete días después de habilitar el estándar, y luego cada siete días de forma continua.

Si utiliza la configuración central, el Security Hub CSPM también intenta crear AWS Config reglas vinculadas a servicios cada vez que asocia una política de configuración que habilita uno o más estándares con las cuentas, las unidades organizativas (OU) o la raíz.

Registrar recursos en AWS Config

Al habilitarla AWS Config, debe especificar qué AWS recursos desea que grabe la grabadora de AWS Config configuración. A través de las reglas vinculadas al servicio, el registrador de configuración permite que el CSPM de Security Hub detecte cambios en las configuraciones de los recursos.

Para que el CSPM de Security Hub genere resultados de control precisos, debe activar el registro en AWS Config para los tipos de recursos que corresponden a los controles habilitados. Principalmente son los controles habilitados con un tipo de programación activada por cambios los que requieren registro de recursos. Algunos controles con un tipo de programación periódica también requieren registro de recursos. Para obtener la lista de estos controles y sus recursos correspondientes, consulte ObligatorioAWS Configrecursos para hallazgos de control.

> **Warning**
>
> Si no configura la AWS Config grabación correctamente para los controles CSPM de Security Hub, se pueden producir resultados de control imprecisos, especialmente en los siguientes casos:
>
> - Nunca registró el recurso para un control determinado, o desactivó el registro de un recurso antes de crear ese tipo de recurso. En estos casos, recibe un resultado `WARNING` para el control correspondiente, incluso si creó recursos dentro del alcance del control después de haber desactivado el registro. Este resultado `WARNING` es un resultado predeterminado que no evalúa realmente el estado de configuración del recurso.
> - Desactiva el registro para un recurso que es evaluado por un control determinado. En este caso, el CSPM de Security Hub retiene los resultados de control generados antes de que desactivara el registro, aún cuando el control ya no evalúe recursos nuevos o actualizados. El CSPM de Security Hub también cambia el estado de cumplimiento de los resultados a `WARNING`. Es posible que estos resultados retenidos no reflejen con precisión el estado de configuración actual de un recurso.

De forma predeterminada, AWS Config registra todos los recursos regionales compatibles que descubre Región de AWS en los que se está ejecutando. Para recibir todos los resultados de control de CSPM de Security Hub, también debe configurarlo AWS Config para registrar los recursos globales. Para optimizar costos, recomendamos registrar los recursos globales únicamente en una sola región. Si utiliza configuración centralizada o agregación entre Regiones, esta región debe ser la región de origen.

En AWS Config, puede elegir entre el registro continuo o el registro diario de los cambios en el estado de los recursos. Si elige el registro diario, AWS Config entrega los datos de configuración de los recursos al final de cada período de 24 horas si se producen cambios en el estado de los recursos. Si no hay cambios, no se entrega ningún dato. Esto puede retrasar la generación de resultados del CSPM de Security Hub para los controles activados por cambios hasta que finalice el periodo completo de 24 horas.

Para obtener más información sobre la AWS Config grabación, consulte Grabación de AWS recursos en la Guía para AWS Config desarrolladores.

Formas de habilitar y configurar AWS Config

Puede habilitar AWS Config y activar el registro de recursos de cualquiera de las siguientes maneras:

- AWS Config consola: puedes habilitar AWS Config una cuenta mediante la AWS Config consola. Para obtener instrucciones, consulte Configuración AWS Config con la consola en la Guía para AWS Config desarrolladores.
- AWS CLI o SDK: puedes habilitar AWS Config una cuenta mediante AWS Command Line Interface (AWS CLI). Para obtener instrucciones, consulta Cómo configurar AWS Config con el AWS CLI en la Guía para AWS Config desarrolladores. AWS Los kits de desarrollo de software (SDK) también están disponibles para muchos lenguajes de programación.
- CloudFormation plantilla: AWS Config para habilitarla en varias cuentas, le recomendamos que utilice la AWS CloudFormation plantilla denominada Enable AWS Config. Para acceder a esta plantilla, consulte las plantillas AWS CloudFormation StackSet de muestra en la Guía del AWS CloudFormation usuario.

  De forma predeterminada, esta plantilla excluye el registro de los recursos globales de IAM. Asegúrese de habilitar el registro de los recursos globales de IAM en una sola Región de AWS para optimizar los costos de registro. Si tiene habilitada la agregación entre regiones, esta debe ser la Región de origen del CSPM de Security Hub. De lo contrario, puede ser cualquier región en la que el CSPM de Security Hub esté disponible y que admita el registro de los recursos globales de IAM. Recomendamos ejecutar una StackSet para registrar todos los recursos, incluidos los recursos globales de IAM, de la región de origen o de otra región seleccionada. A continuación, ejecute un segundo StackSet para registrar todos los recursos, excepto los recursos globales de IAM en otras regiones.
- GitHub script: Security Hub CSPM ofrece un GitHubscript que habilita Security Hub CSPM y AWS Config para múltiples cuentas en todas las regiones. Este script es útil si no te has integrado en una organización AWS Organizations o tienes algunas cuentas de miembros que no forman parte de ella.

Para obtener más información, consulte la siguiente entrada del blog de AWS seguridad: Optimice AWS Config for AWS Security Hub CSPM para gestionar eficazmente su postura de seguridad en la nube.

Consideraciones sobre costos

El CSPM de Security Hub puede afectar a los costes de AWS Config la grabadora de configuración al actualizar el elemento de `AWS::Config::ResourceCompliance` configuración. Las actualizaciones se pueden producir cada vez que un control CSPM de Security Hub asociado a una AWS Config regla cambia de estado de conformidad, se habilita o deshabilita, o se actualiza los parámetros. Si usa la grabadora de AWS Config configuración solo para Security Hub CSPM

y no usa este elemento de configuración para otros fines, le recomendamos que desactive la grabación. AWS Config Esto puede reducir sus costos de AWS Config . No es necesario registrar `AWS::Config::ResourceCompliance` para que las comprobaciones de seguridad funcionen en el CSPM de Security Hub.

Para obtener información sobre los costos asociados al registro de recursos, consulte Precios del CSPM de AWS Security Hub y Precios de AWS Config.

Entender el control Config.1

> **Note**
>
> Cuando AWS Security Hub CSPM y Security Hub están habilitados, el Config.1 control siempre tiene el estado de. `PASSED` Security Hub CSPM tiene acceso directo a los elementos de configuración a través de un grabador de configuración vinculado a un servicio. Para obtener más información, consulte Uso del grabador de configuración vinculado a un servicio.

En Security Hub CSPM, el Config.1control genera `FAILED` resultados en su cuenta si AWS Config está deshabilitado. También genera `FAILED` resultados en tu cuenta si AWS Config está activado pero el registro de recursos no está activado.

Si AWS Config está habilitado y el registro de recursos está activado, pero el registro de recursos no está activado para un tipo de recurso que comprueba un control habilitado, Security Hub CSPM genera una `FAILED` búsqueda para el Config.1 control. Además de este resultado `FAILED`, el CSPM de Security Hub genera resultados `WARNING` para el control habilitado y para los tipos de recursos que dicho control verifica. Por ejemplo, si habilita el KMS.5control y el registro de recursos no está activado AWS KMS keys, Security Hub CSPM generará una `FAILED` búsqueda para el Config.1 control. Security Hub CSPM también genera `WARNING` resultados para el KMS.5 control y sus claves KMS.

Para recibir información sobre el Config.1 control, active el registro de recursos para todos los tipos de recursos que correspondan a los controles habilitados. `PASSED` Desactive también los controles que no necesita en la organización. Esto ayuda a garantizar que no existan vacíos de configuración en las comprobaciones de controles de seguridad. También ayuda a asegurarse de que reciba resultados precisos sobre recursos mal configurados.

Si es el administrador delegado del CSPM de Security Hub para una organización, el registro de AWS Config debe estar configurado correctamente para la cuenta y para las cuentas de miembro. Si

utiliza la agregación entre regiones, el AWS Config registro debe configurarse correctamente en la región de origen y en todas las regiones vinculadas. No es necesario registrar los recursos globales en las regiones vinculadas.

Generación de reglas vinculadas al servicio

Para cada control que utilice una AWS Config regla vinculada a un servicio, Security Hub CSPM crea instancias de la regla requerida en su entorno. AWS

Estas reglas vinculadas al servicio son exclusivas del CSPM de Security Hub. El CSPM de Security Hub crea estas reglas vinculadas al servicio incluso si ya existen otras instancias de las mismas reglas. La regla vinculada al servicio agrega `securityhub` antes del nombre original de la regla y un identificador único después del nombre. Por ejemplo, para la regla AWS Config administrada, el nombre de la regla `vpc-flow-logs-enabled` vinculada al servicio podría ser. `securityhub-vpc-flow-logs-enabled-12345`

Hay cuotas para el número de reglas AWS Config administradas que se pueden usar para evaluar los controles. AWS Config las reglas que crea Security Hub CSPM no cuentan para esas cuotas. Puedes habilitar un estándar de seguridad incluso si ya has alcanzado la AWS Config cuota de reglas administradas en tu cuenta. Para obtener más información sobre las cuotas de AWS Config las reglas, consulta los límites de servicio AWS Config en la Guía para AWS Config desarrolladores.

> **Note**
>
> Si utiliza Security Hub, CSPM y Security Hub, puede ver las reglas vinculadas al servicio, AWS Config pero no podrá ver los recursos compatibles o no conformes asociados a la regla. Los recursos conformes y no conformes solo estarán visibles en Security Hub, CSPM y Security Hub.

Descripción de la configuración local en el CSPM de Security Hub

La configuración local es la forma predeterminada en que se configura una AWS organización en Security Hub CSPM. Si no opta por la configuración centralizada ni la habilita, su organización utilizará la configuración local de forma predeterminada.

Al utilizar la configuración local, la cuenta de administrador delegado del CSPM de Security Hub tiene control limitado sobre los ajustes de configuración. El administrador delegado solo puede

aplicar dos configuraciones: habilitar automáticamente el CSPM de Security Hub y los estándares de seguridad predeterminados en las cuentas nuevas de la organización. Estos ajustes solo se aplican en la región en la que designó la cuenta de administrador delegado. Los estándares de seguridad predeterminados son AWS Foundational Security Best Practices (FSBP) y Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0. Los ajustes de configuración local no se aplican a las cuentas de la organización existentes ni a regiones distintas de aquella en la que se designó la cuenta de administrador delegado.

Aunque puede habilitar el CSPM de Security Hub y los estándares predeterminados para las nuevas cuentas de la organización en una sola región, el resto de la configuración del CSPM de Security Hub, incluidos los estándares y los controles, se debe realizar de forma independiente en cada región y en cada cuenta. Dado que este proceso puede duplicarse, le recomendamos que utilice la configuración centralizada para un entorno de varias cuentas si se presentan una o más de las siguientes situaciones:

- Quiere establecer distintos ajustes para las distintas partes de la organización (por ejemplo, distintos estándares o controles habilitados para los diferentes equipos).
- Trabaja en varias regiones y desea reducir el tiempo y la complejidad de la configuración del servicio en esas regiones.
- Desea que las cuentas nuevas usen ajustes específicos cuando se unan a la organización.
- Desea que las cuentas de la organización hereden ajustes específicos de una cuenta principal o raíz.

Para obtener información acerca de la configuración centralizada, consulte Descripción de la configuración central en el CSPM de Security Hub.

Descripción de la configuración central en el CSPM de Security Hub

La configuración central es una función CSPM del AWS Security Hub que le ayuda a configurar y administrar el Security Hub CSPM en múltiples y. Cuentas de AWS Regiones de AWS Para utilizar la configuración central, primero debe integrar Security Hub CSPM y. AWS Organizations Para integrar los servicios, puede crear una organización y designar una cuenta de administrador delegado del CSPM de Security Hub para la organización.

Desde la cuenta de administrador delegado del CSPM de Security Hub, puede habilitar el CSPM de Security Hub para las cuentas y las unidades organizativas (UO) de la organización en las regiones. También puede habilitar, configurar y desactivar los estándares de seguridad y los controles de

seguridad individuales para las cuentas y las unidades organizativas en las regiones. Puede configurar estos ajustes en tan solo unos pasos desde una región principal, denominada región de origen.

Al utilizar la configuración centralizada, el administrador delegado puede elegir qué cuentas y unidades organizativas desea configurar. Si el administrador delegado designa una cuenta de miembro o una unidad organizativa como autoadministrada, el miembro puede configurar sus propios ajustes por separado en cada región. Si el administrador delegado designa una cuenta de miembro o una unidad organizativa como administrada de forma centralizada, solo el administrador delegado puede configurar la cuenta de miembro o la unidad organizativa en todas las regiones. Puede designar todas las cuentas y unidades organizativas de su organización como administradas de forma centralizada, todas autoadministradas o como una combinación de ambas.

Para configurar las cuentas administradas de forma centralizada, el administrador delegado utiliza las políticas de configuración del CSPM de Security Hub. Las políticas de configuración permiten al administrador delegado especificar si el CSPM de Security Hub está habilitado o desactivado, así como determinar qué estándares y controles están habilitados o desactivados. También se pueden utilizar para personalizar los parámetros de determinados controles.

Las políticas de configuración entran en vigor en la región de origen y en todas las regiones vinculadas. El administrador delegado especifica la región de origen de la organización y las regiones vinculadas antes de empezar a utilizar la configuración centralizada. La especificación de las regiones vinculadas es opcional. El administrador delegado puede crear una única política de configuración para toda la organización, o crear varias políticas de configuración para configurar ajustes variables en diferentes cuentas y unidades organizativas.

> **Tip**
>
> Si no utiliza la configuración centralizada, debe configurar el CSPM de Security Hub, en gran medida, de forma independiente en cada cuenta y región. Esto se denomina configuración local. En la configuración local, el administrador delegado puede habilitar automáticamente el CSPM de Security Hub y un conjunto limitado de estándares de seguridad en las nuevas cuentas de la organización dentro de la región actual. La configuración local no se aplica a las cuentas de la organización existentes ni a otras regiones que no sean la actual. La configuración local tampoco admite el uso de políticas de configuración.

En esta sección, se proporciona información general acerca de la configuración centralizada.

Beneficios de usar la configuración centralizada

Entre los beneficios de la configuración centralizada, se incluyen los siguientes:

Simplificación de la configuración del servicio y las capacidades del CSPM de Security Hub

Cuando utiliza la configuración centralizada, el CSPM de Security Hub proporciona una guía para configurar las prácticas recomendadas de seguridad en la organización. También implementa automáticamente las políticas de configuración resultantes en cuentas y unidades organizativas específicas. Si ya cuenta con configuraciones existentes del CSPM de Security Hub, como habilitar automáticamente nuevos controles de seguridad, puede utilizarlas como punto de partida para las políticas de configuración. Además, la página Configuración de la consola del CSPM de Security Hub muestra un resumen en tiempo real de las políticas de configuración, así como de las cuentas y unidades organizativas que utilizan cada política.

Configuración en todas las cuentas y regiones

Puede utilizar la configuración centralizada para configurar el CSPM de Security Hub en varias cuentas y regiones. Esto ayuda a garantizar que cada parte de la organización mantenga una configuración coherente y una cobertura de seguridad adecuada.

Compatibilidad con diferentes configuraciones en diferentes cuentas y unidades organizativas

Con la configuración centralizada, puede elegir si desea configurar las cuentas y unidades organizativas de su organización de diferentes maneras. Por ejemplo, las cuentas de prueba y de producción pueden utilizar políticas de configuración diferentes. También puede crear una política de configuración que cubra las cuentas nuevas cuando se unan a la organización.

Prevención de desviaciones de la configuración

La desviación de la configuración ocurre cuando un usuario hace un cambio en un servicio o característica que entra en conflicto con las selecciones del administrador delegado. La configuración centralizada evita esta desviación. Cuando se designa una cuenta o unidad organizativa como administrada de forma centralizada, solo el administrador delegado de la organización puede configurarla. Si prefiere que una cuenta o unidad organizativa específica configure sus propios ajustes, puede designarla como autoadministrada.

¿Cuándo se debe utilizar la configuración centralizada?

La configuración central es más beneficiosa para los AWS entornos que incluyen varias cuentas CSPM de Security Hub. Está diseñada para ayudar a administrar el CSPM de Security Hub para varias cuentas.

La configuración centralizada permite configurar el servicio del CSPM de Security Hub, así como los estándares y los controles de seguridad. También pueden utilizarla para personalizar los parámetros de determinados controles. Para obtener más información sobre los estándares de seguridad, consulte Descripción de los estándares de seguridad en el CSPM de Security Hub. Para más información sobre los controles de seguridad, consulte Comprensión de los controles de seguridad en el CSPM de Security Hub.

Términos y conceptos de la configuración centralizada

Comprender los siguientes términos y conceptos clave puede ayudar a utilizar la configuración centralizada del CSPM de Security Hub.

Configuración centralizada

Una característica del CSPM de Security Hub que permite a la cuenta de administrador delegado de una organización configurar el servicio del CSPM de Security Hub, así como sus estándares y controles de seguridad en múltiples cuentas y regiones. Para configurar estos ajustes, el administrador delegado crea y administra las políticas de configuración de CSPM de Security Hub para las cuentas administradas centralmente en su organización. Self-managed las cuentas pueden configurar sus propios ajustes por separado en cada región. Para utilizar la configuración central, debe integrar Security Hub CSPM y. AWS Organizations

Región de origen

Región de AWS Desde el que el administrador delegado configura centralmente el Security Hub CSPM, mediante la creación y administración de políticas de configuración. Las políticas de configuración entran en vigor en la región de origen y en todas las regiones vinculadas.

La región de origen también sirve como la región de agregación del CSPM de Security Hub que recibe resultados, información y otros datos de las regiones vinculadas.

Las regiones que AWS se introdujeron el 20 de marzo de 2019 o después se denominan regiones de suscripción voluntaria. Una región optativa no puede ser la región de origen, pero puede

ser una región vinculada. Para ver una lista de las regiones opcionales, consulte la sección Considerations before enabling and disabling Regions en la Guía de referencia de administración de cuentas de AWS .

Región vinculada

Y Región de AWS que se pueden configurar desde la región de origen. El administrador delegado crea las políticas de configuración en la región de origen. Las políticas entran en vigor en la región de origen y en todas las regiones vinculadas. La especificación de las regiones vinculadas es opcional.

Una región vinculada también envía resultados, información y otros datos a la región de origen.

Las regiones que AWS se introdujeron el 20 de marzo de 2019 o después se denominan regiones con suscripción voluntaria. Debe habilitar dicha región para una cuenta antes de poder aplicarle una política de configuración. La cuenta de administración de Organizations puede habilitar regiones optativas para una cuenta de miembro. Para obtener más información, consulta Especificar qué Regiones de AWS cuenta puedes usar en la Guía de referencia de administración de AWS cuentas.

Destino

Una Cuenta de AWS unidad organizativa (OU) o la raíz de la organización.

Política de configuración del CSPM de Security Hub

Un conjunto de ajustes del CSPM de Security Hub que el administrador delegado puede configurar para los destinos administrados de forma centralizada. Esto incluye:

- Si se habilita o desactiva el CSPM de Security Hub.
- Si se habilitan uno o más estándares de seguridad.
- Qué controles de seguridad se habilitan en todos los estándares habilitados. Para hacerlo, el administrador delegado puede proporcionar una lista de controles específicos que deben estar habilitados, y el CSPM de Security Hub desactivará todos los demás controles (incluidos los controles nuevos cuando se lanzan). Como alternativa, el administrador delegado puede proporcionar una lista de controles específicos que deberían estar desactivados y el CSPM Security Hub habilitará todos los demás controles (incluidos los controles nuevos cuando se lanzan).
- Si lo desea, personalice parámetros de ciertos controles habilitados en los estándares habilitados.

Una política de configuración entra en vigor en la región de origen y en todas las regiones vinculadas una vez que se ha asociado al menos a una cuenta, una unidad organizativa (OU) o la raíz.

En la consola del CSPM de Security Hub, el administrador delegado puede elegir la política de configuración recomendada del CSPM de Security Hub o crear políticas de configuración personalizadas. Con la API CSPM de Security Hub y AWS CLI, el administrador delegado solo puede crear políticas de configuración personalizadas. El administrador delegado puede crear un máximo de 20 políticas de configuración personalizadas.

En la política de configuración recomendada, el CSPM de Security Hub, el estándar Prácticas recomendadas de seguridad básica de AWS (FSBP) y todos los controles FSBP existentes y nuevos están habilitados. Los controles que aceptan parámetros utilizan los valores predeterminados. La política de configuración recomendada se aplica a toda la organización.

Para aplicar diferentes configuraciones a la organización o aplicar diferentes políticas de configuración a diferentes cuentas y unidades organizativas, cree una política de configuración personalizada.

> **Note**
>
> Las políticas de configuración solo son compatibles con los estándares y controles de AWS seguridad. Los estándares multinube, como CIS Azure Foundations Benchmark v4.0.0, y sus controles multicloud asociados, no se pueden incluir en una política de configuración. Para habilitar o configurar los estándares multinube, utilice los mecanismos de configuración local directamente en el lugar deseado. Cuenta de AWS

Configuración local

El tipo de configuración predeterminado para una organización, después de integrar Security Hub CSPM y. AWS Organizations Con la configuración local, el administrador delegado puede optar por habilitar automáticamente el CSPM de Security Hub y los estándares de seguridad predeterminados en las nuevas cuentas de la organización en la región actual. Si el administrador delegado habilita automáticamente los estándares predeterminados, todos los controles que forman parte de estos estándares también se habilitan automáticamente con los parámetros predeterminados para las nuevas cuentas de la organización. Esa configuración no se aplica a las cuentas existentes, por lo que es posible que se modifique la configuración una vez que una cuenta se una a la organización. La deshabilitación de controles específicos que forman parte de

los estándares predeterminados y la configuración de estándares y controles adicionales deben llevarse a cabo por separado en cada cuenta y región.

La configuración local no admite el uso de políticas de configuración. Para usar las políticas de configuración, debe cambiar a la configuración centralizada.

Administración manual de cuentas

Si no integra Security Hub CSPM AWS Organizations o tiene una cuenta independiente, debe especificar la configuración de cada cuenta por separado en cada región. La administración manual de cuentas no admite el uso de políticas de configuración.

API de configuración centralizada

Operaciones del CSPM de Security Hub que solo el administrador delegado del CSPM de Security Hub puede usar en la región de origen para administrar políticas de configuración para cuentas administradas centralmente. Las operaciones incluyen:

- `CreateConfigurationPolicy`
- `DeleteConfigurationPolicy`
- `GetConfigurationPolicy`
- `ListConfigurationPolicies`
- `UpdateConfigurationPolicy`
- `StartConfigurationPolicyAssociation`
- `StartConfigurationPolicyDisassociation`
- `GetConfigurationPolicyAssociation`
- `BatchGetConfigurationPolicyAssociations`
- `ListConfigurationPolicyAssociations`

Account-specific API

Operaciones del CSPM de Security Hub que se pueden utilizar para habilitar o desactivar el CSPM de Security Hub, los estándares y los controles cuenta por cuenta. Estas operaciones se utilizan en cada región individual.

Self-managed las cuentas pueden usar operaciones específicas de la cuenta para configurar sus propios ajustes. Las cuentas administradas de forma centralizada no pueden llevar a cabo las siguientes operaciones específicas de la cuenta en la región de origen y en las regiones vinculadas. En esas regiones, solo el administrador delegado puede configurar las cuentas

administradas de forma centralizada mediante operaciones de configuración y políticas de configuración centralizadas.

- `BatchDisableStandards`
- `BatchEnableStandards`
- `BatchUpdateStandardsControlAssociations`
- `DisableSecurityHub`
- `EnableSecurityHub`
- `UpdateStandardsControl`

Para comprobar el estado de una cuenta, el propietario de una cuenta administrada de forma centralizada puede utilizar cualquiera de las operaciones `Get` o `Describe` de la API del CSPM de Security Hub.

Si utiliza la configuración local o la administración manual de la cuenta, en lugar de la configuración centralizada, puede utilizar estas operaciones específicas de la cuenta.

Self-managed las cuentas también pueden usar las operaciones`*Invitations`. `*Members` Sin embargo, recomendamos que las cuentas autoadministradas no utilicen estas operaciones. Las asociaciones de políticas pueden fallar si la cuenta de miembro tiene sus propios miembros que forman parte de una organización diferente a la del administrador delegado.

Unidad organizativa (OU)

En AWS Organizations Security Hub CSPM, un contenedor para un grupo de. Cuentas de AWS Una unidad organizativa (OU) también puede contener otras unidades organizativas, lo que le permite crear una jerarquía que se asemeja a un árbol invertido, con una unidad organizativa principal en la parte superior y ramas de unidades organizativas que descienden y terminan en cuentas que son las hojas del árbol. Una unidad organizativa puede tener una unidad principal y cada cuenta de la organización puede ser miembro de exactamente una unidad organizativa.

Puede administrar unidades organizativas en AWS Organizations o. AWS Control Tower Para obtener más información, consulte Administración de unidades organizativas en la Guía del usuario de AWS Organizations o Control de organizaciones y cuentas con AWS Control Tower en la Guía del usuario de AWS Control Tower .

El administrador delegado puede asociar las políticas de configuración a cuentas o unidades organizativas específicas, o a la cuenta raíz para abarcar todas las cuentas y unidades organizativas de una organización.

Administrada de forma centralizada

Un destino que solo el administrador delegado puede configurar en todas las regiones mediante políticas de configuración.

La cuenta de administrador delegado especifica si un destino se administra de forma centralizada. El administrador delegado también puede cambiar el estado del destino de administrado centralmente a autoadministrado o al revés.

Self-managed

Un destino que administre su propia configuración del CSPM de Security Hub. Un destino autoadministrado utilice operaciones específicas de la cuenta para configurar el CSPM de Security Hub por separado en cada región. Esto contrasta con los destinos administrados de forma centralizada, que solo el administrador delegado puede configurar en todas las regiones mediante políticas de configuración.

La cuenta de administrador delegado especifica si un destino es autoadministrado. El administrador delegado puede aplicar un comportamiento autoadministrado a un destino. Como alternativa, una cuenta o unidad organizativa pueden heredar el comportamiento autoadministrado de una unidad principal.

La cuenta de administrador delegado en sí puede ser una cuenta autoadministrada. La cuenta de administrador delegado puede cambiar el estado de un destino, de autoadministrado a administrado de forma centralizada o al revés.

Asociación de políticas de configuración

Enlace entre una política de configuración y una cuenta, unidad organizativa (OU) o raíz. Cuando existe una asociación de políticas, la cuenta, la unidad organizativa o la cuenta raíz utiliza los parámetros definidos en la política de configuración. Existe una asociación en cualquiera de estos casos:

- Cuando el administrador delegado aplica directamente una política de configuración a una cuenta, unidad organizativa o raíz
- Cuando una cuenta o unidad organizativa hereda una política de configuración de una unidad organizativa principal o de la cuenta raíz

Existe una asociación hasta que se aplique o herede una configuración diferente.

Política de configuración aplicada

Tipo de asociación de políticas de configuración en la que el administrador delegado aplica directamente una política de configuración a las cuentas de destino, a las unidades organizativas o a la cuenta raíz. Los destinos se configuran de la manera que define la política de configuración y solo el administrador delegado puede cambiar su configuración. Si se aplica a la cuenta raíz, la política de configuración afecta a todas las cuentas y unidades organizativas de la organización que no utilicen una configuración diferente mediante la aplicación o la herencia de la cuenta principal más cercana.

El administrador delegado también puede aplicar una configuración autoadministrada a cuentas específicas, unidades organizativas o la raíz.

Política de configuración heredada

Tipo de asociación de políticas de configuración en la que una cuenta o unidad organizativa adopta la configuración de la unidad organizativa principal más cercana o de la raíz. Si una política de configuración no se aplica directamente a una cuenta o unidad organizativa, hereda la configuración de la unidad principal más cercana. Todos los elementos de una política se heredan. En otras palabras, una cuenta o unidad organizativa no puede elegir si hereda solo partes de una política de forma selectiva. Si la unidad principal más cercana está autoadministrada, la cuenta secundaria o la unidad organizativa hereda el comportamiento autoadministrado de la unidad principal.

La herencia no puede anular una configuración aplicada. Es decir, si una política de configuración o una configuración autoadministrada se aplica directamente a una cuenta o unidad organizativa, utiliza esa configuración y no hereda la configuración de la unidad principal.

Raíz

En AWS Organizations Security Hub CSPM, el nodo principal de nivel superior de una organización. Si el administrador delegado aplica una política de configuración a la cuenta raíz, la política se asocia a todas las cuentas y unidades organizativas de la organización, a menos que utilicen una política diferente, por aplicación o herencia, o se designen como autoadministradas. Si el administrador designa la raíz como autoadministrada, todas las cuentas y unidades organizativas de la organización se autoadministran, a menos que utilicen una política de configuración por aplicación o herencia. Si la raíz es autoadministrada y actualmente no existen políticas de configuración, todas las cuentas nuevas de la organización retienen su configuración actual.

Las cuentas nuevas que se unen a una organización se clasifican en la raíz hasta que se asignan a una unidad organizativa específica. Si una cuenta nueva no está asignada a una unidad organizativa, hereda la configuración raíz, a menos que el administrador delegado la designe como cuenta autoadministrada.

Habilitación de la configuración centralizada en el CSPM de Security Hub

La cuenta de administrador de CSPM de AWS Security Hub delegada puede usar la configuración central para configurar el CSPM, los estándares y los controles de Security Hub para varias cuentas y unidades organizativas (OU) en todas partes. Regiones de AWS

Para obtener información general sobre las ventajas de la configuración centralizada y su funcionamiento, consulte Descripción de la configuración central en el CSPM de Security Hub.

En esta sección, se explican los requisitos previos para la configuración centralizada y cómo empezar a utilizarla.

Requisitos previos para la configuración centralizada

Antes de empezar a utilizar la configuración central, debe integrar Security Hub CSPM AWS Organizations y designar una región de origen. Si usa la consola del CSPM de Security Hub, estos requisitos forman parte del flujo de inscripción para la configuración centralizada.

Integración con Organizations

Debe integrar el CSPM de Security Hub y Organizations para utilizar la configuración centralizada.

Para integrar estos servicios, comience por crear una organización en Organizations. Desde la cuenta de administración de Organizations, se designa una cuenta como administrador delegado del CSPM de Security Hub. Para obtener instrucciones, consulte Integración de Security Hub CSPM conAWS Organizations.

Asegúrese de designar un administrador delegado en la región de origen prevista. Cuando empieza a utilizar la configuración centralizada, también se establece automáticamente el mismo administrador delegado en todas las regiones vinculadas. La cuenta de administración de Organizations no se puede establecer como cuenta de administrador delegado.

> **Important**
>
> Cuando se usa la configuración centralizada, no puede utilizar la consola del CSPM de Security Hub ni las API del CSPM de Security Hub para cambiar o eliminar la cuenta de

administrador delegado. Si la cuenta de administración de la organización utiliza AWS Organizations las API para cambiar o eliminar al administrador delegado de CSPM de Security Hub, Security Hub CSPM detiene automáticamente la configuración central. Sus políticas de configuración también se desasocian y se eliminan. Las cuentas de miembro retienen la configuración que tenían antes de que se cambiara o eliminara el administrador delegado.

Designación de una región de origen

Debe designar una región de origen para utilizar la configuración centralizada. La región de origen es aquella desde la que el administrador delegado configura la organización.

> **Note**
>
> La región de origen no puede ser una región AWS designada como región opcional. Las regiones optativas están deshabilitadas de forma predeterminada. Para ver una lista de las regiones opcionales, consulte la sección Considerations before enabling and disabling Regions en la Guía de referencia de administración de cuentas de AWS.

Si lo desea, puede especificar una o más regiones vinculadas que se puedan configurar desde la región de origen.

El administrador delegado puede crear y administrar políticas de configuración solo desde la región de agregación. Las políticas de configuración entran en vigor en la región de origen y en todas las regiones vinculadas. No puede crear una política de configuración que se aplique exclusivamente a un subconjunto de estas regiones. La excepción a esto son los controles que involucran recursos globales. Si usa la configuración centralizada, el CSPM de Security Hub desactiva automáticamente los controles que implican recursos globales en todas las regiones, excepto en la región de origen. Para obtener más información, consulte Controles que utilizan recursos globales.

La región de origen también es la región de agregación del CSPM de Security Hub que recibe resultados, información y otros datos de las regiones vinculadas.

Si ya ha establecido una región de agregación para la agregación entre regiones, esa será su región de origen predeterminada para la configuración centralizada. Puede cambiar la región de origen antes de empezar a utilizar la configuración centralizada. Para ello, elimine su agregador de

resultados actual y cree uno nuevo en la región de origen que desee. Un agregador de resultados es un recurso del CSPM de Security Hub que especifica la región de origen y las regiones vinculadas.

Para designar una región de origen, consulte los pasos para configurar una región de agregación. Si ya tiene una región de origen, puede invocar la API GetFindingAggregator para ver los detalles de dicha región, lo que incluye las regiones que están vinculadas actualmente a ella.

Instrucciones para habilitar la configuración centralizada

Elija el método que prefiera y siga los pasos para habilitar la configuración centralizada en su organización.

Security Hub CSPM console

Para habilitar la configuración centralizada (consola)

1. Abra la consola CSPM de AWS Security Hub en. https://console.aws.amazon.com/securityhub/
2. En el panel de navegación, seleccione Configuración y Configuración. A continuación, elija Iniciar configuración centralizada.

   Si está en el poceso de incorporación al CSPM de Security Hub, seleccione Ir al CSPM de Security Hub.
3. En la página Designar administrador delegado, seleccione su cuenta de administrador delegado o ingrese su ID de cuenta. Si corresponde, se recomienda que elija el mismo administrador delegado que haya configurado para otros servicios de seguridad y conformidad de AWS. Elija Establecer administrador delegado.
4. En la página Centralizar organización, en la sección Regiones, seleccione su región de origen. Debe haber iniciado sesión en dicha región para continuar. Si ya ha configurado una región de agregación para la agregación entre regiones, aparecerá como la región de origen. Para cambiar la región de origen, seleccione Editar configuración de la región. A continuación, puede seleccionar la región de origen que prefiera y volver a este flujo de trabajo.
5. Seleccione al menos una región para vincularla a la región de origen. De manera opcional, elija si desea vincular automáticamente las futuras regiones compatibles con la región de origen. El administrador delegado configurará las regiones que seleccione aquí desde la región de origen. Las políticas de configuración entran en vigor en la región de origen y en todas las regiones vinculadas.

6. Seleccione Confirmar y continuar.
7. A partir de ahora, puede utilizar la configuración centralizada. Siga las instrucciones de la consola para crear su primera política de configuración. Si aún no lo tiene todo preparado para crear una política de configuración, seleccione Aún no lo tengo todo listo para configurarla. Para crear una política más adelante, puede seleccionar Configuración y, a continuación, Configuración en el panel de navegación. Para obtener instrucciones sobre cómo crear una política de configuración, consulte Creación y asociación de políticas de configuración.

Security Hub CSPM API

Para habilitar la configuración centralizada (API)

1. Con las credenciales de la cuenta de administrador delegado, invoque la API UpdateOrganizationConfiguration desde la región de origen.
2. Establezca el campo `AutoEnable` como `false`.
3. Establezca el campo `ConfigurationType` del objeto `OrganizationConfiguration` en `CENTRAL`. Esta acción tiene los siguientes efectos:
   - Designa a la cuenta que realiza la llamada como administrador delegado del CSPM de Security Hub en todas las regiones vinculadas.
   - Habilita el CSPM de Security Hub en la cuenta de administrador delegado en todas las regiones vinculadas.
   - Designa a la cuenta que realiza la llamada como administrador delegado del CSPM de Security Hub para las cuentas nuevas y existentes que utilizan el CSPM de Security Hub y pertenecen a la organización. Esto ocurre en la región de origen y en todas las regiones vinculadas. La cuenta que realiza la llamada se establece como administrador delegado para las nuevas cuentas de la organización solo si están asociadas a una política de configuración que tenga el CSPM de Security Hub habiliado. La cuenta que realiza la llamada se establece como administrador delegado de las cuentas de la organización existentes solo si ya tienen el CSPM de Security Hub habilitado.
   - Se establece AutoEnable como `false` en todas las regiones vinculadas y se establece AutoEnableStandards como `NONE` en la región de origen y en todas las regiones vinculadas. Estas parámetros no son relevantes en la región de origen ni en las regiones vinculadas cuando utiliza la configuración centralizada. Sin embargo, puede

habilitar automáticamente el CSPM de Security Hub y los estándares de seguridad predeterminados en las cuentas de la organización mediante políticas de configuración.

4. A partir de ahora, puede utilizar la configuración centralizada. El administrador delegado puede crear políticas de configuración para configurar el CSPM de Security Hub en la organización. Para obtener instrucciones sobre cómo crear una política de configuración, consulte Creación y asociación de políticas de configuración.

Ejemplo de solicitud de API:

```
{
    "AutoEnable": false,
    "OrganizationConfiguration": {
        "ConfigurationType": "CENTRAL"
    }
}
```

AWS CLI

Para habilitar la configuración central (AWS CLI)

1. Con las credenciales de la cuenta de administrador delegado, ejecute el comando update-organization-configuration desde la región de origen.
2. Incluya el parámetro `no-auto-enable`.
3. Establezca el campo `ConfigurationType` del objeto `organization-configuration` en `CENTRAL`. Esta acción tiene los siguientes efectos:
   - Designa a la cuenta que realiza la llamada como administrador delegado del CSPM de Security Hub en todas las regiones vinculadas.
   - Habilita el CSPM de Security Hub en la cuenta de administrador delegado en todas las regiones vinculadas.
   - Designa a la cuenta que realiza la llamada como administrador delegado del CSPM de Security Hub para las cuentas nuevas y existentes que utilizan el CSPM de Security Hub y pertenecen a la organización. Esto ocurre en la región de origen y en todas las regiones vinculadas. La cuenta que llama se establece como administrador delegado para las nuevas cuentas de la organización solo si están asociadas a una política de configuración que tenga habilitado Security Hub. La cuenta que realiza la llamada se establece como

administrador delegado de las cuentas de la organización existentes solo si ya tienen el CSPM de Security Hub habilitado.

- Establece la opción de habilitación automática como no-auto-enable en todas las regiones vinculadas y establece auto-enable-standards como `NONE` en la región de origen y en todas las regiones vinculadas. Estas parámetros no son relevantes en la región de origen ni en las regiones vinculadas cuando utiliza la configuración centralizada. Sin embargo, puede habilitar automáticamente el CSPM de Security Hub y los estándares de seguridad predeterminados en las cuentas de la organización mediante políticas de configuración.

4. A partir de ahora, puede utilizar la configuración centralizada. El administrador delegado puede crear políticas de configuración para configurar el CSPM de Security Hub en la organización. Para obtener instrucciones sobre cómo crear una política de configuración, consulte Creación y asociación de políticas de configuración.

Comando de ejemplo:

```
aws securityhub --region us-east-1 update-organization-configuration \
--no-auto-enable \
--organization-configuration '{"ConfigurationType": "CENTRAL"}'
```

Destinos administrados centralmente y destinos autoadministrados

Al habilitar la configuración central, el administrador de CSPM de AWS Security Hub delegado puede designar cada cuenta, unidad organizativa (OU) y raíz de la organización como gestionada de forma centralizada o autogestionada. El tipo de administración de un destino determina cómo se puede especificar la configuración del CSPM de Security Hub.

Para obtener información general sobre las ventajas de la configuración centralizada y su funcionamiento, consulte Descripción de la configuración central en el CSPM de Security Hub.

En esta sección se explican las diferencias entre una designación administrada de forma centralizada y una autoadministrada, y cómo elegir el tipo de administración de una cuenta, una unidad organizativa o la raíz.

Self-managed

El propietario de una cuenta, unidad organizativa o raíz autogestionada debe configurar sus ajustes por separado en cada una de ellas. Región de AWS El administrador delegado no puede crear políticas de configuración para destinos autoadministrados.

Administrada de forma centralizada

Solo el administrador delegado del CSPM de Security Hub puede configurar los ajustes de las cuentas, las unidades organizativas o la raíz administradas de forma centralizada en la región de origen y las regiones vinculadas. Las políticas de configuración se pueden asociar a cuentas y unidades organizativas administradas de forma centralizada.

El administrador delegado puede cambiar el estado de un destino entre autoadministrado y administrado de forma centralizada. De forma predeterminada, al iniciar la configuración centralizada mediante la API del CSPM de Security Hub, todas las cuentas y la unidad organizativa se establecen como destinos autoadministrados. En la consola, el tipo de administración depende de la primera política de configuración. Las cuentas y unidades organizativas que asocie a su primera política se administran de forma centralizada. El resto de cuentas y unidades organizativas se autoadministran de forma predeterminada.

Si se asocia una política de configuración a una cuenta que anteriormente era autoadministrada, la configuración de la política reemplaza la designación de autoadministración. La cuenta pasa a administrarse de forma centralizada y adopta los ajustes reflejados en la política de configuración.

Si cambia un destino administrado centralmente a un destino autoadministrado, las configuraciones que se habían aplicado previamente a la cuenta mediante una política de configuración permanecen vigentes. Por ejemplo, una cuenta gestionada de forma centralizada podría asociarse inicialmente a una política que habilitara el CSPM de Security Hub, habilitara las prácticas recomendadas de seguridad AWS fundamentales y la deshabilitara. CloudTrail.1 Si luego designa la cuenta como autoadministrada, todas las configuraciones permanecen sin cambios. Sin embargo, el propietario de la cuenta puede modificar de manera independiente la configuración de la cuenta en adelante.

Las cuentas secundarias y las unidades organizativas pueden heredar el comportamiento autoadministrado de una cuenta principal autoadministrada, del mismo modo que las cuentas secundarias y unidades organizativas pueden heredar las políticas de configuración de una cuenta principal administrada de forma centralizada. Para obtener más información, consulte Asociación de políticas mediante la aplicación y la herencia.

Una cuenta o una unidad organizativa autoadministrada no puede heredar una política de configuración de un nodo principal o de la raíz. Por ejemplo, si desea que todas las cuentas y las unidades organizativas de su organización hereden una política de configuración de la raíz, debe cambiar el tipo de administración de los nodos autoadministrados a nodos de administración centralizada.

Opciones para configurar los ajustes en las cuentas autoadministradas

Self-managed las cuentas deben configurar sus propios ajustes por separado en cada región.

Los propietarios de cuentas autoadministradas pueden invocar las siguientes operaciones de la API del CSPM de Security Hub en cada región para establecer sus ajustes:

- `EnableSecurityHub` y `DisableSecurityHub` para habilitar o desativar el servicio del CSPM de Security Hub (si una cuenta autoadministrada tiene un administrador delegado del CSPM de Security Hub, el administrador debe desasociar la cuenta antes de que el propietario de la cuenta pueda desactivar el CSPM de Security Hub).
- `BatchEnableStandards` y `BatchDisableStandards` para habilitar o deshabilitar estándares
- `BatchUpdateStandardsControlAssociations` o `UpdateStandardsControl` para habilitar o deshabilitar controles

Self-managed las cuentas también pueden usar `*Invitations` y `*Members` operar. Sin embargo, recomendamos que las cuentas autoadministradas no utilicen estas operaciones. Las asociaciones de políticas pueden fallar si la cuenta de miembro tiene sus propios miembros que forman parte de una organización diferente a la del administrador delegado.

Para obtener descripciones de las acciones de la API del CSPM de Security Hub, consulte la Referencia de la API del CSPM de AWS Security Hub.

Self-managed las cuentas también pueden usar la consola CSPM de Security Hub o AWS CLI configurar sus ajustes en cada región.

Self-managed las cuentas no pueden invocar ninguna API relacionada con las políticas de configuración y asociaciones de políticas de CSPM de Security Hub. Solo el administrador delegado puede invocar las API de configuración centralizada y utilizar las políticas de configuración para configurar las cuentas administradas de forma centralizada.

Elección del tipo de administración de un destino

Elija el método que prefiera y siga los pasos para designar una cuenta o unidad organizativa como gestionada de forma centralizada o autogestionada en AWS Security Hub CSPM.

Security Hub CSPM console

Elección del tipo de administración de una cuenta o unidad organizativa

1. Abra la consola CSPM de AWS Security Hub en. https://console.aws.amazon.com/securityhub/

   Inicie sesión con las credenciales de la cuenta de administrador delegado del CSPM de Security Hub en la región de origen.
2. Elija Configuración.
3. En la pestaña Organización, seleccione la cuenta o la unidad organizativa de destino. Elija Edit (Edición de).
4. En la página Definir configuración, en Tipo de administración, elija Administrada de forma centralizada si desea que el administrador delegado configure la cuenta o unidad organizativa de destino. A continuación, elija Aplicar una política específica si desea asociar una política de configuración existente al destino. Elija Heredar de mi organización si desea que el destino herede la configuración de la cuenta principal más cercana. Elija Self-managedsi desea que la cuenta o la unidad organizativa configure sus propios ajustes.
5. Elija Siguiente. Revise los cambios y seleccione Guardar.

Security Hub CSPM API

Elección del tipo de administración de una cuenta o unidad organizativa

1. Invoque la API StartConfigurationPolicyAssociation desde la cuenta de administrador delegado del CSPM de Security Hub en la región de origen.
2. En el campo `ConfigurationPolicyIdentifier`, indique `SELF_MANAGED_SECURITY_HUB` si desea que la cuenta o unidad organizativa controle su propia configuración. Indique el nombre de recurso de Amazon (ARN) o el ID de la política de configuración correspondiente si desea que el administrador delegado controle la configuración de la cuenta o unidad organizativa.

3. Para el `Target` campo, proporcione el Cuenta de AWS ID, el ID de la OU o el ID raíz del objetivo cuyo tipo de administración desee cambiar. Esto asocia el comportamiento autoadministrado o la política de configuración especificada al destino. Las cuentas secundarias del destino pueden heredar el comportamiento autoadministrado o la política de configuración.

Ejemplo de solicitud de la API para designar una cuenta autoadministrada:

```
{
    "ConfigurationPolicyIdentifier": "SELF_MANAGED_SECURITY_HUB",
    "Target": {"AccountId": "123456789012"}
}
```

AWS CLI

Elección del tipo de administración de una cuenta o unidad organizativa

1. Ejecute el comando start-configuration-policy-association desde la cuenta de administrador delegado del CSPM de Security Hub en la región de origen.
2. En el campo `configuration-policy-identifier`, indique `SELF_MANAGED_SECURITY_HUB` si desea que la cuenta o unidad organizativa controle su propia configuración. Indique el nombre de recurso de Amazon (ARN) o el ID de la política de configuración correspondiente si desea que el administrador delegado controle la configuración de la cuenta o unidad organizativa.
3. Para el `target` campo, proporcione el Cuenta de AWS ID, el ID de la OU o el ID raíz del objetivo cuyo tipo de administración desee cambiar. Esto asocia el comportamiento autoadministrado o la política de configuración especificada al destino. Las cuentas secundarias del destino pueden heredar el comportamiento autoadministrado o la política de configuración.

Ejemplo de comando para designar una cuenta autoadministrada:

```
aws securityhub --region us-east-1 start-configuration-policy-association \
--configuration-policy-identifier "SELF_MANAGED_SECURITY_HUB" \
--target '{"AccountId": "123456789012"}'
```

Cómo funcionan las políticas de configuración del CSPM de Security Hub

El administrador de CSPM de AWS Security Hub delegado puede crear políticas de configuración para configurar el CSPM del Security Hub, los estándares de seguridad y los controles de seguridad de una organización. Tras crear una política de configuración, el administrador delegado puede asociarla a las determinadas cuentas, unidades organizativas (OU) o a la raíz de la organización. A continuación, la política entra en vigor en las cuentas, unidades organizativas o en la raíz especificadas.

Para obtener información general sobre las ventajas de la configuración centralizada y su funcionamiento, consulte Descripción de la configuración central en el CSPM de Security Hub.

En esta sección, se proporciona información general y detallada de las políticas de configuración.

Consideraciones respecto de la política

Antes de crear una política de configuración en el CSPM de Security Hub, tenga en cuenta los siguientes detalles.

- Las políticas de configuración deben estar asociadas para que surtan efecto: después de crear una política de configuración, puede asociarla a una o más cuentas, unidades organizativas (OU) o a la raíz. Una política de configuración se puede asociar a cuentas o unidades organizativas mediante una aplicación directa o mediante la herencia de una unidad organizativa principal.
- Se puede asociar una cuenta o unidad organizativa a una sola política de configuración: para evitar ajustes conflictivos, una cuenta o unidad organizativa solo se puede asociar a una política de configuración en un momento dado. Como alternativa, una cuenta o unidad organizativa puede autoadministrarse.
- Las políticas de configuración están completas: las políticas de configuración proporcionan una especificación completa de la configuración. Por ejemplo, una cuenta secundaria no puede aceptar la configuración de algunos controles de una política ni la configuración de otros controles de otra política. Cuando asocie una política a una cuenta secundaria, asegúrese de que la política especifique toda la configuración que desea que utilice dicha cuenta.
- No se pueden revertir las políticas de configuración: no existe la opción de revertir una política de configuración después de asociarla a cuentas o unidades organizativas. Por ejemplo, si asocia una política de configuración que deshabilita los CloudWatch controles a una cuenta específica y, a continuación, disocia esa política, los CloudWatch controles seguirán deshabilitados en esa cuenta. Para volver a habilitar CloudWatch los controles, puede asociar la cuenta a una nueva

política que habilite los controles. Como alternativa, puede cambiar la cuenta a autogestionada y habilitar cada CloudWatch control de la cuenta.

- Las políticas de configuración entran en vigor en la región de origen y en todas las regiones vinculadas: una política de configuración afecta a todas las cuentas asociadas de la región de origen y a todas las regiones vinculadas. No puede crear una política de configuración que surta efecto solo en algunas de estas regiones y no en otras. La excepción a esto son los controles que utilizan recursos globales. El CSPM de Security Hub desactiva automáticamente los controles que implican recursos globales en todas las regiones, excepto en la región de origen.

  Las regiones que AWS se introdujeron el 20 de marzo de 2019 o después se denominan regiones con suscripción voluntaria. Debe habilitar dicha región para una cuenta antes de que una política de configuración entre en vigor en ella. La cuenta de administración de Organizations puede habilitar regiones optativas para una cuenta de miembro. Para obtener instrucciones sobre cómo habilitar las regiones opcionales, consulta Especificar qué regiones puedes usar en Regiones de AWS tu cuenta en la Guía de referencia sobre la administración de AWS cuentas.

  Si la política configura un control que no está disponible en la región de origen o en una o más regiones vinculadas, el CSPM de Security Hub omite la configuración de ese control en las regiones donde no está disponible, pero aplica la configuración en las regiones donde sí lo está. No posee cobertura para un control que no está disponible en la región de origen ni en ninguna de las regiones vinculadas.
- Las políticas de configuración son recursos: como recurso, una política de configuración tiene un Nombre de recurso de Amazon (ARN) y un identificador único universal (UUID). El ARN del producto tiene el siguiente formato: `arn:`*`partition:`*`securityhub:`*`region`*`:`*`delegated administrator account ID`*`:configuration-policy/`*`configuration policy UUID`*. Una configuración autoadministrada no tiene ARN o UUID. El identificador de una configuración autoadministrada es `SELF_MANAGED_SECURITY_HUB`.
- Las políticas de configuración no admiten los estándares multinube; las políticas de configuración solo pueden incluir estándares y AWS controles de seguridad. Los estándares multinube, como CIS Azure Foundations Benchmark v4.0.0, y sus controles asociados (por ejemplo`Azure.Storage.1`) no se pueden incluir en una política de configuración. Si incluye un ARN o un ID de control estándar multinube en una política de configuración, la solicitud devuelve un. `InvalidInputException` Para habilitar o configurar los estándares multinube, utilice los mecanismos de configuración local directamente en el lugar deseado. Cuenta de AWS

Tipos de políticas de configuración

Cada política de configuración especifica la configuración siguiente:

- Habilite o desactive el CSPM de Security Hub.
- Habilite uno o más estándares de seguridad.
- Indique qué controles de seguridad están habilitados en todos los estándares habilitados. Para ello, proporcione una lista de controles específicos que deberían estar habilitados y el CSPM de Security Hub desactivará todos los demás controles, lo que incluye los controles nuevos cuando se lanzan. De forma alternativa, proporcione una lista de controles específicos que deberían estar desactivados y el CSPM de Security Hub habilitará todos los demás controles, incluidos los controles nuevos cuando se lanzan.
- Si lo desea, personalice parámetros de ciertos controles habilitados en los estándares habilitados.

Las políticas de configuración central no incluyen los ajustes de la AWS Config grabadora. Debe habilitar AWS Config y activar por separado la grabación de los recursos necesarios para que Security Hub CSPM pueda generar hallazgos de control. Para obtener más información, consulte Consideraciones antes de habilitar y configurar AWS Config.

Si usa la configuración centralizada, el CSPM de Security Hub desactiva automáticamente los controles que implican recursos globales en todas las regiones, excepto en la región de origen. Los controles que elija habilitar a través de una política de configuración están habilitados en todas las regiones en las que están disponibles. Para limitar los resultados de estos controles a una sola región, puede actualizar la configuración de la AWS Config grabadora y desactivar el registro de recursos globales en todas las regiones, excepto en la región de origen.

Si un control habilitado que implica recursos globales no es compatible en la región de origen, el CSPM de Security Hub intenta habilitarlo en una región vinculada donde sí se admita. Con la configuración centralizada, no se obtiene cobertura para un control que no está disponible ni en la región de origen ni en ninguna de las regiones vinculadas.

Para obtener una lista de los controles que implican recursos globales, consulte Controles que utilizan recursos globales.

Política de configuración recomendada

Al crear una política de configuración por primera vez en la consola del CSPM de Security Hub, tiene la opción de elegir la política recomendada del CSPM de Security Hub.

La política recomendada habilita el CSPM de Security Hub, el estándar AWS Foundational Security Best Practices (FSBP) y todos los controles FSBP nuevos y existentes. Los controles que aceptan parámetros utilizan los valores predeterminados. La política recomendada se aplica a la raíz (todas las cuentas y unidades organizativas, tanto nuevas como existentes). Tras crear la política recomendada para su organización, puede modificarla desde la cuenta de administrador delegado. Por ejemplo, puede habilitar estándares o controles adicionales o deshabilitar controles específicos del FSBP. Para obtener instrucciones sobre cómo modificar una política de configuración, consulte Actualización de las políticas de configuración.

Política de configuración personalizada

En lugar de la política recomendada, el administrador delegado puede crear hasta 20 políticas de configuración personalizadas. Puede asociar una única política personalizada a toda la organización o distintas políticas personalizadas a distintas cuentas y unidades organizativas. En el caso de una política de configuración personalizada, debe especificar la configuración que desee. Por ejemplo, puede crear una política personalizada que habilite el FSBP, AWS Foundations Benchmark v1.4.0 de Center for Internet Security (CIS) y todos los controles de esos estándares, excepto los controles de Amazon Redshift. El nivel de granularidad que utilice en las políticas de configuración personalizadas depende del alcance previsto de la cobertura de seguridad en toda la organización.

> **Note**
>
> No puede asociar una política de configuración que desactive el CSPM de Security Hub con la cuenta de administrador delegado. Esta política se puede asociar a otras cuentas, pero omite la asociación con el administrador delegado. La cuenta de administrador delegado retiene su configuración actual.

Tras crear una política de configuración personalizada, puede cambiar a la política de configuración recomendada mediante su actualización para que refleje la configuración recomendada. Sin embargo, no aparece la opción de crear la política de configuración recomendada en la consola del CSPM de Security Hub después de crear la primera política.

Asociación de políticas mediante la aplicación y la herencia

Cuando opta por la configuración centralizada por primera vez, su organización no tiene asociaciones y se comporta de la misma manera que antes de la configuración. A continuación, el administrador delegado puede establecer asociaciones entre una política de configuración o la

cuenta y el comportamiento autoadministrado, las unidades organizativas o la raíz. Las asociaciones se pueden establecer mediante aplicación o herencia.

Desde la cuenta del administrador delegado, puede aplicar directamente una política de configuración a una cuenta, unidad organizativa o la raíz. Como alternativa, el administrador delegado puede aplicar directamente una designación autoadministrada a una cuenta, unidad organizativa o raíz.

En ausencia de una aplicación directa, una cuenta o unidad organizativa hereda la configuración de la cuenta principal más cercana que tenga una política de configuración o un comportamiento autoadministrado. Si la cuenta principal más cercana está asociada a una política de configuración, la cuenta secundaria hereda esa política y solo la puede configurar el administrador delegado de la región de origen. Si el progenitor más cercano es autogestionado, el hijo hereda el comportamiento autogestionado y tiene la capacidad de especificar su propia configuración en cada uno de ellos. Región de AWS

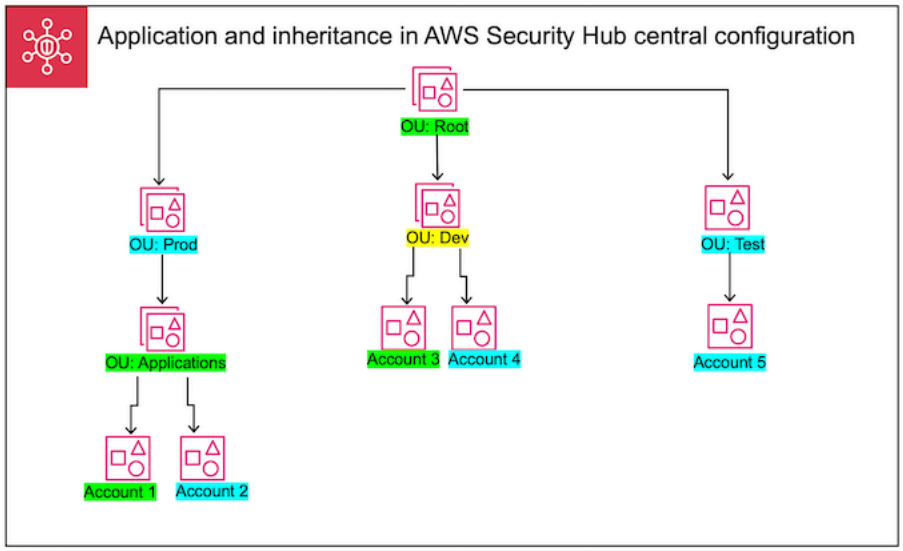
La aplicación tiene prioridad sobre la herencia. En otras palabras, la herencia no anula una política de configuración o una designación autoadministrada que el administrador delegado haya aplicado directamente a una cuenta o unidad organizativa.

Si aplica directamente una política de configuración a una cuenta autoadministrada, la política anula la designación autoadministrada. La cuenta pasa a administrarse de forma centralizada y adopta los ajustes reflejados en la política de configuración.

Recomendamos aplicar directamente una política de configuración a la raíz. Si aplica una política a la raíz, las nuevas cuentas que se unan a su organización heredarán automáticamente la política raíz, a menos que las asocie a una política diferente o las designe como autoadministrables.

Solo se puede asociar una política de configuración a una cuenta o unidad organizativa en un momento dado, ya sea mediante aplicación o herencia. Se diseñó así para evitar configuraciones conflictivas.

El siguiente diagrama ilustra cómo funcionan la aplicación de políticas y la herencia en una configuración centralizada.



En este ejemplo, se ha aplicado una política de configuración a un nodo resaltado en verde. No se ha aplicado ninguna política de configuración al nodo resaltado en azul. Un nodo resaltado en amarillo se ha designado como autoadministrado. Cada cuenta y unidad organizativa usa la siguiente configuración:

- OU:Root (Verde): esta unidad organizativa usa la política de configuración que se le ha aplicado.
- OU:Prod (Azul): esta OU hereda la política de configuración de OU:Root.
- OU:Applications (Verde): esta OU usa la política de configuración que se le ha aplicado.
- Cuenta 1 (verde): esta cuenta usa la política de configuración que se le ha aplicado.
- Cuenta 2 (azul): esta cuenta hereda la política de configuración de OU:Applications.
- OU:Dev (Amarillo): esta unidad organizativa es autogestionada.
- Cuenta 3 (verde): esta cuenta usa la política de configuración que se le ha aplicado.
- Cuenta 4 (azul): esta cuenta hereda el comportamiento autogestionado de. OU:Dev
- OU:Test (Azul): esta cuenta hereda la política de configuración de. OU:Root
- Cuenta 5 (azul): esta cuenta hereda la política de configuración OU:Test, OU:Root ya que su matriz inmediata no está asociada a ninguna política de configuración.

Prueba de una política de configuración

Para asegurarse de que comprende cómo funcionan las políticas de configuración, le recomendamos crear una política y asociarla a una cuenta de prueba o unidad organizativa.

Prueba de una política de configuración

1. Cree una política de configuración personalizada y verifique que los ajustes especificados para la habilitación del CSPM de Security Hub, los estándares y los controles sean correctos. Para obtener instrucciones, consulte Creación y asociación de políticas de configuración.
2. Aplique la política de configuración a una cuenta de prueba o unidad organizativa que no tenga cuentas secundarias ni unidades organizativas.
3. Compruebe que la cuenta de prueba o la unidad organizativa utilicen la política de configuración de la manera esperada en su región de origen y en todas las regiones vinculadas. También puede comprobar que todas las demás cuentas y unidades organizativas de su organización sigan siendo autoadministradas y pueden cambiar su propia configuración en cada región.

Después de probar una política de configuración en una sola cuenta o unidad organizativa, puede asociarla a otras cuentas y unidades organizativas.

Creación y asociación de políticas de configuración

La cuenta de administrador de CSPM de AWS Security Hub delegada puede crear políticas de configuración que especifiquen cómo se configuran el CSPM, los estándares y los controles de Security Hub en cuentas y unidades organizativas (OU) específicas. Una política de configuración solo entra en vigor una vez que el administrador delegado la asocia a al menos una cuenta o una unidad organizativa (OU), o a la raíz. El administrador delegado también puede asociar una configuración autoadministrada a cuentas, unidades organizativas o a la raíz.

Si es la primera vez que crea una política de configuración, le recomienda que revise antes Cómo funcionan las políticas de configuración del CSPM de Security Hub.

> **Note**
>
> Las políticas de configuración solo admiten AWS estándares y controles. No puede incluir estándares multinube (como CIS Azure Foundations Benchmark v4.0.0) ni controles de Azure en una política de configuración. Se incluye un ARN estándar multinube o un identificador de control. `InvalidInputException` Para habilitar o configurar los estándares multinube, utilice los mecanismos de configuración local directamente en el lugar deseado. Cuenta de AWS

Elija el método de acceso que prefiera y siga los pasos para crear y asociar una política de configuración o una configuración autoadministrada. Cuando utiliza la consola del CSPM de Security Hub, puede asociar una configuración a varias cuentas o unidades organizativas al mismo tiempo. Al utilizar la API CSPM de Security Hub o AWS CLI, puede asociar una configuración a una sola cuenta o unidad organizativa en cada solicitud.

> **Note**
>
> Si usa la configuración centralizada, el CSPM de Security Hub desactiva automáticamente los controles que implican recursos globales en todas las regiones, excepto en la región de origen. Los controles que elija habilitar a través de una política de configuración están habilitados en todas las regiones en las que están disponibles. Para limitar los resultados de estos controles a una sola región, puede actualizar la configuración de la AWS Config grabadora y desactivar el registro de recursos globales en todas las regiones, excepto en la región de origen.
>
> Si un control habilitado que implica recursos globales no es compatible en la región de origen, el CSPM de Security Hub intenta habilitarlo en una región vinculada donde sí se admita. Con la configuración centralizada, no se obtiene cobertura para un control que no está disponible ni en la región de origen ni en ninguna de las regiones vinculadas.
>
> Para obtener una lista de los controles que implican recursos globales, consulte Controles que utilizan recursos globales.

Security Hub CSPM console

Creación y asociación de políticas de configuración

1. Abra la consola CSPM de AWS Security Hub en. https://console.aws.amazon.com/securityhub/

   Inicie sesión con las credenciales de la cuenta de administrador delegado del CSPM de Security Hub en la región de origen.

2. En el panel de navegación, seleccione Configuración y la pestaña Políticas. A continuación, seleccione Crear política.

3. En la página Configurar organización, si es la primera vez que crea una política de configuración, verá tres opciones en Tipo de configuración. Si ya ha creado al menos una política de configuración, solo verá la opción Política personalizada.

- Elija Usar la configuración CSPM de Security Hub AWS recomendada en toda mi organización para usar nuestra política recomendada. La política recomendada habilita el CSPM de Security Hub en todas las cuentas de la organización, habilita el estándar AWS Foundational Security Best Practices (FSBP) y habilita todos los controles FSBP nuevos y existentes. Los controles utilizan valores de parámetros predeterminados.
- Para crear una política de configuración más tarde, seleccione Aún no lo tengo todo listo para configurarla.
- Seleccione Política personalizada para crear una política de configuración personalizada. Especifique si desea habilitar o desactivar el CSPM de Security Hub, qué estándares desea habilitar y qué controles desea habilitar dentro de esos estándares. Si lo desea, especifique valores de parámetros personalizados para uno o más controles habilitados que admitan parámetros personalizados.

4. En la sección Cuentas, seleccione las cuentas de destino, las unidades organizativas o la raíz a las que desea que se aplique la política de configuración.

   - Seleccione Todas las cuentas si desea aplicar la política de configuración a la raíz. Esto incluye todas las cuentas y unidades organizativas de la organización a las que no se les ha aplicado ninguna otra política o que no hayan sido heredadas.
   - Seleccione Cuentas específicas si desea aplicar la política de configuración a cuentas o unidades organizativas específicas. Ingrese los ID de las cuentas o seleccione las cuentas y unidades organizativas en la estructura de la organización. Puede aplicar la política a un máximo de 15 destinos (cuentas, unidades organizativas o raíz) cuando la crea. Para especificar un número mayor, edite la política después de crearla y aplíquela a destinos adicionales.
   - Seleccione Solo el administrador delegado para aplicar la política de configuración a la cuenta de administrador delegado actual.
5. Elija Siguiente.
6. En la página Revisar y aplicar, revise los detalles de la política de configuración. A continuación, seleccione Crear y aplicar política. Tanto en su región de origen como en las regiones vinculadas, esta acción anula los ajustes de configuración existentes de las cuentas asociadas a esta política de configuración. Las cuentas se pueden asociar a la política de configuración mediante una aplicación o la herencia de un nodo principal. Las cuentas secundarias y las unidades organizativas de los destinos aplicados heredarán automáticamente esta política de configuración, a menos que se excluyan específicamente, se autoadministren o utilicen una política de configuración diferente.

Security Hub CSPM API

Creación y asociación de políticas de configuración

1. Invoque la API CreateConfigurationPolicy desde la cuenta de administrador delegado del CSPM de Security Hub en la región de origen.
2. En `Name`, especifique un nombre para la política de configuración. Si lo desea, en el caso de `Description`, proporcione una descripción de la política de configuración.
3. En el campo `ServiceEnabled`, especifique si desea que el CSPM de Security Hub esté habilitado o desactivado en esta política de configuración.
4. En el campo `EnabledStandardIdentifiers`, especifique qué estándares del CSPM de Security Hub desea habilitar en esta política de configuración.
5. Para el objeto `SecurityControlsConfiguration`, especifique qué controles desea habilitar o deshabilitar en esta política de configuración. Elegir `EnabledSecurityControlIdentifiers` significa que los controles especificados están habilitados. Otros controles que forman parte de los estándares habilitados (como los controles recién lanzados) están deshabilitados. Elegir `DisabledSecurityControlIdentifiers` significa que los controles especificados están deshabilitados. Otros controles que forman parte de los estándares habilitados (como los controles recién lanzados) están habilitados.
6. Si lo desea, en el campo `SecurityControlCustomParameters`, especifique los controles habilitados para los que desee personalizar los parámetros. Indique `CUSTOM` en el campo `ValueType` y el valor del parámetro personalizado para el campo `Value`. El valor debe ser del tipo de datos correcto y estar dentro de los rangos válidos que especifique el CSPM de Security Hub. Solo algunos controles admiten valores de parámetros personalizados. Para obtener más información, consulte Comprensión de los parámetros de control en el CSPM de Security Hub.
7. Para aplicar la política de configuración a las cuentas o unidades organizativas, invoque la API StartConfigurationPolicyAssociation desde la cuenta de administrador delegado del CSPM de Security Hub en la región de origen.
8. En el campo `ConfigurationPolicyIdentifier`, indique el nombre de recurso de Amazon (ARN) o el identificador único universal (UUID) de la política. La API `CreateConfigurationPolicy` devuelve el ARN y el UUID. En una configuración autoadministrada, el campo `ConfigurationPolicyIdentifier` es igual a `SELF_MANAGED_SECURITY_HUB`.

9. En el campo `Target`, indique el ID de raíz, unidad organizativa, o cuenta donde desea que se aplique esta política de configuración. Solo puede proporcionar un objetivo en cada solicitud de API. Las cuentas secundarias y las unidades organizativas de los destinos aplicados heredarán automáticamente esta política de configuración, a menos que se autoadministren o utilicen una política de configuración diferente.

Ejemplo de solicitud de API para crear una política de configuración:

```
{
    "Name": "SampleConfigurationPolicy",
    "Description": "Configuration policy for production accounts",
    "ConfigurationPolicy": {
        "SecurityHub": {
             "ServiceEnabled": true,
             "EnabledStandardIdentifiers": [
                    "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0",
                    "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0"
                ],
            "SecurityControlsConfiguration": {
                "DisabledSecurityControlIdentifiers": [
                    "CloudTrail.2"
                ],
                "SecurityControlCustomParameters": [
                    {
                        "SecurityControlId": "ACM.1",
                        "Parameters": {
                            "daysToExpiration": {
                                "ValueType": "CUSTOM",
                                "Value": {
                                    "Integer": 15
                                }
                            }
                        }
                    }
                ]
            }
        }
    }
}
```

Ejemplo de solicitud de API para asociar una política de configuración:

```
{
    "ConfigurationPolicyIdentifier": "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Target": {"OrganizationalUnitId": "ou-examplerootid111-exampleouid111"}
}
```

AWS CLI

Creación y asociación de políticas de configuración

1. Ejecute el comando create-configuration-policy desde la cuenta de administrador delegado del CSPM de Security Hub en la región de origen.
2. En `name`, especifique un nombre para la política de configuración. Si lo desea, en el caso de `description`, proporcione una descripción de la política de configuración.
3. En el campo `ServiceEnabled`, especifique si desea que el CSPM de Security Hub esté habilitado o desactivado en esta política de configuración.
4. En el campo `EnabledStandardIdentifiers`, especifique qué estándares del CSPM de Security Hub desea habilitar en esta política de configuración.
5. En el campo `SecurityControlsConfiguration`, especifique qué controles desea habilitar o deshabilitar en esta política de configuración. Elegir `EnabledSecurityControlIdentifiers` significa que los controles especificados están habilitados. Otros controles que forman parte de los estándares habilitados (como los controles recién lanzados) están deshabilitados. Elegir `DisabledSecurityControlIdentifiers` significa que los controles especificados están deshabilitados. Se han habilitado otros controles que se aplican a los estándares habilitados (como los controles recién lanzados).
6. Si lo desea, en el campo `SecurityControlCustomParameters`, especifique los controles habilitados para los que desee personalizar los parámetros. Indique `CUSTOM` en el campo `ValueType` y el valor del parámetro personalizado para el campo `Value`. El valor debe ser del tipo de datos correcto y estar dentro de los rangos válidos que especifique el CSPM de Security Hub. Solo algunos controles admiten valores de parámetros personalizados. Para

obtener más información, consulte Comprensión de los parámetros de control en el CSPM de Security Hub.

7. Para aplicar la política de configuración a las cuentas o unidades organizativas, ejecute el comando start-configuration-policy-association desde la cuenta de administrador delegado del CSPM de Security Hub en la región de origen.
8. En el campo `configuration-policy-identifier`, indique el nombre de recurso de Amazon (ARN) o el ID de la política de configuración. El comando `create-configuration-policy` devuelve este ARN e ID.
9. En el campo `target`, indique el ID de raíz, unidad organizativa, o cuenta donde desea que se aplique esta política de configuración. Solo puede proporcionar un destino cada vez que ejecute el comando. Las entidades secundarias de los destinos seleccionados heredarán automáticamente esta política de configuración, a menos que se autoadministren o utilicen una política de configuración diferente.

Ejemplo de comando para crear una política de configuración:

```
aws securityhub --region us-east-1 create-configuration-policy \
--name "SampleConfigurationPolicy" \
--description "Configuration policy for production accounts" \
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,
 "EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-
foundational-security-best-practices/v/1.0.0","arn:aws:securityhub:::ruleset/
cis-aws-foundations-benchmark/v/1.2.0"],"SecurityControlsConfiguration":
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2"],
 "SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters":
 {"daysToExpiration": {"ValueType": "CUSTOM", "Value": {"Integer": 15}}}}]}}}'
```

Ejemplo de comando para asociar una política de configuración:

```
aws securityhub --region us-east-1 start-configuration-policy-association \
--configuration-policy-identifier "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
--target '{"OrganizationalUnitId": "ou-examplerootid111-exampleouid111"}'
```

La API `StartConfigurationPolicyAssociation` devuelve un campo llamado `AssociationStatus`. Este campo indica si la asociación de una política está pendiente o si su

estado es correcto o incorrecto. El estado puede tardar hasta 24 horas minutos en cambiar de `PENDING` a `SUCCESS` o `FAILURE`. Para obtener más información sobre el estado de una asociación, consulte Revisión del estado de asociación de una política de configuración.

Revisión del estado y los detalles de las políticas de configuración

El administrador de CSPM de AWS Security Hub delegado puede ver las políticas de configuración de una organización y sus detalles. Esto incluye las cuentas y unidades organizativas (OU) a las que está asociada una política.

Para obtener información general sobre las ventajas de la configuración centralizada y su funcionamiento, consulte Descripción de la configuración central en el CSPM de Security Hub.

Elija su método preferido y siga estos pasos para ver las políticas de configuración.

Security Hub CSPM console

Para ver políticas de configuración (consola)

1. Abra la consola CSPM de AWS Security Hub en. https://console.aws.amazon.com/securityhub/

   Inicie sesión con las credenciales de la cuenta de administrador delegado del CSPM de Security Hub en la región de origen.
2. En el panel de navegación, seleccione Configuración y Configuración.
3. Seleccione la pestaña Políticas para obtener un resumen de las políticas de configuración.
4. Seleccione una política de configuración y elija Ver detalles para ver información adicional al respecto, incluyendo las cuentas y OU a las que está asociada.

Security Hub CSPM API

Para ver una lista resumida de todas las políticas de configuración, utilice la operación ListConfigurationPolicies de la API del CSPM de Security Hub. Si usa elAWS CLI, ejecute el list-configuration-policiescomando. La cuenta de administrador delegado del CSPM de Security Hub debe invocar la operación en la región de origen.

```
$ aws securityhub list-configuration-policies \
--max-items 5 \
--starting-token U2FsdGVkX19nUI2zoh+Pou9YyutlYJHWpn9xnG4hqSOhvw3o2JqjI23QDxdf
```

Para ver los detalles sobre una política de configuración específica, utilice la operación GetConfigurationPolicy. Si usa elAWS CLI, ejecute el get-configuration-policy. La cuenta de administrador delegado debe invocar la operación en la región de origen. Proporcione el nombre de recurso de Amazon (ARN) o el ID de la política de configuración cuyos detalles desea ver.

```
$ aws securityhub get-configuration-policy \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Para ver una lista resumida de todas las políticas de configuración y sus respectivas asociaciones de cuentas, utilice la operación de configuración ListConfigurationPolicyAssociations. Si usa elAWS CLI, ejecute el list-configuration-policy-associationscomando. La cuenta de administrador delegado debe invocar la operación en la región de origen. Si lo desea, puede proporcionar parámetros de paginación o filtrar los resultados por un ID de política, un tipo de asociación o un estado de asociación específico.

```
$ aws securityhub list-configuration-policy-associations \
--filters '{"AssociationType": "APPLIED"}'
```

Para ver las asociaciones de una cuenta específica, utilice la operación GetConfigurationPolicyAssociation. Si usa elAWS CLI, ejecute el get-configuration-policy-associationcomando. La cuenta de administrador delegado debe invocar la operación en la región de origen. En `target`, indique el número de cuenta, el ID de unidad organizativa o el ID de raíz.

```
$ aws securityhub get-configuration-policy-association \
--target '{"AccountId": "123456789012"}'
```

Revisión del estado de asociación de una política de configuración

Las siguientes operaciones de la API de configuración centralizada devuelven un campo denominado `AssociationStatus`:

- `BatchGetConfigurationPolicyAssociations`
- `GetConfigurationPolicyAssociation`
- `ListConfigurationPolicyAssociations`
- `StartConfigurationPolicyAssociation`

Este campo se devuelve cuando la configuración subyacente es una política de configuración y cuando se trata de un comportamiento autoadministrado.

El valor de `AssociationStatus` indica si una asociación de política está pendiente o si se encuentra en un estado de éxito o de error para una cuenta específica. El estado puede tardar hasta 24 horas minutos en cambiar de `PENDING` a `SUCCESS` o `FAILED`. Un estado de `SUCCESS` significa que todos los ajustes especificados en la política de configuración están asociados a la cuenta. Un estado de `FAILED` significa que uno o más ajustes especificados en la política de configuración no se asociaron a la cuenta. A pesar de un estado `FAILED`, la cuenta podría estar configurada parcialmente conforme a la política. Por ejemplo, puede intentar asociar una cuenta a una política de configuración que habilite el CSPM de Security Hub, habilite las prácticas recomendadas de seguridad AWS fundamentales y lo deshabilite. CloudTrail.1 Las dos configuraciones iniciales podrían funcionar correctamente, pero la configuración podría fallar CloudTrail.1. En este ejemplo, el estado de la asociación es `FAILED`, incluso cuando algunos ajustes se configuraron correctamente.

El estado de asociación de una unidad organizativa principal o de la raíz depende del estado de sus entidades secundarias. Si el estado de asociación de todas las entidades secundarias es `SUCCESS`, el estado de asociación de la entidad principal es `SUCCESS`. Si el estado de asociación de una o más entidades secundarias es `FAILED`, el estado de asociación de la entidad principal es `FAILED`.

El valor de `AssociationStatus` depende del estado de asociación de la política en todas las regiones pertinentes. Si la asociación tiene éxito en la región de origen y en todas las regiones vinculadas, el valor de `AssociationStatus` es `SUCCESS`. Si se produce un error en la asociación en una o más de estas regiones, el valor de `AssociationStatus` es `FAILED`.

El siguiente comportamiento también afecta al valor de `AssociationStatus`:

- Si el destino es una unidad organizativa principal o de la raíz, tiene un `AssociationStatus` de `SUCCESS` o `FAILED` solo cuando todas las entidades secundarias tienen un estado `SUCCESS` o `FAILED`. Si el estado de asociación de una cuenta o unidad organizativa secundaria cambia (por ejemplo, cuando se agrega o elimina una región vinculada) después de asociar por primera vez la entidad principal a una configuración, el cambio no actualiza el estado de asociación de la entidad principal a menos que vuelva a invocar la API `StartConfigurationPolicyAssociation`.
- Si el destino es una cuenta, tiene un `AssociationStatus` de `SUCCESS` o `FAILED` solo si la asociación tiene un resultado de `SUCCESS` o `FAILED` en la región de origen y en todas las regiones vinculadas. Si el estado de asociación de una cuenta de destino cambia (por ejemplo, cuando se agrega o elimina una región vinculada) después de asociarla por primera vez a una configuración, su estado de asociación se actualiza. Sin embargo, el cambio no

actualiza el estado de asociación de la entidad principal a menos que vuelva a invocar la API `StartConfigurationPolicyAssociation`.

Si agrega una región vinculada nueva, el CSPM de Security Hub replica las asociaciones existentes que se encuentran en un estado `PENDING`, `SUCCESS` o `FAILED` en la nueva región.

Incluso cuando el estado de la asociación es `SUCCESS`, el estado de habilitación de un estándar incluido en la política puede pasar a un estado incompleto. En ese caso, el CSPM de Security Hub no puede generar resultados para los controles del estándar. Para obtener más información, consulte Verificación del estado de un estándar.

Solución de problemas de la asociación

En AWS Security Hub CSPM, la asociación de una política de configuración puede fallar por los siguientes motivos habituales.

- La cuenta de administración de Organizations no es miembro: si desea asociar una política de configuración a la cuenta de administración de Organizations, esa cuenta ya debe tener activado AWS Security Hub CSPM. Esto convierte a la cuenta de administración en una cuenta de miembro de la organización.
- AWS Configno está habilitada o configurada correctamente: para habilitar los estándares en una política de configuración, AWS Config debe estar habilitada y configurada para registrar los recursos relevantes.
- Debe asociarse desde una cuenta de administrador delegado: solo puede asociar una política a las cuentas y UO de destino si ha iniciado sesión en la cuenta de administrador delegado del CSPM de Security Hub.
- Debe asociarse desde la región de origen: solo puede asociar una política a las cuentas y OU de destino si ha iniciado sesión en su región de origen.
- Opt-in Región no habilitada: la asociación de políticas no se puede realizar en el caso de una cuenta miembro o unidad organizativa de una región vinculada si se trata de una región opcional que el administrador delegado no ha habilitado. Puede volver a intentarlo después de habilitar la región desde la cuenta de administrador delegado.
- Cuenta de miembro suspendida: la asociación de políticas es muestra error si se intenta asociar una política a una cuenta de miembro suspendida.

Actualización de las políticas de configuración

Tras crear una política de configuración, la cuenta de administrador CSPM AWS de Security Hub delegada puede actualizar los detalles de la política y las asociaciones de políticas. Cuando se actualizan los detalles de la política, las cuentas asociadas a la política de configuración comienzan a utilizar de manera automática la política actualizada.

Para obtener información general sobre las ventajas de la configuración centralizada y su funcionamiento, consulte Descripción de la configuración central en el CSPM de Security Hub.

> **Note**
>
> Las políticas de configuración solo admiten AWS estándares y controles. No puede incluir estándares multinube (como CIS Azure Foundations Benchmark v4.0.0) ni controles de Azure en una política de configuración. Se incluye un ARN estándar multinube o un identificador de control. `InvalidInputException` Para habilitar o configurar los estándares multinube, utilice los mecanismos de configuración local directamente en el lugar deseado. Cuenta de AWS

El administrador delegado puede actualizar los siguientes ajustes de la política:

- Habilite o desactive el CSPM de Security Hub.
- Habilite uno o más estándares de seguridad.
- Indique qué controles de seguridad están habilitados en todos los estándares habilitados. Para ello, proporcione una lista de controles específicos que deberían estar habilitados y el CSPM de Security Hub desactivará todos los demás controles, lo que incluye los controles nuevos cuando se lanzan. De forma alternativa, proporcione una lista de controles específicos que deberían estar desactivados y el CSPM de Security Hub habilitará todos los demás controles, incluidos los controles nuevos cuando se lanzan.
- Si lo desea, personalice parámetros de ciertos controles habilitados en los estándares habilitados.

Elija su método preferido y siga estos pasos para actualizar una política de configuración.

> **Note**
>
> Si usa la configuración centralizada, el CSPM de Security Hub desactiva automáticamente los controles que implican recursos globales en todas las regiones, excepto en la región

de origen. Los controles que elija habilitar a través de una política de configuración están habilitados en todas las regiones en las que están disponibles. Para limitar los resultados de estos controles a una sola región, puede actualizar la configuración de la AWS Config grabadora y desactivar el registro de recursos globales en todas las regiones, excepto en la región de origen.
Si un control habilitado que implica recursos globales no es compatible en la región de origen, el CSPM de Security Hub intenta habilitarlo en una región vinculada donde sí se admita. Con la configuración centralizada, no se obtiene cobertura para un control que no está disponible ni en la región de origen ni en ninguna de las regiones vinculadas.
Para obtener una lista de los controles que implican recursos globales, consulte Controles que utilizan recursos globales.

Console

Actualización de las políticas de configuración

1. Abra la consola CSPM de AWS Security Hub en. https://console.aws.amazon.com/securityhub/

   Inicie sesión con las credenciales de la cuenta de administrador delegado del CSPM de Security Hub en la región de origen.
2. En el panel de navegación, seleccione Configuración y Configuración.
3. Elija la pestaña Policies.
4. Seleccione la política de configuración que desea modificar y elija Editar. Si lo desea, edite la configuración de la política. Deje esta sección como está si desea mantener la configuración de la política sin cambios.
5. Seleccione Siguiente. Si lo desea, edite las asociaciones de políticas. Deje esta sección como está si desea mantener las asociaciones de políticas sin cambios. Puede asociar o desasociar la política a un máximo de 15 destinos (cuentas, unidades organizativas o raíz) cuando la actualiza.
6. Elija Siguiente.
7. Revise los cambios y seleccione Guardar y aplicar. Tanto en su región de origen como en las regiones vinculadas, esta acción anula los ajustes de configuración existentes de las cuentas asociadas a esta política de configuración. Las cuentas se pueden asociar a una política de configuración mediante una aplicación o la herencia de un nodo principal.

API

Actualización de las políticas de configuración

1. Para actualizar los ajustes de una política de configuración, invoque la API UpdateConfigurationPolicy desde la cuenta de administrador delegado del CSPM de Security Hub en la región de origen.
2. Proporcione el nombre de recurso de Amazon (ARN) o el ID de la política de configuración que desea actualizar.
3. Proporcione valores actualizados para los campos de `ConfigurationPolicy`. También tiene la opción de indicar el motivo de la actualización.
4. Para agregar asociaciones nuevas para esta política de configuración, invoque la API StartConfigurationPolicyAssociation desde la cuenta de administrador delegado del CSPM de Security Hub en la región de origen. Para eliminar una o más asociaciones actuales, invoque la API StartConfigurationPolicyDisassociation desde la cuenta de administrador delegado del CSPM de Security Hub en la región de origen.
5. En el campo `ConfigurationPolicyIdentifier`, indique el ARN o el ID de la política de configuración cuyas asociaciones desee actualizar.
6. En el campo `Target`, indique las cuentas, las unidades organizativas o el ID de raíz que desee asociar o desasociar. Esta acción anula las asociaciones de políticas anteriores para las unidades organizativas o cuentas especificadas.

> **Note**
>
> Al invocar la API `UpdateConfigurationPolicy`, el CSPM de Security Hub sustituye por completo la lista de los campos `EnabledStandardIdentifiers`, `EnabledSecurityControlIdentifiers`, `DisabledSecurityControlIdentifiers` y `SecurityControlCustomParameters`. Cada vez que invoque esta API, proporcione la lista completa de estándares que desee habilitar y la lista completa de controles que desee habilitar o deshabilitar y para los que desee personalizar los parámetros.

Ejemplo de solicitud de API para actualizar una política de configuración:

```
{
```

```
    "Identifier": "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Description": "Updated configuration policy",
    "UpdatedReason": "Disabling CloudWatch.1",
    "ConfigurationPolicy": {
        "SecurityHub": {
             "ServiceEnabled": true,
             "EnabledStandardIdentifiers": [
                    "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0",
                    "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0"
                ],
            "SecurityControlsConfiguration": {
                "DisabledSecurityControlIdentifiers": [
                    "CloudTrail.2",
                    "CloudWatch.1"
                ],
                "SecurityControlCustomParameters": [
                    {
                        "SecurityControlId": "ACM.1",
                        "Parameters": {
                            "daysToExpiration": {
                                "ValueType": "CUSTOM",
                                "Value": {
                                    "Integer": 15
                                }
                            }
                        }
                    }
                ]
            }
        }
    }
}
```

AWS CLI

Actualización de las políticas de configuración

1. Para actualizar los ajustes de una política de configuración, ejecute el comando update-configuration-policy desde la cuenta de administrador delegado del CSPM de Security Hub en la región de origen.
2. Proporcione el nombre de recurso de Amazon (ARN) o el ID de la política de configuración que desea actualizar.
3. Proporcione valores actualizados para los campos de `configuration-policy`. También tiene la opción de indicar el motivo de la actualización.
4. Para agregar nuevas asociaciones para esta política de configuración, ejecute el comando start-configuration-policy-association desde la cuenta de administrador delegado del CSPM de Security Hub en la región de origen. Para eliminar una o más asociaciones actuales, ejecute el comando start-configuration-policy-disassociation desde la cuenta de administrador delegado del CSPM de Security Hub en la región de origen.
5. En el campo `configuration-policy-identifier`, indique el ARN o el ID de la política de configuración cuyas asociaciones desee actualizar.
6. En el campo `target`, indique las cuentas, las unidades organizativas o el ID de raíz que desee asociar o desasociar. Esta acción anula las asociaciones de políticas anteriores para las unidades organizativas o cuentas especificadas.

> **Note**
>
> Al ejecutar el comando `update-configuration-policy`, el CSPM de Security Hub sustituye por completo la lista de los campos `EnabledStandardIdentifiers`, `EnabledSecurityControlIdentifiers`, `DisabledSecurityControlIdentifiers` y `SecurityControlCustomParameters`. Cada vez que ejecute este comando, proporcione la lista completa de estándares que desee habilitar y la lista completa de controles que desee habilitar o deshabilitar y para los que desee personalizar los parámetros.

Ejemplo de comando para actualizar una política de configuración:

```
aws securityhub update-configuration-policy \
--region us-east-1 \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
--description "Updated configuration policy" \
--updated-reason "Disabling CloudWatch.1" \
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,
 "EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-
foundational-security-best-practices/v/1.0.0","arn:aws:securityhub:::ruleset/
cis-aws-foundations-benchmark/v/1.2.0"],"SecurityControlsConfiguration":
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2","CloudWatch.1"],
 "SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters":
 {"daysToExpiration": {"ValueType": "CUSTOM", "Value": {"Integer": 15}}}}]}}}'
```

La API `StartConfigurationPolicyAssociation` devuelve un campo llamado `AssociationStatus`. Este campo indica si la asociación de una política está pendiente o si su estado es correcto o incorrecto. El estado puede tardar hasta 24 horas minutos en cambiar de `PENDING` a `SUCCESS` o `FAILURE`. Para obtener más información sobre el estado de una asociación, consulte Revisión del estado de asociación de una política de configuración.

Eliminación de políticas de configuración

Tras crear una política de configuración, el administrador CSPM AWS de Security Hub delegado puede eliminarla. Como alternativa, el administrador delegado puede retener la política, pero desasociarla de cuentas o de unidades organizativas (OU) específicas, o de la raíz. Para obtener instrucciones sobre cómo desasociar una política, consulte Desasociación de una configuración de sus objetivos.

Para obtener información general sobre las ventajas de la configuración centralizada y su funcionamiento, consulte Descripción de la configuración central en el CSPM de Security Hub.

En esta sección se explica cómo eliminar políticas de configuración.

Al eliminar una política de configuración, esta deja de existir en su organización. Las cuentas de destino, las unidades organizativas y la raíz de la organización ya no pueden utilizar la política de configuración. Los destinos que estaban asociados a una política de configuración eliminada heredan la política de configuración de la entidad principal más próxima o se vuelven autoadministrados si la entidad principal más próxima se autoadministra. Si desea que un destino

utilice una configuración diferente, puede asociar el destino a una nueva política de configuración. Para obtener más información, consulte Creación y asociación de políticas de configuración.

Se recomienda crear y asociar al menos una política de configuración a su organización para proporcionar una cobertura de seguridad adecuada.

Antes de eliminar una política de configuración, debe desasociarla de cualquier cuenta, unidad organizativa o raíz a la que se aplique en la actualidad.

Elija su método preferido y siga estos pasos para eliminar una política de configuración.

Console

Eliminación de una política de configuración

1. Abra la consola CSPM de AWS Security Hub en. https://console.aws.amazon.com/securityhub/

   Inicie sesión con las credenciales de la cuenta de administrador delegado del CSPM de Security Hub en la región de origen.
2. En el panel de navegación, seleccione Configuración y Configuración.
3. Elija la pestaña Policies. Seleccione la política de configuración que desea eliminar y, a continuación, elija Eliminar. Si la política de configuración sigue asociada a alguna cuenta o unidad organizativa, se le solicitará que desasocie antes la política de esos destinos antes de poder eliminarla.
4. Revise el mensaje de confirmación. Ingrese **`confirm`** y elija Eliminar.

API

Eliminación de una política de configuración

Invoque la API DeleteConfigurationPolicy desde la cuenta de administrador delegado del CSPM de Security Hub en la región de origen.

Proporcione el nombre de recurso de Amazon (ARN) o el ID de la política de configuración que desea eliminar. Si recibe un error `ConflictException`, la política de configuración seguirá aplicándose a las cuentas o unidades organizativas de su organización. Para resolver el error, desasocie la política de configuración de estas cuentas o unidades organizativas antes de intentar eliminarla.

Ejemplo de solicitud de API para eliminar una política de configuración:

```
{
    "Identifier": "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
}
```

AWS CLI

Eliminación de una política de configuración

Ejecute el comando delete-configuration-policy desde la cuenta de administrador delegado del CSPM de Security Hub en la región de origen.

Proporcione el nombre de recurso de Amazon (ARN) o el ID de la política de configuración que desea eliminar. Si recibe un error `ConflictException`, la política de configuración seguirá aplicándose a las cuentas o unidades organizativas de su organización. Para resolver el error, desasocie la política de configuración de estas cuentas o unidades organizativas antes de intentar eliminarla.

```
aws securityhub --region us-east-1 delete-configuration-policy \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Desasociación de una configuración de sus objetivos

Desde la cuenta de administrador CSPM de AWS Security Hub delegada, puede desasociar una política de configuración o una configuración autogestionada de una cuenta, unidad organizativa o raíz. La desasociación conserva la política para su uso en el futuro, pero elimina las asociaciones existentes de cuentas, unidades organizativas o raíz específicas. Solo puede desasociar una configuración aplicada directamente, no una configuración heredada. Para cambiar una configuración heredada, puede aplicar una política de configuración o un comportamiento autoadministrado a la cuenta o unidad organizativa afectada. También puede aplicar una nueva política de configuración, que incluya las modificaciones que desee, a la entidad principal más próxima.

La desasociación no elimina una política de configuración. La política se retiene en su cuenta, por lo que puede asociarla a otros destinos de su organización. Para obtener instrucciones sobre

cómo eliminar una política de configuración, consulte Eliminación de políticas de configuración. Cuando se completa la desasociación, el destino afectado hereda la política de configuración o el comportamiento autoadministrado de la entidad principal más próxima. Si no hay una configuración heredable, el destino conserva la configuración que tenía antes de la desasociación, pero pasa a ser autoadministrado.

Elija el método que prefiera y siga los pasos para desasociar una cuenta, unidad organizativa o raíz de su configuración actual.

Console

Desasociación de una cuenta o unidad organizativa de su configuración actual

1. Abra la consola CSPM de AWS Security Hub en. https://console.aws.amazon.com/securityhub/

   Inicie sesión con las credenciales de la cuenta de administrador delegado del CSPM de Security Hub en la región de origen.
2. En el panel de navegación, seleccione Configuración y Configuración.
3. En la pestaña Organizaciones, seleccione la cuenta, unidad organizativa o la raíz que desee desasociar de su configuración actual. Elija Edit (Edición de).
4. En la página Definir configuración, en Administración, elija Política aplicada si desea que el administrador delegado tenga autorización para aplicar las políticas directamente al destino. Elija Heredada si desea que el destino herede la configuración de su entidad principal más próxima. En cualquiera de estos casos, el administrador delegado controla la configuración del destino. Elija Self-managedsi desea que la cuenta o la unidad organizativa controlen sus propios ajustes.
5. Tras revisar los cambios, seleccione Siguiente y Aplicar. Si las configuraciones entran en conflicto con las selecciones actuales, esta acción anula las configuraciones existentes de cualquier cuenta o unidad organizativa que esté dentro del ámbito de aplicación.

API

Desasociación de una cuenta o unidad organizativa de su configuración actual

1. Invoque la API StartConfigurationPolicyDisassociation desde la cuenta de administrador delegado del CSPM de Security Hub en la región de origen.

2. En `ConfigurationPolicyIdentifier`, indique el nombre de recurso de Amazon (ARN) o el ID de la política de configuración que desee desasociar. Indique `SELF_MANAGED_SECURITY_HUB` en este campo para desasociar el comportamiento autoadministrado.
3. En `Target`, indique las cuentas, las unidades organizativas o la raíz que desee desasociar de esta política de configuración.

Ejemplo de solicitud de API para desasociar una política de configuración:

```
{
    "ConfigurationPolicyIdentifier": "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Target": {"RootId": "r-f6g7h8i9j0example"}
}
```

AWS CLI

Desasociación de una cuenta o unidad organizativa de su configuración actual

1. Ejecute el comando start-configuration-policy-disassociation desde la cuenta de administrador delegado del CSPM de Security Hub en la región de origen.
2. En `configuration-policy-identifier`, indique el nombre de recurso de Amazon (ARN) o el ID de la política de configuración que desee desasociar. Indique `SELF_MANAGED_SECURITY_HUB` en este campo para desasociar el comportamiento autoadministrado.
3. En `target`, indique las cuentas, las unidades organizativas o la raíz que desee desasociar de esta política de configuración.

Ejemplo de comando para desasociar una política de configuración:

```
aws securityhub --region us-east-1 start-configuration-policy-disassociation \
--configuration-policy-identifier "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
--target '{"RootId": "r-f6g7h8i9j0example"}'
```

Cómo configurar un estándar o un control en contexto

Cuando se utiliza la configuración central en AWS Security Hub CSPM, el administrador delegado del Security Hub CSPM puede crear políticas de configuración que especifiquen cómo se configuran el CSPM de Security Hub, los estándares de seguridad y los controles de seguridad para una organización. El administrador delegado puede asociar políticas a cuentas y unidades organizativas (UO) específicas. Las políticas entran en vigor en la región de origen y en todas las regiones vinculadas. El administrador delegado puede actualizar políticas según sea necesario.

En la consola del CSPM de Security Hub, el administrador delegado puede actualizar las políticas de configuración de dos maneras: desde la página de Configuración o dentro del contexto de los flujos de trabajo existentes. Esto último puede resultar útil porque, al revisar los resultados de seguridad, es posible identificar qué estándares y controles son más relevantes para su entorno y configurarlos al mismo tiempo.

In-context la configuración solo está disponible en la consola CSPM de Security Hub. Mediante programación, el administrador delegado debe invocar la operación UpdateConfigurationPolicy de la API del CSPM de Security Hub para cambiar la forma en que se configuran estándares o controles específicos en la organización.

Siga estos pasos para configurar un estándar o un control del CSPM de Security Hub en contexto.

Para configurar un estándar o un control en contexto (consola)

1. Abra la consola CSPM de AWS Security Hub en. https://console.aws.amazon.com/securityhub/

   Inicie sesión con las credenciales de la cuenta de administrador delegado del CSPM de Security Hub en la región de origen.
2. En el panel de navegación, elija una de las siguientes opciones:

   - Para configurar un estándar, seleccione Estándares de seguridad y elija un estándar específico.
   - Para configurar un control, seleccione Controles y elija un control específico.
3. La consola muestra las políticas de configuración del CSPM de Security Hub existentes y el estado del estándar o control seleccionado en cada una. Elija las opciones para habilitar o desactivar el estándar o el control en cada política de configuración existente. En el caso de los controles, también puede optar por personalizar los parámetros del control. No puede crear una política nueva durante la configuración en contexto. Para crear una nueva política, debe ir a la página Configuración, elegir la pestaña Políticas y, a continuación, elegir Crear política.

4. Cuando termine de aplicar los cambios, seleccione Siguiente.
5. Revise los cambios y elija Aplicar. Las actualizaciones afectan todas las cuentas y unidades organizativas asociadas a la política de configuración modificada. Las actualizaciones también tienen efecto en la región de origen y en todas las regiones vinculadas.

Desactivación de la configuración centralizada en el CSPM de Security Hub

Al deshabilitar la configuración central en AWS Security Hub CSPM, el administrador delegado pierde la capacidad de configurar Security Hub CSPM, los estándares de seguridad y los controles de seguridad en varias unidades organizativas (Cuentas de AWSOU) y. Regiones de AWS En su lugar, debe configurar la mayoría de los ajustes por separado para cada cuenta en cada región.

> **Important**
>
> Antes de deshabilitar la configuración centralizada, debe desasociar las cuentas y las unidades organizativas de su configuración actual, independientemente de si se trata de una política de configuración o de un comportamiento autoadministrado.
> Antes de poder deshabilitar la configuración centralizada, también debe eliminar las políticas de configuración existentes.

Al deshabilitar la configuración centralizada, se producen los siguientes cambios:

- El administrador delegado ya no puede crear políticas de configuración para la organización.
- Las cuentas que tenían una política de configuración aplicada o heredada retienen su configuración actual, pero se vuelven autoadministradas.
- Su organización cambia a la configuración local. Al utilizar el enfoque de configuración local, la mayoría de los ajustes del CSPM de Security Hub se deben configurar por separado para cada cuenta y región de la organización. El administrador delegado puede optar por habilitar automáticamente el CSPM de Security Hub, los estándares de seguridad predeterminados y todos los controles que forman parte de los estándares predeterminados en las nuevas cuentas de la organización. Los estándares predeterminados son AWS Foundational Security Best Practices (FSBP) y Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0. Esta configuración entra en vigor en la región actual y afecta únicamente a las cuentas nuevas de la organización. El administrador delegado no puede cambiar los estándares predeterminados. La configuración local no admite el uso de políticas de configuración ni la configuración a nivel de la unidad organizativa.

La identidad de la cuenta de administrador delegado sigue siendo la misma cuando se deja de utilizar la configuración centralizada. Su región de origen y las regiones vinculadas también siguen siendo las mismas (su región de origen ahora se denomina región de agregación y se puede utilizar para la agregación de resultados).

Elija el método que prefiera y siga los pasos para dejar de utilizar la configuración centralizada y cambiar a la configuración local.

Security Hub CSPM console

Para deshabilitar la configuración centralizada (consola)

1. Abra la consola CSPM de AWS Security Hub en. https://console.aws.amazon.com/securityhub/

   Inicie sesión con las credenciales de la cuenta de administrador delegado del CSPM de Security Hub en la región de origen.
2. En el panel de navegación, seleccione Configuración y Configuración.
3. En la sección Información general, seleccione Editar.
4. En el cuadro Editar configuración de la organización, seleccione Configuración local. Si aún no lo ha hecho, se le solicitará que desasocie y elimine las políticas de configuración actuales antes de poder dejar de utilizar la configuración centralizada. Las cuentas o unidades organizativas que se designan como autoadministradas deben desasociarse de su configuración autoadministrada. Para ello, en la consola puede cambiar el tipo de administración de cada cuenta u unidad organizativa autoadministrada a Administrada de forma centralizada y Heredar de mi organización.
5. Si lo desea, seleccione los ajustes predeterminados de la configuración local para las nuevas cuentas de la organización.
6. Elija Confirmar.

Security Hub CSPM API

Para deshabilitar la configuración centralizada (API)

1. Invoque la API UpdateOrganizationConfiguration.
2. Establezca el campo `ConfigurationType` del objeto `OrganizationConfiguration` en `LOCAL`. La API devuelve un error si tiene políticas de configuración o asociaciones

de políticas existentes. Para desasociar una política de configuración, invoque la API `StartConfigurationPolicyDisassociation`. Para eliminar una política de configuración, invoque la API `DeleteConfigurationPolicy`.

3. Si quiere habilitar automáticamente el CSPM de Security Hub en las nuevas cuentas de la organización, establezca el campo `AutoEnable` en `true`. De forma predeterminada, el valor de este campo es `false` y el CSPM de Security Hub no se habilita automáticamente en las nuevas cuentas de la organización. De forma opcional, si quiere habilitar automáticamente Security Hub en las nuevas cuentas de la organización, establezca el campo `AutoEnableStandards` en `DEFAULT`. Este es el valor predeterminado. Si no quiere habilitar automáticamente los estándares de seguridad predeterminados en las nuevas cuentas de la organización, establezca el campo `AutoEnableStandards` en `NONE`.

Ejemplo de solicitud de API:

```
{
    "AutoEnable": true,
    "OrganizationConfiguration": {
        "ConfigurationType" : "LOCAL"
    }
}
```

AWS CLI

Para deshabilitar la configuración central (AWS CLI)

1. Ejecute el comando update-organization-configuration.
2. Establezca el campo `ConfigurationType` del objeto `organization-configuration` en `LOCAL`. El comando devuelve un error si tiene políticas de configuración o asociaciones de políticas existentes. Para desasociar una política de configuración, ejecute el comando `start-configuration-policy-disassociation`. Para eliminar una política de configuración, ejecute el comando `delete-configuration-policy`.
3. Si quiere habilitar automáticamente el CSPM de Security Hub en las nuevas cuentas de la organización, incluya el parámetro `auto-enable`. De forma predeterminada, el valor de este parámetro es `no-auto-enable` y el CSPM de Security Hub no se habilita automáticamente en las nuevas cuentas de la organización. De forma opcional, si quiere habilitar automáticamente Security Hub en las nuevas cuentas de la organización, establezca

el campo `auto-enable-standards` en `DEFAULT`. Este es el valor predeterminado. Si no quiere habilitar automáticamente los estándares de seguridad predeterminados en las nuevas cuentas de la organización, establezca el campo `auto-enable-standards` en `NONE`.

```
aws securityhub --region us-east-1 update-organization-configuration \
--auto-enable \
--organization-configuration '{"ConfigurationType": "LOCAL"}'
```

Administración de cuentas de administrador y de miembro en el CSPM de Security Hub

Si su AWS entorno tiene varias cuentas, puede tratar las cuentas que utilizan AWS Security Hub CSPM como cuentas de miembro y asociarlas a una sola cuenta de administrador. El administrador puede supervisar el estado general de seguridad y tomar medidas permitidas en las cuentas de miembro. El administrador también puede realizar diversas tareas de gestión y administración de cuentas a gran escala, como supervisar los costos de uso estimados y evaluar las cuotas de las cuentas.

Puede asociar las cuentas de los miembros a un administrador de dos maneras: integrando Security Hub CSPM AWS Organizations o enviando y aceptando manualmente las invitaciones de membresía en Security Hub CSPM.

Administrar cuentas conAWS Organizations

AWS Organizationses un servicio de administración de cuentas global que permite a AWS los administradores consolidar y administrar múltiples cuentas. Cuentas de AWS Proporciona características de facturación unificada y administración de cuentas que están diseñadas para satisfacer las necesidades de presupuestos, seguridad y conformidad. Se ofrece sin costo adicional y se integra con variosServicios de AWS, incluidos AWS Security Hub CSPM, Amazon Macie y Amazon. GuardDuty Para obtener más información, consulte la Guía del usuario de AWS Organizations.

Al integrar Security Hub CSPM yAWS Organizations, la cuenta de administración de Organizations designa a un administrador delegado de Security Hub CSPM. El CSPM de Security Hub se habilita automáticamente en la cuenta de administrador delegado Región de AWS en la que se designó.

Tras designar un administrador delegado, recomendamos administrar las cuentas en el CSPM de Security Hub con una configuración centralizada. Esta es la manera más eficaz de personalizar el CSPM de Security Hub y garantizar una cobertura de seguridad adecuada en la organización.

La configuración central permite al administrador delegado personalizar el CSPM de Security Hub en varias cuentas y regiones de la organización en lugar de configurarlo. Region-by-Region Puede crear una política de configuración para toda la organización o diferentes políticas de configuración para las distintas cuentas y unidades organizativas. Las políticas especifican si el CSPM de Security Hub está habilitado o desactivado en las cuentas asociadas, así como los estándares y controles de seguridad que se deben habilitar.

El administrador delegado puede designar las cuentas como administradas de manera centralizada o autoadministradas. Las cuentas administradas centralmente solo las puede configurar el administrador delegado. Self-managed las cuentas pueden especificar su propia configuración.

Si no utiliza la configuración centralizada, el administrador delegado dispone de capacidades más limitadas para configurar el CSPM de Security Hub; a este enfoque se le denomina configuración local. En la configuración local, el administrador delegado puede habilitar automáticamente el CSPM de Security Hub y los estándares de seguridad predeterminados en las nuevas cuentas de la organización dentro de la región actual. Sin embargo, las cuentas existentes no utilizan esta configuración, por lo que se pueden producir cambios en la configuración después de que una cuenta se una a la organización.

Además de estos nuevos ajustes de cuenta, la configuración local es específica de la cuenta y. Region-specific Cada cuenta de la organización debe configurar el servicio, los estándares y los controles del CSPM de Security Hub por separado en cada región. La configuración local tampoco admite el uso de políticas de configuración.

Administración manual de cuentas mediante invitación

Si tiene una cuenta independiente, debe administrar manualmente las cuentas de miembro mediante invitación en el CSPM de Security Hub o si no ha integrado con Organizations. Una cuenta independiente no se puede integrar con Organizations, por lo que es necesario administrarla manualmente. Recomendamos la integración AWS Organizations y el uso de la configuración central si agrega cuentas adicionales en el futuro.

Cuando utiliza la administración manual de cuentas, designa una cuenta como administradora del CSPM de Security Hub. La cuenta de administrador puede ver los datos de las cuentas de miembro y tomar determinadas medidas en función de los resultados de las cuentas de miembro. El

administrador del CSPM de Security Hub invita a otras cuentas para que sean cuentas de miembro. La relación administrador-miembro se establece cuando una potencial cuenta de miembro acepta la invitación.

La administración manual de cuentas no admite el uso de políticas de configuración. Sin políticas de configuración, el administrador no puede personalizar el CSPM de Security Hub de forma centralizada mediante el ajuste de parámetros distintos para diferentes cuentas. En su lugar, cada cuenta de la organización debe habilitar y configurar el CSPM de Security Hub por separado en cada región. Esto puede hacer que garantizar una cobertura de seguridad adecuada en todas las cuentas y regiones donde utilice el CSPM de Security Hub sea un proceso más lento y complejo. También puede provocar cambios en la configuración, ya que las cuentas de miembro pueden especificar su propia configuración sin la intervención del administrador.

Para administrar las cuentas mediante invitación, consulte Administración de cuentas por invitación en el CSPM de Security Hub.

Recomendaciones para la administración de múltiples cuentas en el CSPM de Security Hub

En la siguiente sección se resumen algunas restricciones y recomendaciones que se deben tener en cuenta al administrar las cuentas de los miembros en AWS Security Hub CSPM.

Número máximo de cuentas miembro

Si utiliza la integración conAWS Organizations, Security Hub CSPM admite hasta 10 000 cuentas de miembros por cuenta de administrador delegado en cada una de ellas. Región de AWS Si habilita y administra el CSPM de Security Hub de manera manual, el CSPM de Security Hub admite hasta 1000 invitaciones a cuentas de miembro por cuenta de administrador en cada región.

Creación de relaciones administrador-miembro

> **Note**
>
> Si utilizas la integración CSPM de Security Hub con AWS Organizations una cuenta de miembro y no has invitado manualmente a ninguna cuenta de miembro, esta sección no se aplica a ti.

Una cuenta no puede ser cuenta de administrador y cuenta de miembro al mismo tiempo.

Una cuenta miembro solo se puede asociar con una cuenta de administrador. Si una cuenta de la organización está habilitada por la cuenta de administrador del CSPM de Security Hub, esa cuenta no puede aceptar una invitación de otra cuenta. Si una cuenta ya aceptó una invitación, no puede ser habilitada por la cuenta de administrador del CSPM de Security Hub para la organización. Tampoco puede recibir invitaciones de otras cuentas.

En el caso del proceso de invitación manual, aceptar una invitación para convertirse en miembro es opcional.

Membresía medianteAWS Organizations

Si integra Security Hub CSPM conAWS Organizations, la cuenta de administración de la organización puede designar una cuenta de administrador delegado (DA) para Security Hub CSPM. En Organizations, la cuenta de administración de la organización no se puede configurar como el administrador delegado. Aunque esto está permitido en el CSPM de Security Hub, recomendamos que la cuenta de administración de Organizations no sea el administrador delegado.

Le recomendamos que seleccione la misma cuenta de administrador delegado en todas las regiones. Si utiliza la configuración centralizada, el CSPM de Security Hub establece la misma cuenta de administrador delegado en todas las regiones en las que configure el CSPM de Security Hub para la organización.

También le recomendamos que elija la misma cuenta DA en todos los servicios de AWS seguridad y cumplimiento para ayudarle a gestionar los problemas relacionados con la seguridad desde un único panel de control.

Membresía por invitación

En el caso de las cuentas miembro creadas mediante invitación, la asociación de cuentas administrador-miembro se crea únicamente en la región desde la que se envía la invitación. La cuenta de administrador debe habilitar el CSPM de Security Hub en cada región en la que desee utilizarlo. A continuación, la cuenta de administrador invita a cada cuenta a convertirse en cuenta de miembro en esa región.

> **Note**
>
> Recomendamos utilizar, AWS Organizations en lugar de Security Hub, invitaciones CSPM para gestionar las cuentas de los miembros.

Coordinar cuentas de administrador en todos los servicios

Security Hub CSPM agrega los hallazgos de varios AWS servicios, como Amazon, Amazon GuardDuty Inspector y Amazon Macie. Security Hub CSPM también permite a los usuarios pasar de un GuardDuty hallazgo a iniciar una investigación en Amazon Detective.

Sin embargo, las relaciones administrador-miembro que se configuran en estos otros servicios no se aplican automáticamente al CSPM de Security Hub. El CSPM de Security Hub recomienda usar la misma cuenta como cuenta de administrador para todos estos servicios. Esta cuenta de administrador debe ser una cuenta responsable de las herramientas de seguridad. La misma cuenta también debe ser la cuenta de agregador de AWS Config.

Por ejemplo, un usuario de la cuenta de GuardDuty administrador A puede ver los resultados de las cuentas de los GuardDuty miembros B y C en la consola. GuardDuty Si la cuenta A activa el CSPM de Security Hub, los usuarios de la cuenta A no ven automáticamente los GuardDuty resultados de las cuentas B y C en Security Hub CSPM. Estas cuentas también requieren una relación de administrador-miembro del CSPM de Security Hub.

Para hacerlo, designe la cuenta A como la cuenta de administrador del CSPM de Security Hub y habilite las cuentas B y C para que se conviertan en cuentas de miembro del CSPM de Security Hub.

Administrar Security Hub CSPM para varias cuentas conAWS Organizations

Puede integrar AWS Security Hub CSPM con Security Hub CSPM yAWS Organizations, a continuación, administrarlo para las cuentas de su organización.

Para integrar Security Hub CSPM conAWS Organizations, debe crear una organización en. AWS Organizations La cuenta de administración de Organizations designa una cuenta como el administrador delegado del CSPM de Security Hub para la organización. El administrador delegado puede habilitar el CSPM de Security Hub para otras cuentas de la organización, agregar esas cuentas como cuentas de miembro del CSPM de Security Hub y realizar las acciones permitidas en las cuentas de miembro. El administrador delegado del CSPM de Security Hub puede habilitar y administrar el CSPM de Security Hub para un máximo de 10 000 cuentas de miembro.

El alcance de las capacidades de configuración del administrador delegado depende de si utiliza la configuración centralizada. Con la configuración centralizada habilitada, no necesita configurar el CSPM de Security Hub por separado en cada cuenta de miembro ni en cada Región de AWS. El

administrador delegado puede aplicar configuraciones específicas del CSPM de Security Hub en cuentas de miembro y unidades organizativas (UO) seleccionadas en las regiones.

La cuenta de administrador delegado del CSPM de Security Hub puede realizar las acciones siguientes en las cuentas de miembro:

- Si utiliza la configuración centralizada, configure de forma centralizada el CSPM de Security Hub para las cuentas de miembro y las UO mediante la creación de políticas de configuración del CSPM de Security Hub. Las políticas de configuración se pueden utilizar para habilitar y desactivar el CSPM de Security Hub, habilitar y desactivar estándares, y habilitar y desactivar controles.
- Trate automáticamente las cuentas nuevas como cuentas de miembro del CSPM de Security Hub cuando se unan a la organización. Si utiliza la configuración centralizada, una política de configuración asociada a una unidad organizativa incluye las cuentas nuevas y existentes que forman parte de la unidad organizativa.
- Trate las cuentas existentes como cuentas de miembro del CSPM de Security Hub. Esto ocurre automáticamente si utiliza una configuración centralizada.
- Desasociar las cuentas miembro que pertenecen a la organización. Si utiliza la configuración centralizada, solo podrá desasociar una cuenta de miembro después de designarla como autoadministrada. Como alternativa, puede asociar una política de configuración que desactive el CSPM de Security Hub en cuentas de miembro administradas de forma centralizada específicas.

Si no opta por la configuración centralizada, su organización utilizará el tipo de configuración predeterminada denominada configuración local. En la configuración local, el administrador delegado tiene una capacidad más limitada para aplicar la configuración en las cuentas de miembro. Para obtener más información, consulte Descripción de la configuración local en el CSPM de Security Hub.

Para obtener una lista completa de las acciones que el administrador delegado puede llevar a cabo en las cuentas de los miembros, consulte Acciones permitidas para cuentas de administrador y cuentas de miembro en el CSPM de Security Hub.

En los temas de esta sección se explica cómo integrar el Security Hub CSPM AWS Organizations y cómo administrar el Security Hub CSPM para las cuentas de una organización. Cuando proceda, en cada sección, se identifican las ventajas y diferencias de administración para los usuarios de la configuración centralizada.

Temas

- Integración de Security Hub CSPM conAWS Organizations
- Habilitación automática de nuevas cuentas de la organización en el CSPM de Security Hub
- Habilitación manual del CSPM de Security Hub en las cuentas nuevas de la organización
- Desasociación de cuentas de miembro del CSPM de Security Hub de la organización

Integración de Security Hub CSPM conAWS Organizations

Para integrar AWS Security Hub CSPM yAWS Organizations, debe crear una organización en Organizations y utilizar la cuenta de administración de la organización para designar una cuenta de administrador delegada de Security Hub CSPM. Esto habilita el CSPM de Security Hub como un servicio de confianza en Organizations. También habilita el CSPM de Security Hub en la Región de AWS actual para la cuenta de administrador delegado y permite que el administrador delegado habilite el CSPM de Security Hub para las cuentas de miembro, consulte los datos de estas cuentas y realice otras acciones permitidas en ellas.

Si utiliza la configuración centralizada, el administrador delegado también puede crear políticas de configuración del CSPM de Security Hub que especifiquen cómo se deben configurar el servicio, los estándares y los controles del CSPM de Security Hub en las cuentas de la organización.

Creación de una organización

Una organización es una entidad que se crea para consolidar la suya y Cuentas de AWS poder administrarla como una sola unidad.

Puede crear una organización mediante la AWS Organizations consola o mediante un comando de la API del SDK AWS CLI o de una de ellas. Para obtener instrucciones detalladas sobre cómo hacerlo, consulte Creación de una organización en la Guía del usuario de AWS Organizations.

Puede utilizarla AWS Organizations para ver y gestionar de forma centralizada todas las cuentas de su organización. Una organización tiene una cuenta de administración junto con cero o más cuentas miembro. Puede organizar las cuentas jerárquicamente en una estructura de árbol con una raíz en la parte superior y unidades organizativas (OU) anidadas bajo la raíz. Cada cuenta puede estar directamente en el nodo raíz o colocarse en una de las unidades organizativas de la jerarquía. Una unidad organizativa es un contenedor para cuentas específicas. Por ejemplo, puede crear una unidad organizativa de finanzas que incluya todas las cuentas relacionadas con las operaciones financieras.

Recomendaciones para elegir al administrador delegado del CSPM de Security Hub

Si dispone de una cuenta de administrador gracias al proceso de invitación manual y está realizando la transición a la administración de cuentas con ellaAWS Organizations, le recomendamos que designe esa cuenta como administrador delegado de CSPM de Security Hub.

Aunque las API y la consola del CSPM de Security Hub permiten que la cuenta de administración de la organización sea el administrador delegado del CSPM de Security Hub, recomendamos utilizar dos cuentas distintas. Esto se debe a que quienes acceden a la cuenta de administración de la organización para administrar la facturación suelen ser diferentes de quienes necesitan acceder al CSPM de Security Hub para administrar la seguridad.

Le recomendamos que utilice el mismo administrador delegado en todas las regiones. Si opta por la configuración centralizada, el CSPM de Security Hub designa automáticamente el mismo administrador delegado en la región de origen y en cualquier región vinculada.

Verificación de permisos para configurar al administrador delegado

Para designar y eliminar una cuenta de administrador delegado del CSPM de Security Hub, la cuenta de administración de la organización debe tener permisos para las acciones `EnableOrganizationAdminAccount` y `DisableOrganizationAdminAccount` en el CSPM de Security Hub. La cuenta de administración de Organizations también debe contar con permisos administrativos para Organizations.

Para conceder todos los permisos necesarios, asocie las siguientes políticas administradas del CSPM de Security Hub a la entidad principal de IAM de la cuenta de administración de la organización:

- AWSSecurityHubFullAccess
- AWSSecurityHubOrganizationsAccess

Designación del administrador delegado

Para designar la cuenta de administrador delegado del CSPM de Security Hub, puede usar la consola del CSPM de Security Hub, la API del CSPM de Security Hub o la AWS CLI. Security Hub CSPM establece el administrador delegado Región de AWS solo en la actual, y debe repetir la acción en otras regiones. Si comienza a usar la configuración centralizada, el CSPM de Security Hub establece automáticamente el mismo administrador delegado en la región de origen y en las regiones vinculadas.

La cuenta de administración de la organización no necesita tener habilitado el CSPM de Security Hub para designar a la cuenta de administrador delegado del CSPM de Security Hub.

Recomendamos que la cuenta de administración de la organización no sea la cuenta de administrador delegado del CSPM de Security Hub. Sin embargo, si decide usar la cuenta de administración de la organización como la cuenta de administrador delegado del CSPM de Security Hub, la cuenta de administración debe tener habilitado el CSPM de Security Hub. Si la cuenta de administración no tiene habilitado el CSPM de Security Hub, debe habilitar el CSPM de Security Hub manualmente para esa cuenta. El CSPM de Security Hub no se puede habilitar automáticamente para la cuenta de administración de la organización.

Debe designar al administrador delegado del CSPM de Security Hub mediante uno de los siguientes métodos. La designación del administrador delegado del CSPM de Security Hub a través de las API de Organizations no se refleja en el CSPM de Security Hub.

Elija el método que prefiera y siga los pasos para designar la cuenta de administrador delegado del CSPM de Security Hub.

Security Hub CSPM console

Para designar al administrador delegado durante el proceso de incorporación

1. Abra la consola CSPM de AWS Security Hub en. https://console.aws.amazon.com/securityhub/
2. Seleccione Ir al CSPM de Security Hub. Se le solicitará que inicie sesión en la cuenta de administración de la organización.
3. En la página Designar administrador delegado, en la sección Cuenta de administrador delegado, especifique la cuenta de administrador delegado. Se recomienda que elija el mismo administrador delegado que haya configurado para otros servicios de seguridad y conformidad de AWS.
4. Elija Establecer administrador delegado. Se le solicitará que inicie sesión en la cuenta de administrador delegado (si aún no lo ha hecho) para continuar con la integración con la configuración centralizada. Si no desea iniciar la configuración centralizada, seleccione Cancelar. Su administrador delegado está configurado, pero usted todavía no utiliza la configuración centralizada.

Para designar al administrador delegado desde Configuración page

1. Abra la consola CSPM de AWS Security Hub en. https://console.aws.amazon.com/securityhub/
2. En el panel de navegación del CSPM de Security Hub, elija Configuración. A continuación, elija General.
3. Si actualmente hay asignada una cuenta de administrador del CSPM de Security Hub, debe eliminarla antes de poder designar una nueva cuenta.

   En Administrador delegado, para eliminar la cuenta actual, seleccione Eliminar.
4. Ingrese el ID de la cuenta que desea designar como administrador del CSPM de Security Hub.

   Debe designar la misma cuenta de administrador del CSPM de Security Hub en todas las regiones. Si designa una cuenta diferente de la que ha designado en otras regiones, la consola le mostrará un error.
5. Elija Delegar.

Security Hub CSPM API,AWS CLI

Desde la cuenta de administración de la organización, use la operación EnableOrganizationAdminAccount de la API del CSPM de Security Hub. Si utiliza la AWS CLI, ejecute el comando enable-organization-admin-account. Proporcione el ID de la Cuenta de AWS del administrador delegado del CSPM de Security Hub.

El siguiente ejemplo designa al administrador delegado del CSPM de Security Hub- Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$ aws securityhub enable-organization-admin-account --admin-account-id 123456789012
```

Eliminación o cambio del administrador delegado

Solo la cuenta de administración de la organización puede eliminar la cuenta de administrador delegado del CSPM de Security Hub.

Para cambiar al administrador delegado del CSPM de Security Hub, primero debe eliminar la cuenta de administrador delegado actual y luego designar una nueva.

> **Warning**
>
> Cuando se usa la configuración centralizada, no puede utilizar la consola del CSPM de Security Hub ni las API del CSPM de Security Hub para cambiar o eliminar la cuenta de administrador delegado. Si la cuenta de administración de la organización usa la AWS Organizations consola o AWS Organizations las API para cambiar o eliminar el administrador de CSPM de Security Hub delegado, Security Hub CSPM detiene automáticamente la configuración central y elimina las políticas de configuración y las asociaciones de políticas. Las cuentas de los miembros retienen la configuración que tenían antes de que se cambiara o eliminara el administrador delegado.

Si utiliza la consola del CSPM de Security Hub para eliminar al administrador delegado en una región, este se elimina automáticamente en todas las regiones.

La API del CSPM de Security Hub solo elimina la cuenta de administrador delegado del CSPM de Security Hub en la región donde se emite la llamada a la API o el comando. Debe repetir la acción en las demás regiones.

Si utiliza la API de Organizations para eliminar la cuenta de administrador delegado del CSPM de Security Hub, esta se elimina automáticamente en todas las regiones.

Eliminar el administrador delegado (Organizations API,AWS CLI)

Puede usar Organizations para eliminar al administrador delegado del CSPM de Security Hub en todas las regiones.

Si utiliza la configuración centralizada para administrar las cuentas, al eliminar la cuenta de administrador delegado, se eliminarán las políticas de configuración y las asociaciones de políticas. Las cuentas de miembro retienen las configuraciones que tenían antes de que se cambiara o eliminara el administrador delegado. Sin embargo, la cuenta de administrador delegado eliminada ya no puede administrar estas cuentas. Se convierten en cuentas autoadministradas que deben configurarse por separado en cada región.

Elija el método que prefiera y siga las instrucciones para eliminar la cuenta de administrador de CSPM de Security Hub delegada con ella. AWS Organizations

Organizations API,AWS CLI

Para eliminar al administrador delegado del CSPM de Security Hub

Desde la cuenta de administración de la organización, use la operación DeregisterDelegatedAdministrator de la API de Organizations. Si utiliza la AWS CLI, ejecute el comando deregister-delegated-administrator. Proporcione el ID de la cuenta del administrador delegado y la entidad principal de servicio para el CSPM de Security Hub, que es `securityhub.amazonaws.com`.

El siguiente ejemplo elimina al administrador delegado del CSPM de Security Hub. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$ aws organizations deregister-delegated-administrator --account-id 123456789012 --
service-principal securityhub.amazonaws.com
```

Eliminación del administrador delegado (consola del CSPM de Security Hub)

Puede usar la consola del CSPM de Security Hub para eliminar al administrador delegado del CSPM de Security Hub en todas las regiones.

Cuando se elimina la cuenta de administrador delegado del CSPM de Security Hub, las cuentas de miembro se desasocian de esa cuenta de administrador delegado eliminada.

El CSPM de Security Hub permanece habilitado en las cuentas de miembro. Estas se convierten en cuentas independientes hasta que un nuevo administrador del CSPM de Security Hub las habilite nuevamente como cuentas de miembro.

Si la cuenta de administración de la organización no es una cuenta habilitada en el CSPM de Security Hub, use la opción de la página Le damos la bienvenida al CSPM de Security Hub.

Para eliminar la cuenta de administrador CSPM de Security Hub delegada del Bienvenido a Security Hub CSPM page

1. Abra la consola CSPM de AWS Security Hub en. https://console.aws.amazon.com/securityhub/
2. Seleccione Ir a Security Hub.
3. En Administrador delegado, seleccione Eliminar.

Si la cuenta de administración de la organización es una cuenta habilitada en Security Hub, utilice la opción de la pestaña General de la página Configuración.

Para eliminar la cuenta de administrador CSPM de Security Hub delegada del Configuración page

1. Abra la consola CSPM de AWS Security Hub en. https://console.aws.amazon.com/securityhub/
2. En el panel de navegación del CSPM de Security Hub, elija Configuración. A continuación, elija General.
3. En Administrador delegado, seleccione Eliminar.

Eliminar el administrador delegado (API CSPM de Security Hub),AWS CLI)

Puede utilizar la API CSPM de Security Hub o las operaciones CSPM de Security Hub para eliminar AWS CLI al administrador de CSPM de Security Hub delegado. Al eliminar al administrador delegado con uno de estos métodos, este solo se elimina en la región en la que se emitió el comando o la llamada a la API. Security Hub CSPM no actualiza otras regiones ni elimina la cuenta de administrador delegado en ellas. AWS Organizations

Elija el método que prefiera y siga estos pasos para eliminar la cuenta del administrador delegado del CSPM de Security Hub con el CSPM de Security Hub.

Security Hub CSPM API,AWS CLI

Para eliminar al administrador delegado del CSPM de Security Hub

Desde la cuenta de administración de la organización, use la operación DisableOrganizationAdminAccount de la API del CSPM de Security Hub. Si está utilizando elAWS CLI, ejecute el comando. disable-organization-admin-account Proporcione el ID de la cuenta del administrador delegado del CSPM de Security Hub.

El siguiente ejemplo elimina al administrador delegado del CSPM de Security Hub. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$ aws securityhub disable-organization-admin-account --admin-account-id 123456789012
```

Desactivar la integración de Security Hub CSPM conAWS Organizations

Una vez que una AWS Organizations organización se ha integrado con AWS Security Hub CSPM, la cuenta de administración de Organizations puede deshabilitar posteriormente la integración. Como usuario de la cuenta de administración de Organizations, puede hacerlo mediante la desactivación del acceso de confianza del CSPM de Security Hub en AWS Organizations.

Cuando se desactica el acceso de confianza del CSPM de Security Hub, ocurre lo siguiente:

- Security Hub CSPM pierde su condición de servicio de confianza en. AWS Organizations
- La cuenta de administrador delegado del CSPM de Security Hub pierde el acceso a la configuración, los datos y los recursos del CSPM de Security Hub para todas las cuentas de miembro del CSPM de Security Hub en todas las Regiones de AWS.
- Si utilizaba la configuración centralizada, el CSPM de Security Hub deja de usarla automáticamente para la organización. Se eliminan las políticas de configuración y las asociaciones de políticas. Las cuentas retienen las configuraciones que tenían antes de deshabilitar el acceso de confianza.
- Todas las cuentas de miembro del CSPM de Security Hub pasan a ser cuentas independientes y conservan su configuración actual. Si el CSPM de Security Hub estaba habilitado para una cuenta de miembro en una o más regiones, el CSPM de Security Hub continúa habilitado para la cuenta en esas regiones. Los estándares y controles habilitados tampoco se modifican. Puede modificar esta configuración por separado en cada cuenta y región. Sin embargo, la cuenta ya no está asociada a un administrador delegado en ninguna región.

Para obtener información adicional sobre los resultados de la desactivación del acceso a un servicio de confianza, consulte Uso AWS Organizations con otros Servicios de AWS en la Guía del AWS Organizations usuario.

Para deshabilitar el acceso de confianza, puede usar la AWS Organizations consola, la API de Organizations o laAWS CLI. Solo un usuario de la cuenta de administración de Organizations puede desactivar el acceso como servicio de confianza para el CSPM de Security Hub. Para obtener más información sobre los permisos que necesita, consulte Permisos necesarios para deshabilitar el acceso de confianza en la Guía del usuario de AWS Organizations.

Antes de desactivar el acceso como servicio de confianza, recomendamos trabajar con el administrador delegado de la organización para desactivar el CSPM de Security Hub en las cuentas de miembro y limpiar los recursos del CSPM de Security Hub en esas cuentas.

Elija el método que prefiera y siga los pasos para desactivar el acceso como servicio de confianza para el CSPM de Security Hub.

Organizations console

Para desactivar el acceso como servicio de confianza para el CSPM de Security Hub

1. Inicie sesión Consola de administración de AWS con las credenciales de la cuenta de AWS Organizations administración.
2. Abra la consola de Organizations en https://console.aws.amazon.com/organizations/.
3. En el panel de navegación, elija Servicios.
4. En Servicios integrados, elija CSPM de AWS Security Hub.
5. Seleccione Deshabilitar el acceso de confianza.
6. Confirme que desea deshabilitar el acceso de confianza.

Organizations API

Para desactivar el acceso como servicio de confianza para el CSPM de Security Hub

Invoca el DisableAWSServiceAccessfuncionamiento de la AWS Organizations API. En el parámetro `ServicePrincipal`, especifique la entidad principal de servicio del CSPM de Security Hub (`securityhub.amazonaws.com`).

AWS CLI

Para desactivar el acceso como servicio de confianza para el CSPM de Security Hub

Ejecute el comando disable-aws-service-access de la API. AWS Organizations En el parámetro `service-principal`, especifique la entidad principal de servicio del CSPM de Security Hub (`securityhub.amazonaws.com`).

Ejemplo:

```
aws organizations disable-aws-service-access --service-principal
 securityhub.amazonaws.com
```

Habilitación automática de nuevas cuentas de la organización en el CSPM de Security Hub

Cuando se incorporan nuevas cuentas a su organización, se añaden a la lista de la página Cuentas de la consola CSPM de AWS Security Hub. En el caso de las cuentas de la organización, el Tipo

es Por organización. De forma predeterminada, las cuentas nuevas no se convierten en cuentas de miembro del CSPM de Security Hub cuando se unen a la organización. Su estado es No es miembro. La cuenta de administrador delegado puede agregar de manera automática cuentas nuevas como miembros y habilitar el CSPM de Security Hub en estas cuentas cuando se unen a la organización.

> **Note**
>
> Aunque muchas de Regiones de AWS ellas están activas de forma predeterminadaCuenta de AWS, debe activar algunas regiones de forma manual. En el presente documento estas regiones se denominan regiones de suscripción voluntaria. Para habilitar automáticamente el CSPM de Security Hub en una cuenta nueva en una región de suscripción voluntaria, primero debe activar esa región en la cuenta. Solo el propietario de la cuenta puede activar la región de suscripción voluntaria. Para obtener más información sobre las regiones con las que puedes suscribirte, consulta Cómo especificar qué regiones puede usar Regiones de AWS tu cuenta.

Este proceso es diferente en función de si se utiliza la configuración centralizada (recomendada) o la configuración local.

Habilitación automática de nuevas cuentas de la organización (configuración centralizada)

Si utiliza la configuración centralizada, puede habilitar automáticamente el CSPM de Security Hub en las cuentas nuevas y las existentes de la organización mediante la creación de una política de configuración en la que el CSPM de Security Hub esté habilitado. Luego, puede asociar la política a la raíz de la organización o a unidades organizativas (OU) específicas.

Si asocia una política de configuración que habilita el CSPM de Security Hub a una UO específica, el CSPM de Security Hub se habilita automáticamente en todas las cuentas (existentes y nuevas) que pertenecen a esa UO. Las cuentas nuevas que no pertenecen a la unidad organizativa se autoadministran y no tienen habilitado el CSPM de Security Hub automáticamente. Si asocia a la raíz una política de configuración en la que el CSPM de Security Hub esté habilitado, el CSPM de Security Hub se habilitará automáticamente en todas las cuentas (existentes y nuevas) que se unan a la organización. Las excepciones son si una cuenta usa una política diferente por aplicación o herencia, o si es autoadministrada.

En su política de configuración, también puede definir qué estándares y controles de seguridad deben habilitarse en la unidad organizativa. Para generar resultados de control para los estándares habilitados, las cuentas de la OU deben estar AWS Config habilitadas y configuradas para registrar

los recursos necesarios. Para obtener más información sobre el AWS Config registro, consulte Habilitación y configuración AWS Config.

Para obtener instrucciones sobre cómo crear una política de configuración, consulte Creación y asociación de políticas de configuración.

Habilitación automática de nuevas cuentas de la organización (configuración local)

Cuando utiliza la configuración local y activa la habilitación automática de los estándares predeterminados, el CSPM de Security Hub agrega cuentas nuevas de la organización como miembros y habilita el CSPM de Security Hub en estas en la región actual. Otras regiones no se ven afectadas. Además, al activar la habilitación automática, no se habilita el CSPM de Security Hub en las cuentas de la organización existentes, a menos que ya se hayan agregado como cuentas de miembro.

Después de activar la habilitación automática, los estándares de seguridad predeterminados se habilitan para las cuentas de miembro nuevas en la región actual cuando se unen a la organización. Los estándares predeterminados son AWS Foundational Security Best Practices (FSBP) y Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0. No puede cambiar los estándares predeterminados. Si desea habilitar otros estándares en toda su organización o habilitar estándares para cuentas y unidades organizativas seleccionadas, le recomendamos que utilice la configuración centralizada.

Para generar resultados de control para los estándares predeterminados (y otros estándares habilitados), las cuentas de su organización deben estar AWS Config habilitadas y configuradas para registrar los recursos necesarios. Para obtener más información sobre el AWS Config registro, consulte Habilitar y configurar AWS Config.

Elija el método que prefiera y siga estos pasos para habilitar el CSPM de Security Hub en nuevas cuentas de la organización. Estas instrucciones solo se aplican si utiliza la configuración local.

Security Hub CSPM console

Para habilitar automáticamente las cuentas nuevas de la organización como cuentas de miembro del CSPM de Security Hub

1. Abra la consola CSPM de AWS Security Hub en. https://console.aws.amazon.com/securityhub/

   Inicie sesión con las credenciales de la cuenta de administrador delegado.

2. En el panel de navegación del CSPM de Security Hub, en Ajustes, elija Configuración.
3. En la sección Cuentas, active las cuentas. Auto-enable

Security Hub CSPM API

Para habilitar automáticamente las cuentas nuevas de la organización como cuentas de miembro del CSPM de Security Hub

Invoque la API `UpdateOrganizationConfiguration` desde la cuenta de administrador delegado. Defina el campo `AutoEnable` en `true` para habilitar automáticamente el CSPM de Security Hub en las nuevas cuentas de la organización.

AWS CLI

Para habilitar automáticamente las cuentas nuevas de la organización como cuentas de miembro del CSPM de Security Hub

Ejecute el comando `update-organization-configuration` desde la cuenta de administrador delegado. Incluya el parámetro `auto-enable` para habilitar automáticamente el CSPM de Security Hub en las nuevas cuentas de la organización.

```
aws securityhub update-organization-configuration --auto-enable
```

Habilitación manual del CSPM de Security Hub en las cuentas nuevas de la organización

Si no habilita automáticamente el CSPM de Security Hub en las cuentas nuevas de la organización cuando se unen a la organización, puede agregar esas cuentas como cuentas de miembro y habilitar el CSPM de Security Hub en ellas de forma manual después de que se unan. También debe habilitar manualmente el CSPM de Security Hub si anteriormente Cuentas de AWS se desasoció de una organización.

> **Note**
>
> Esta sección no se aplica a su caso si utiliza la configuración centralizada. Si utiliza la configuración centralizada, puede crear políticas de configuración que habiliten el CSPM de Security Hub en cuentas de miembro y unidades organizativas (UO) especificadas. También puede habilitar estándares y controles específicos en esas cuentas y unidades organizativas.

No puede habilitar el CSPM de Security Hub en una cuenta si ya es una cuenta de miembro de otra organización.

Tampoco puede habilitar el CSPM de Security Hub en una cuenta que esté suspendida. Si intenta habilitar el servicio en una cuenta suspendida, el estado de la cuenta cambia a Cuenta suspendida.

- Si la cuenta no tiene habilitado el CSPM de Security Hub, el CSPM de Security Hub se habilita para esa cuenta. El estándar AWS Foundational Security Best Practices (FSBP) y CIS AWS Foundations Benchmark v1.2.0 también están habilitados en la cuenta, a menos que desactive los estándares de seguridad predeterminados.

  La excepción a esto es la cuenta de administración de Organizations. El CSPM de Security Hub no se puede habilitar automáticamente para la cuenta de administración de Organizations. Debe habilitar el CSPM de Security Hub de forma manual en la cuenta de administración de Organizations antes de poder agregarla como una cuenta de miembro.
- Si la cuenta ya tiene habilitado el CSPM de Security Hub, el CSPM de Security Hub no hace ningún otro cambio en la cuenta. Solo habilita la membresía.

Para que el CSPM de Security Hub genere resultados de control, las cuentas de los miembros deben estar AWS Config habilitadas y configuradas para registrar los recursos necesarios. Para obtener más información, consulte Habilitación y configuración de AWS Config.

Elija el método que prefiera y siga los pasos para habilitar una cuenta de organización como cuenta de miembro del CSPM de Security Hub.

Security Hub CSPM console

Habilitación manual de cuentas de la organización como miembros del CSPM de Security Hub

1. Abra la consola CSPM de AWS Security Hub en. https://console.aws.amazon.com/securityhub/

   Inicie sesión con las credenciales de la cuenta de administrador delegado.
2. En el panel de navegación del CSPM de Security Hub, en Ajustes, elija Configuración.
3. En la lista Cuentas, seleccione cada cuenta de la organización que desee habilitar.
4. Elija Acciones y Agregar miembro.

Security Hub CSPM API

Para habilitar manualmente cuentas de la organización como miembros del CSPM de Security Hub

Invoque la API `CreateMembers` desde la cuenta de administrador delegado. Debe indicar el ID de cada cuenta que desee habilitar.

A diferencia del proceso de invitación manual, al invocar `CreateMembers` para habilitar una cuenta de la organización, no es necesario enviar una invitación.

AWS CLI

Para habilitar manualmente cuentas de la organización como miembros del CSPM de Security Hub

Ejecute el comando `create-members` desde la cuenta de administrador delegado. Debe indicar el ID de cada cuenta que desee habilitar.

A diferencia del proceso de invitación manual, al ejecutar `create-members` para habilitar una cuenta de la organización, no es necesario enviar una invitación.

```
aws securityhub create-members --account-details '[{"AccountId": "<accountId>"}]'
```

Ejemplo

```
aws securityhub create-members --account-details '[{"AccountId": "123456789111"},
 {"AccountId": "123456789222"}]'
```

Desasociación de cuentas de miembro del CSPM de Security Hub de la organización

Para dejar de recibir y ver los resultados de una cuenta de miembro de CSPM de AWS Security Hub, puede desasociar la cuenta de miembro de su organización.

> **Note**
>
> Si utiliza la configuración centralizada, la desasociación funciona de forma diferente. Puede crear una política de configuración que desactive el CSPM de Security Hub en una o más cuentas de miembro administradas de forma centralizada. Después de eso, las cuentas continúan en la organización, pero no generarán resultados del CSPM de Security Hub.

Si utiliza la configuración centralizada, pero también tiene cuentas de miembro invitadas manualmente, puede desasociar una o más cuentas invitadas manualmente.

Las cuentas de los miembros que se administran mediante no AWS Organizations pueden disociar sus cuentas de la cuenta de administrador. Solo la cuenta de administrador puede desasociar cuentas de miembro.

Al desasociar una cuenta de miembro, esta no se elimina. En su lugar, la cuenta de miembro se elimina de la organización. La cuenta de miembro disociada se convierte en una cuenta independiente Cuenta de AWS que ya no se administra mediante la integración de CSPM de Security Hub. AWS Organizations

Elija el método que prefiera y siga los pasos para desasociar una cuenta de miembro de la organización.

Security Hub CSPM console

Desasociación de una cuenta de miembro de la organización

1. Abra la consola CSPM de AWS Security Hub en. https://console.aws.amazon.com/securityhub/

   Inicie sesión con las credenciales de la cuenta de administrador delegado.
2. En el panel de navegación, en Configuración, elija Configuración.
3. En la sección Cuentas, seleccione las cuentas que desee desasociar. Si utiliza la configuración centralizada, puede seleccionar una cuenta invitada manualmente para desvincularla desde la pestaña `Invitation accounts`. Esta pestaña solo es visible si utiliza la configuración centralizada.
4. Seleccione Acciones y, a continuación, Desasociar cuenta.

Security Hub CSPM API

Desasociación de una cuenta de miembro de la organización

Invoque la API `DisassociateMembers` desde la cuenta de administrador delegado. Debe proporcionar los Cuenta de AWS ID de las cuentas de los miembros para que se desasocien. Para ver una lista de las cuentas de miembro, invoque la API `ListMembers`.

AWS CLI

Desasociación de una cuenta de miembro de la organización

Ejecute el comando `>disassociate-members` desde la cuenta de administrador delegado. Debe proporcionar los Cuenta de AWS ID de las cuentas de los miembros para desasociarlas. Para ver una lista de las cuentas de miembro, ejecute el comando `>list-members`.

```
aws securityhub disassociate-members --account-ids "<accountIds>"
```

Ejemplo

```
aws securityhub disassociate-members --account-ids "123456789111" "123456789222"
```

También puedes usar la AWS Organizations consola o los AWS SDK para desasociar una cuenta de miembro de tu organización. AWS CLI Para obtener más información, consulte Eliminación de una cuenta miembro de la organización en la Guía del usuario de AWS Organizations.

Administración de cuentas por invitación en el CSPM de Security Hub

Puede administrar de forma centralizada varias cuentas CSPM de AWS Security Hub de dos maneras: integrando Security Hub CSPM AWS Organizations o enviando y aceptando manualmente las invitaciones de membresía. Debe utilizar el proceso manual si tiene una cuenta independiente o no la integra. AWS Organizations En la administración manual de cuentas, el administrador del CSPM de Security Hub invita a cuentas a convertirse en miembros. La relación administrador-miembro se establece cuando un potencial miembro acepta la invitación. Una cuenta de administrador del CSPM de Security Hub puede administrar el CSPM de Security Hub para hasta 1000 cuentas de miembro basadas en invitaciones.

> **Note**
>
> Si crea una organización basada en invitaciones en el CSPM de Security Hub, puede hacer la transición con AWS Organizations posteriormente como alternativa. Si tiene más de una cuenta de miembro, le recomendamos que utilice AWS Organizations en lugar de las invitaciones de CSPM de Security Hub para administrar sus cuentas de miembro. Para obtener información, consulte Administrar Security Hub CSPM para varias cuentas conAWS Organizations.

Cross-Region La agregación de los resultados y otros datos está disponible para las cuentas que invite mediante el proceso de invitación manual. Sin embargo, el administrador debe invitar a la cuenta de miembro de la región de agregación y de todas las regiones vinculadas para que funcione la agregación entre regiones. Además, la cuenta de miembro debe tener habilitado el CSPM de Security Hub en la región de agregación y en todas las regiones vinculadas para que el administrador pueda ver los resultados de la cuenta miembro.

Las políticas de configuración no son compatibles con las cuentas miembros invitadas de forma manual. En su lugar, debe configurar los ajustes de CSPM de Security Hub por separado en cada cuenta de miembro y Región de AWS cuando utilice el proceso de invitación manual.

También debe utilizar el proceso manual basado en invitaciones para las cuentas que no pertenezcan a su organización. Por ejemplo, es posible que no incluya una cuenta de prueba en su organización. También puede optar por consolidar cuentas de varias organizaciones en una sola cuenta de administrador del CSPM de Security Hub. La cuenta de administrador del CSPM de Security Hub debe enviar invitaciones a las cuentas que pertenecen a otras organizaciones.

En la página Configuración de la consola del CSPM de Security Hub, las cuentas agregadas mediante invitación aparecen en la pestaña Cuentas invitadas. Si utiliza la configuración centralizada, pero también invita cuentas externas a la organización, podrá ver los resultados de esas cuentas basadas en invitación en esta pestaña. Sin embargo, el administrador del CSPM de Security Hub no puede configurar las cuentas basadas en invitación en las regiones mediante políticas de configuración.

En esta sección, se explica cómo administrar cuentas de miembros mediante invitaciones.

Temas

- Cómo agregar e invitar cuentas de miembro en el CSPM de Security Hub
- Cómo responder a una invitación para convertirse en una cuenta de miembro del CSPM de Security Hub
- Cómo desasociar cuentas de miembro en el CSPM de Security Hub
- Cómo eliminar cuentas de miembro en el CSPM de Security Hub
- Cómo desasociarse de una cuenta de administrador del CSPM de Security Hub
- Transición a Organizations para administrar cuentas en el CSPM de Security Hub

Cómo agregar e invitar cuentas de miembro en el CSPM de Security Hub

> **Note**
>
> Recomendamos utilizar, AWS Organizations en lugar de Security Hub, invitaciones CSPM para gestionar las cuentas de los miembros. Para obtener información, consulte Administrar Security Hub CSPM para varias cuentas conAWS Organizations.

Su cuenta pasa a ser la administradora de AWS Security Hub CSPM para las cuentas que aceptan su invitación para convertirse en una cuenta miembro de Security Hub CSPM.

Al aceptar una invitación de otra cuenta, su cuenta se convierte en cuenta de miembro, mientras que la otra cuenta se convierte en su administrador.

Si su cuenta es la cuenta de administrador, no podrá aceptar una invitación para convertirse en cuenta de miembro.

El proceso para agregar una cuenta de miembro consta de los siguientes pasos:

1. La cuenta de administrador agrega la cuenta de miembro a su lista.
2. La cuenta de administrador envía una invitación a la cuenta de miembro.
3. La cuenta de miembro acepta la invitación.

Adición de cuentas de miembro

Desde la consola del CSPM de Security Hub, puede agregar cuentas a la lista de cuentas de miembro. En la consola del CSPM de Security Hub, puede seleccionar cuentas de forma individual o cargar un archivo `.csv` que contenga la información de las cuentas.

Para cada cuenta, debe proporcionar el ID de la cuenta y una dirección de correo electrónico. La dirección de correo electrónico debe ser la dirección de correo electrónico de contacto en caso de problemas de seguridad de la cuenta. No se utiliza para verificar la cuenta.

Elija el método que prefiera y siga estos pasos para agregar cuentas de miembro.

Security Hub CSPM console

Cómo agregar cuentas a su lista de cuentas de miembro

1. Abra la consola CSPM de AWS Security Hub en. https://console.aws.amazon.com/securityhub/

   Inicie sesión en las credenciales de una cuenta del administrador.
2. En el panel izquierdo, seleccione Configuración.
3. En la página Configuración, seleccione Cuentas, elija Agregar cuentas y, a continuación, realice alguna de las siguientes operaciones: A continuación, puede agregar cuentas de forma individual o cargar un archivo `.csv` que contenga la lista de cuentas.
4. Para seleccionar las cuentas, realice una de las operaciones siguientes:

   - Para agregar las cuentas de una en una, debajo de Introducir cuentas escriba el ID y la dirección de correo electrónico de la cuenta que se va a agregar y, a continuación, elija Agregar.

     Repita este proceso para cada cuenta.
   - Para utilizar un archivo de valores separados por comas (.csv) para agregar varias cuentas, primero debe crear el archivo. El archivo debe contener el ID y la dirección de correo electrónico de cada cuenta que desee agregar.

     En la lista `.csv`, las cuentas deben aparecer de una en una en cada línea. La primera línea del archivo `.csv` debe contener el encabezado. En el encabezado, la primera columna es **`Account ID`** y la segunda **`Email`**.

     Cada una de las líneas siguientes debe contener un ID de cuenta y una dirección de correo electrónico válidos para la cuenta que se va a añadir.

     Este es un ejemplo de un archivo `.csv` visto en un editor de texto.

     ```
     Account ID,Email
     111111111111,user@example.com
     ```

     En un programa de hojas de cálculo, los campos aparecen en columnas independientes. El formato subyacente sigue separado por comas. Debe formatear los identificadores de cuenta como números no decimales. Por ejemplo, el ID de cuenta 444455556666 no

puede tener el formato 444455556666.0. Asegúrese también de que el formato numérico no elimine ningún cero inicial del ID de la cuenta.

Para seleccionar el archivo, en la consola, seleccione Cargar lista (.csv). A continuación, seleccione Examinar.

Después de seleccionar el archivo, elija Agregar cuentas.

5. Cuando haya terminado de agregar cuentas, en Cuentas que se van a agregar, seleccione Siguiente.

Security Hub CSPM API

Agregación de cuentas a su lista de cuentas de miembro

Invoque la API `CreateMembers` desde la cuenta de administrador. Para añadir cada cuenta de miembro, debe proporcionar el Cuenta de AWS ID.

AWS CLI

Agregación de cuentas a su lista de cuentas de miembro

Ejecute el comando `create-members` desde la cuenta de administrador. Para añadir cada cuenta de miembro, debe proporcionar la Cuenta de AWS identificación.

```
aws securityhub create-members --account-details '[{"AccountId": "<accountID1>"}]'
```

Ejemplo

```
aws securityhub create-members --account-details '[{"AccountId": "123456789111"},
 {"AccountId": "123456789222"}]'
```

Cómo invitar cuentas de miembro

Una vez agregadas las cuentas de miembro, envíe una invitación a la cuenta de miembro. También puede volver a enviar una invitación a una cuenta que haya desvinculado del administrador.

Security Hub CSPM console

Invitación a potenciales cuentas de miembro

1. Abra la consola CSPM de AWS Security Hub en. https://console.aws.amazon.com/securityhub/

   Inicie sesión en las credenciales de una cuenta del administrador.
2. En el panel de navegación, elija Configuración y Cuentas.
3. En la cuenta que va a invitar, elija Invite (Invitar) en la columna Status (Estado).
4. Cuando se le pida confirmación, elija Invitar.

> **Note**
>
> Para volver a enviar invitaciones a cuentas desasociadas, seleccione cada una de las cuentas desasociadas en la página Cuentas. En Acciones, seleccione Volver a enviar invitación.

Security Hub CSPM API

Invitación a potenciales cuentas de miembro

Invoque la API `InviteMembers` desde la cuenta de administrador. Para cada cuenta a la que desee invitar, debe proporcionar el Cuenta de AWS ID.

AWS CLI

Invitación a potenciales cuentas de miembro

Ejecute el comando `invite-members` desde la cuenta de administrador. Para cada cuenta a la que quieras invitar, debes proporcionar el Cuenta de AWS ID.

```
aws securityhub invite-members --account-ids <accountIDs>
```

Ejemplo

```
aws securityhub invite-members --account-ids "123456789111" "123456789222"
```

Cómo responder a una invitación para convertirse en una cuenta de miembro del CSPM de Security Hub

> **Note**
>
> Recomendamos utilizar, AWS Organizations en lugar de Security Hub, invitaciones CSPM para gestionar las cuentas de los miembros. Para obtener información, consulte Administrar Security Hub CSPM para varias cuentas conAWS Organizations.

Puedes aceptar o rechazar una invitación para ser miembro de AWS Security Hub CSPM.

Si acepta una invitación, la cuenta se convierte en una cuenta de miembro del CSPM de Security Hub. La cuenta que envió la invitación se convierte en la cuenta de administrador del CSPM de Security Hub. El usuario de la cuenta de administrador puede ver los resultados de la cuenta de miembro en el CSPM de Security Hub.

Si rechaza la invitación, su cuenta se marcará como Renunciada en la lista de cuentas de miembro de la cuenta de administrador.

Solo puede aceptar una invitación para ser miembro de la cuenta.

Antes de aceptar o rechazar una invitación, debe habilitar el CSPM de Security Hub.

Recuerde que todas las cuentas CSPM de Security Hub deben estar AWS Config habilitadas y configuradas para registrar todos los recursos. Para obtener más información sobre los requisitosAWS Config, consulte Habilitar y configurar. AWS Config

Cómo aceptar una invitación

Puede enviar una invitación para convertirse en una cuenta de miembro del CSPM de Security Hub desde la cuenta de administrador. A continuación, podrá aceptar la invitación tras iniciar sesión en la cuenta de miembro.

Elija el método que prefiera y siga los pasos para aceptar una invitación y convertirse en una cuenta de miembro.

Security Hub CSPM console

Aceptación de una invitación a una suscripción

1. Abra la consola CSPM de AWS Security Hub en. https://console.aws.amazon.com/securityhub/
2. En el panel de navegación, elija Configuración y Cuentas.
3. En la sección Cuenta de administrador, active Aceptar y, a continuación, seleccione Aceptar invitación.

Security Hub CSPM API

Aceptación de una invitación a una suscripción

Invoque la API `AcceptAdministratorInvitation`. Debe proporcionar el identificador de la invitación y el Cuenta de AWS ID de la cuenta de administrador. Para recuperar los detalles de la invitación, utilice la operación `ListInvitations`.

AWS CLI

Aceptación de una invitación a una suscripción

Ejecute el comando `accept-administrator-invitation`. Debe proporcionar el identificador de la invitación y el Cuenta de AWS ID de la cuenta de administrador. Para recuperar los detalles de la invitación, ejecute el comando `list-invitations`.

```
aws securityhub accept-administrator-invitation --administrator-
id <administratorAccountID> --invitation-id <invitationID>
```

Ejemplo

```
aws securityhub accept-administrator-invitation --administrator-id 123456789012 --
invitation-id 7ab938c5d52d7904ad09f9e7c20cc4eb
```

> **Note**
>
> La consola del CSPM de Security Hub aún utiliza `AcceptInvitation`. Con el tiempo, pasará a usar `AcceptAdministratorInvitation`. Cualquier política de IAM que controle

específicamente el acceso a esta función debe seguir empleando `AcceptInvitation`. También debe agregar `AcceptAdministratorInvitation` a sus políticas los permisos correctos una vez que la consola comience a utilizar `AcceptAdministratorInvitation`.

Cómo rechazar una invitación

Puede rechazar una invitación para convertirse en una cuenta de miembro del CSPM de Security Hub. Cuando rechaza una invitación en la consola del CSPM de Security Hub, la cuenta se marca como Renunció en la lista de cuentas de miembro de la cuenta de administrador. El estado Renunció solo aparece cuando inicia sesión en la consola del CSPM de Security Hub con la cuenta de administrador. Sin embargo, no habrá cambios en la invitación en la consola de la cuenta de miembro hasta que inicie sesión en la cuenta de administrador y elimine la invitación.

Para rechazar una invitación, debe iniciar sesión en la cuenta de miembro que recibió la invitación.

Elija el método preferido y siga los pasos para rechazar una invitación para ser una cuenta de miembro.

Security Hub CSPM console

Rechazo de una invitación a una membresía

1. Abra la consola CSPM de AWS Security Hub en. https://console.aws.amazon.com/securityhub/
2. En el panel de navegación, elija Configuración y Cuentas.
3. En la sección Cuenta de administrador, seleccione Rechazar la invitación.

Security Hub CSPM API

Rechazo de una invitación a una membresía

Invoque la API `DeclineInvitations`. Debe proporcionar el Cuenta de AWS ID de la cuenta de administrador que emitió la invitación. Para ver la información sobre sus invitaciones, utilice la operación `ListInvitations`.

AWS CLI

Rechazo de una invitación a una membresía

Ejecute el comando `decline-invitations`. Debe proporcionar el Cuenta de AWS ID de la cuenta de administrador que emitió la invitación. Para ver la información sobre sus invitaciones, ejecute el comando `list-invitations`.

```
aws securityhub decline-invitations --account-ids "<administratorAccountId>"
```

Ejemplo

```
aws securityhub decline-invitations --account-ids "123456789012"
```

Cómo desasociar cuentas de miembro en el CSPM de Security Hub

> **Note**
>
> Recomendamos utilizar, AWS Organizations en lugar de Security Hub, invitaciones CSPM para gestionar las cuentas de los miembros. Para obtener información, consulte Administrar Security Hub CSPM para varias cuentas conAWS Organizations.

Una cuenta de administrador de CSPM de AWS Security Hub puede desasociar una cuenta de miembro para dejar de recibir y ver los resultados de esa cuenta. Debe desvincular una cuenta de miembro antes de poder eliminarla.

Al desvincular una cuenta de miembro, permanece en la lista de cuentas de miembro con el estado Eliminada (desvinculada). Su cuenta se elimina de la información de la cuenta de administrador de la cuenta de miembro.

Para volver a recibir los resultados de la cuenta, puede volver a enviar la invitación. Para eliminar la cuenta de miembro por completo, puede eliminarla.

Elija el método que prefiera y siga los pasos para desasociar una cuenta de miembro invitada manualmente desde la cuenta de administrador.

Security Hub CSPM console

Desasociación de una cuenta de miembro invitada manualmente

1. Abra la consola CSPM de AWS Security Hub en. https://console.aws.amazon.com/securityhub/

Inicie sesión en las credenciales de una cuenta del administrador.

2. En el panel de navegación, en Configuración, elija Configuración.
3. En la sección Cuentas, seleccione las cuentas que desee desasociar.
4. Seleccione Acciones y, a continuación, Desasociar cuenta.

Security Hub CSPM API

Desasociación de una cuenta de miembro invitada manualmente

Invoque la API `DisassociateMembers` desde la cuenta de administrador. Debe proporcionar los Cuenta de AWS ID de las cuentas de los miembros que desee desasociar. Para ver una lista de las cuentas miembro, utilice la operación `ListMembers`.

AWS CLI

Desasociación de una cuenta de miembro invitada manualmente

Ejecute el comando `disassociate-members` desde la cuenta de administrador. Debe proporcionar los Cuenta de AWS ID de las cuentas de los miembros que desee desasociar. Para ver una lista de las cuentas de miembro, ejecute el comando `list-members`.

```
aws securityhub disassociate-members --account-ids <accountIds>
```

Ejemplo

```
aws securityhub disassociate-members --account-ids "123456789111" "123456789222"
```

Cómo eliminar cuentas de miembro en el CSPM de Security Hub

> **Note**
>
> Recomendamos utilizar, AWS Organizations en lugar de Security Hub, invitaciones CSPM para gestionar las cuentas de los miembros. Para obtener información, consulte Administrar Security Hub CSPM para varias cuentas conAWS Organizations.

Como cuenta de administrador de CSPM de AWS Security Hub, puede eliminar las cuentas de miembros que se agregaron por invitación. Antes de poder eliminar una cuenta habilitada, debe desvincularla.

Al eliminar una cuenta de miembro, se elimina por completo de la lista. Para restaurar la suscripción de la cuenta, debe agregarla e invitarla de nuevo, como si se tratara de una cuenta de miembro completamente nueva.

No puede eliminar las cuentas que pertenecen a una organización y que se administran mediante la integración con. AWS Organizations

Elija el método que prefiera y siga los pasos para eliminar las cuentas de miembro invitados manualmente.

Security Hub CSPM console

Eliminación de una cuenta de miembro invitada manualmente

1. Abra la consola CSPM de AWS Security Hub en. https://console.aws.amazon.com/securityhub/

   Inicie sesión con la cuenta de administrador.
2. En el panel de navegación, elija Configuración y, a continuación, elija Configuración.
3. Seleccione la pestaña Cuentas de invitación. A continuación, seleccione las cuentas que desea eliminar.
4. Elija Acciones y, a continuación, elija Eliminar. Esta opción solo está disponible si ha desasociado la cuenta. Debe desasociar una cuenta de miembro antes de poder eliminarla.

Security Hub CSPM API

Eliminación de una cuenta de miembro invitada manualmente

Invoque la API `DeleteMembers` desde la cuenta de administrador. Debe proporcionar los ID de Cuenta de AWS de las cuentas de miembro de que desee eliminar. Para recuperar la lista de cuentas de miembro, invoque la API `ListMembers`.

AWS CLI

Eliminación de una cuenta de miembro invitada manualmente

Ejecute el comando `delete-members` desde la cuenta de administrador. Debe proporcionar los ID de Cuenta de AWS de las cuentas de miembro de que desee eliminar. Para recuperar la lista de cuentas de miembro, ejecute el comando `list-members`.

```
aws securityhub delete-members --account-ids <memberAccountIDs>
```

Ejemplo

```
aws securityhub delete-members --account-ids "123456789111" "123456789222"
```

Cómo desasociarse de una cuenta de administrador del CSPM de Security Hub

> **Note**
>
> Recomendamos utilizar, AWS Organizations en lugar de Security Hub, invitaciones CSPM para gestionar las cuentas de los miembros. Para obtener información, consulte Administrar Security Hub CSPM para varias cuentas conAWS Organizations.

Si su cuenta se agregó como cuenta de miembro de AWS Security Hub CSPM por invitación, puede desasociar la cuenta de miembro de la cuenta de administrador. Después de desasociar una cuenta de miembro, el CSPM de Security Hub deja de enviar resultados de la cuenta a la cuenta de administrador.

Las cuentas de los miembros que se administran mediante la integración con no AWS Organizations pueden disociar sus cuentas de la cuenta de administrador. Solo el administrador delegado del CSPM de Security Hub puede desasociar cuentas de miembro que se administran con Organizations.

Cuando se desvincula de su cuenta de administrador, su cuenta permanece en la lista de miembros de la cuenta de administrador con el estado Renunciado. Sin embargo, la cuenta de administrador no recibe ningún dato sobre su cuenta.

Tras desasociarse de la cuenta de administrador, la invitación para ser miembro seguirá vigente. Puede volver a aceptar la invitación en el futuro.

Security Hub CSPM console

Cómo desvincularse de su cuenta de administrador

1. Abra la consola CSPM de AWS Security Hub en. https://console.aws.amazon.com/securityhub/
2. En el panel de navegación, elija Configuración y Cuentas.
3. En la sección Cuenta de administrador, desactive Aceptar y, a continuación, seleccione Actualizar.

Security Hub CSPM API

Desasociación de su cuenta de administrador

Invoque la API `DisassociateFromAdministratorAccount`.

AWS CLI

Desasociación de su cuenta de administrador

Ejecute el comando `disassociate-from-administrator-account`.

```
aws securityhub disassociate-from-administrator-account
```

> **Note**
>
> La consola del CSPM de Security Hub aún utiliza `DisassociateFromMasterAccount`. Con el tiempo, pasará a usar `DisassociateFromAdministratorAccount`. Cualquier política de IAM que controle específicamente el acceso a esta función debe seguir empleando `DisassociateFromMasterAccount`. También debe agregar `DisassociateFromAdministratorAccount` a sus políticas los permisos correctos una vez que la consola comience a utilizar `DisassociateFromAdministratorAccount`.

Transición a Organizations para administrar cuentas en el CSPM de Security Hub

Al administrar las cuentas manualmente en AWS Security Hub CSPM, debe invitar a posibles cuentas de miembros y configurar cada cuenta de miembro por separado en cada una de ellas. Región de AWS

Al integrar Security Hub CSPMAWS Organizations, puede eliminar la necesidad de enviar invitaciones y obtener un mayor control sobre cómo se configura y personaliza Security Hub CSPM en su organización. Por esta razón, recomendamos usar AWS Organizations en lugar de las invitaciones del CSPM de Security Hub para administrar las cuentas de miembro. Para obtener información, consulte Administrar Security Hub CSPM para varias cuentas conAWS Organizations.

Es posible utilizar un enfoque combinado en el que se utiliza la AWS Organizations integración, pero también se pueden invitar manualmente a cuentas ajenas a la organización. Sin embargo, recomendamos utilizar exclusivamente la integración de Organizations. La configuración centralizada, una característica que ayuda a administrar el CSPM de Security Hub en múltiples cuentas y regiones, solo está disponible cuando se integra con Organizations.

En esta sección, se explica cómo pasar de la administración manual de cuentas basada en invitaciones a la administración de cuentas con AWS Organizations.

Integración de Security Hub CSPM conAWS Organizations

En primer lugar, debe integrar Security Hub CSPM y. AWS Organizations

Siga los pasos que se indican a continuación para integrar estos servicios:

- Creación de una organización en AWS Organizations. Para obtener instrucciones sobre cómo hacerlo, consulte Creación de una organización en la Guía del usuario de AWS Organizations.
- Desde la cuenta de administración de Organizations, designe una cuenta de administrador delegado del CSPM de Security Hub.

> **Note**
>
> La cuenta de administración de Organizations no se puede establecer como cuenta de administrador delegado.

Para obtener instrucciones detalladas, consulte Integración de Security Hub CSPM conAWS Organizations.

Al completar los pasos anteriores, se concede un acceso de confianza para el Security Hub CSPM en. AWS Organizations Esto también habilita el CSPM de Security Hub en la cuenta actual Región de AWS de administrador delegado.

El administrador delegado puede administrar la organización en el CSPM de Security Hub, principalmente al agregar las cuentas de la organización como cuentas de miembro del CSPM de Security Hub. El administrador también puede acceder a ciertos ajustes, datos y recursos del CSPM de Security Hub para esas cuentas.

Al hacer la transición a la administración de cuentas mediante Organizations, las cuentas basadas en invitaciones no se convierten automáticamente en miembros del CSPM de Security Hub. Solo las cuentas que agregue a la nueva organización se pueden convertir en miembros del CSPM de Security Hub.

Tras activar la integración, puede administrar las cuentas con Organizations. Para obtener información, consulte Administrar Security Hub CSPM para varias cuentas conAWS Organizations. La administración de cuentas varía en función del tipo de configuración de la organización.

Acciones permitidas para cuentas de administrador y cuentas de miembro en el CSPM de Security Hub

Las cuentas de administrador y miembro tienen acceso a las acciones de CSPM de AWS Security Hub que se indican en las siguientes tablas. En las tablas, los valores tienen los siguientes significados:

- Cualquiera: la cuenta puede llevar a cabo la acción para todas las cuentas de miembro del mismo administrador.
- Actual: la cuenta solo puede llevar a cabo la acción por sí misma (la cuenta en la que ha iniciado sesión).
- Guion: indica que la cuenta no puede llevar a cabo la acción.

Como se indica en las tablas, las acciones permitidas varían según el tipo de configuración que utilice la organización AWS Organizations y el tipo de configuración que utilice. Para obtener más información acerca de la diferencia la configuración local y centralizada, consulte Administrar cuentas conAWS Organizations.

El CSPM de Security Hub no copia los resultados de las cuentas de miembro en la cuenta de administrador. En el CSPM de Security Hub, todos los resultados se ingestan en una región específica para una cuenta específica. En cada región, la cuenta del administrador puede ver y gestionar los resultados de sus cuentas de miembro en esa región.

Si establece una región de agregación, la cuenta de administrador puede ver y administrar los resultados de las cuentas de miembro de las regiones vinculadas que se replican en la región de agregación. Para obtener más información sobre la agregación entre regiones, consulte Cross-Region Agregación.

Las siguientes tablas especifican los permisos predeterminados para las cuentas de administrador y las cuentas de miembro. Puede utilizar políticas de IAM personalizadas para restringir aún más el acceso a las características y funciones del CSPM de Security Hub. Para obtener orientación y ejemplos, consulte la entrada del blog Alineación de las políticas de IAM con las personas de los usuarios para AWS Security Hub CSPM.

Acciones permitidas si integra con Organizations y usa la configuración centralizada

Cuando se integra con Organizations y se utiliza la configuración centralizada, las cuentas de administrador y de miembro pueden acceder a las acciones del CSPM de Security Hub de la siguiente manera.

Action	Cuenta de administrador delegado del CSPM de Security Hub	Cuenta de miembro administrada de forma centralizada	Self-managed cuenta de miembro
Creación y administración de políticas de configuración del CSPM de Security Hub	Para cuentas administradas automáticamente y de forma centralizada	–	–
Visualización de cuentas de la organización	Cualquiera	–	–
Desvincular cuenta de miembro	Cualquiera	–	–
Eliminar cuenta de miembro	Cualquier cuenta que no sea de una organización	–	–

Action	Cuenta de administrador delegado del CSPM de Security Hub	Cuenta de miembro administrada de forma centralizada	Self-managed cuenta de miembro
Desactivación del CSPM de Security Hub	Para cuentas actuales y cuentas administradas de forma centralizada	–	Actuales (deben desasociarse de la cuenta de administrador)
Vea los resultados y el historial de búsquedas	Cualquiera	Actuales	Actuales
Actualizar los resultados	Cualquiera	Actuales	Actuales
Ver los resultados de los hallazgos	Cualquiera	Actuales	Actuales
Ver los detalles de control	Cualquiera	Actuales	Actuales
Activación o desactivación de los resultados de control consolidados	Cualquiera	–	–
Habilitar y deshabilitar estándares	Para cuentas actuales y cuentas administradas de forma centralizada	–	Actuales
Habilitar y deshabilitar controles	Para cuentas actuales y cuentas administradas de forma centralizada	–	Actuales

Action	Cuenta de administrador delegado del CSPM de Security Hub	Cuenta de miembro administrada de forma centralizada	Self-managed cuenta de miembro
Habilitar y deshabilitar integraciones	Actuales	Actuales	Actuales
Configurar agregación entre regiones	Cualquiera	–	–
Selección de la región de origen y las regiones vinculadas	Cualquiera (debe detener y reiniciar la configuración centralizada para cambiar la región de origen)	–	–
Configurar acciones personalizadas	Actuales	Actuales	Actuales
Configurar reglas de automatización	Cualquiera	–	–
Configurar hallazgos personalizados	Actuales	Actuales	Actuales

Acciones permitidas si integra con Organizations y usa la configuración local

Las cuentas de administrador y de miembro pueden acceder a las acciones del CSPM de Security Hub de la siguiente manera cuando se integra con Organizations y se utiliza la configuración local.

Action	Cuenta de administrador delegado del CSPM de Security Hub	Cuenta de miembro
Creación y administración de políticas de configuración del CSPM de Security Hub	–	–

Action	Cuenta de administrador delegado del CSPM de Security Hub	Cuenta de miembro
Visualización de cuentas de la organización	Cualquiera	–
Desvincular cuenta de miembro	Cualquiera	–
Eliminar cuenta de miembro	–	–
Desactivación del CSPM de Security Hub	–	Actual (si la cuenta está desasociada del administrador delegado)
Vea los resultados y el historial de búsquedas	Cualquiera	Actuales
Actualizar los resultados	Cualquiera	Actuales
Ver los resultados de los hallazgos	Cualquiera	Actuales
Ver los detalles de control	Cualquiera	Actuales
Activación o desactivación de los resultados de control consolidados	Cualquiera	–
Habilitar y deshabilitar estándares	Actuales	Actuales
Habilitar automáticamente el CSPM de Security Hub y los estándares predeterminados en las nuevas cuentas de la organización	Para cuentas actuales y cuentas nuevas de la organización	–

Action	Cuenta de administrador delegado del CSPM de Security Hub	Cuenta de miembro
Habilitar y deshabilitar controles	Actuales	Actuales
Habilitar y deshabilitar integraciones	Actuales	Actuales
Configurar agregación entre regiones	Cualquiera	–
Configurar acciones personalizadas	Actuales	Actuales
Configurar reglas de automatización	Cualquiera	–
Configurar hallazgos personalizados	Actuales	Actuales

Acciones permitidas para las cuentas basadas en invitaciones

Las cuentas de administrador y miembro pueden acceder a las acciones de CSPM de Security Hub de la siguiente manera si utiliza el método basado en invitaciones para administrar las cuentas manualmente en lugar de integrarlas. AWS Organizations

Action	Cuenta de administrador del CSPM de Security Hub	Cuenta de miembro
Creación y administración de políticas de configuración del CSPM de Security Hub	–	–
Visualización de cuentas de la organización	Cualquiera	–

Action	Cuenta de administrador del CSPM de Security Hub	Cuenta de miembro
Desvincular cuenta de miembro	Cualquiera	Actuales
Eliminar cuenta de miembro	Cualquiera	–
Desactivación del CSPM de Security Hub	Actual (si no hay cuentas de miembro habilitadas)	Actual (si la cuenta está desasociada de la cuenta de administrador)
Vea los resultados y el historial de búsquedas	Cualquiera	Actuales
Actualizar los resultados	Cualquiera	Actuales
Ver los resultados de los hallazgos	Cualquiera	Actuales
Ver los detalles de control	Cualquiera	Actuales
Activación o desactivación de los resultados de control consolidados	Cualquiera	–
Habilitar y deshabilitar estándares	Actuales	Actuales
Habilitar automáticamente el CSPM de Security Hub y los estándares predeterminados en las nuevas cuentas de la organización	–	–
Habilitar y deshabilitar controles	Actuales	Actuales

Action	Cuenta de administrador del CSPM de Security Hub	Cuenta de miembro
Habilitar y deshabilitar integraciones	Actuales	Actuales
Configurar agregación entre regiones	Cualquiera	–
Configurar acciones personalizadas	Actuales	Actuales
Configurar reglas de automatización	Cualquiera	–
Configurar hallazgos personalizados	Actuales	Actuales

Efecto de las acciones de la cuenta en los datos del CSPM de Security Hub

Estas acciones de la cuenta tienen los siguientes efectos en los datos AWS de CSPM de Security Hub.

Desactivación del CSPM de Security Hub

Si utiliza la configuración centralizada, el administrador delegado (DA) puede crear políticas de configuración del CSPM de Security Hub que desactiven el CSPM de AWS Security Hub en cuentas y unidades organizativas (UO) específicas. En este caso, el CSPM de Security Hub se desactiva en las cuentas y UO especificadas, tanto en la región de origen como en cualquier región vinculada. Si no utiliza la configuración centralizada, debe desactivar el CSPM de Security Hub por separado en cada cuenta y región donde lo haya habilitado. No puede usar la configuración centralizada si el CSPM de Security Hub está desactivado en la cuenta del administrador delegado.

No se generan ni actualizan resultados para la cuenta de administrador si el CSPM de Security Hub está desactivado en esa cuenta. Los resultados archivados existentes se eliminan después de 30 días. Los resultados activos existentes se eliminan después de 90 días.

Se eliminan las integraciones con otrasServicios de AWS.

Los estándares de seguridad y controles habilitados se deshabilitan.

Otros datos y configuraciones del CSPM de Security Hub, incluidas las acciones personalizadas, la información y las suscripciones a productos de terceros, se retienen durante 90 días.

Cuenta miembro disociada de la cuenta de administrador

Cuando una cuenta miembro se desvincula de la cuenta de administrador, esta pierde el permiso para ver los resultados en la cuenta de miembro. Sin embargo, el CSPM de Security Hub permanece habilitado en ambas cuentas.

Si utiliza la configuración centralizada, el administrador delegado no puede configurar el CSPM de Security Hub para una cuenta de miembro que esté desasociada de la cuenta del administrador delegado.

La configuración personalizada o las integraciones definidas para la cuenta de administrador no se aplican a los resultados de la antigua cuenta de miembro. Por ejemplo, después de disociar las cuentas, es posible que tengas una acción personalizada en la cuenta de administrador utilizada como patrón de eventos en una EventBridge regla de Amazon. Sin embargo, esta acción personalizada no se puede utilizar en la cuenta de miembro.

En la lista Cuentas de la cuenta de administrador del CSPM de Security Hub, una cuenta eliminada aparece con el estado Desasociada.

Cómo eliminar una cuenta miembro de una organización

Cuando se elimina una cuenta de miembro de una organización, la cuenta de administrador del CSPM de Security Hub pierde el permiso para ver los resultados de la cuenta de miembro. Sin embargo, el CSPM de Security Hub permanece habilitado en ambas cuentas con la misma configuración que tenían antes de la eliminación.

Si utiliza la configuración centralizada, no puede configurar el CSPM de Security Hub para una cuenta de miembro después de que se haya eliminado de la organización a la que pertenece el administrador delegado. Sin embargo, la cuenta retiene la configuración que tenía antes de la eliminación, a menos que la cambie manualmente.

En la lista Cuentas de la cuenta de administrador del CSPM de Security Hub, una cuenta eliminada aparece con el estado Eliminada.

Cuenta suspendida

Cuando Cuenta de AWS se suspende una, la cuenta pierde el permiso para ver sus hallazgos en Security Hub CSPM. No se generan ni actualizan resultados para esa cuenta. La cuenta de administrador de una cuenta suspendida puede ver los resultados existentes de la cuenta.

En el caso de una cuenta de organización, el estado de la cuenta de miembro también puede cambiar a Cuenta suspendida. Esto sucede si la cuenta se suspende en el mismo momento en que la cuenta del administrador intenta habilitarla. La cuenta de administrador de una Cuenta suspendida no puede ver los resultados de esa cuenta. De lo contrario, el estado suspendido no afectará al estado de la cuenta miembro.

Si utiliza la configuración centralizada, se producirá un error en la asociación de políticas si el administrador delegado intenta asociar una política de configuración a una cuenta suspendida.

Transcurridos 90 días, la cuenta se termina o se reactiva. Cuando la cuenta se reactiva, se restauran sus permisos del CSPM de Security Hub. Si el estado de la cuenta de miembro es Cuenta suspendida, la cuenta del administrador debe habilitar la cuenta manualmente.

Cuenta cerrada

Cuando un Cuenta de AWS está cerrado, el Security Hub CSPM responde al cierre de la siguiente manera.

Si la cuenta es una cuenta de administrador del CSPM de Security Hub, se elimina como cuenta de administrador y se eliminan todas las cuentas de miembro. Si la cuenta es una cuenta de miembro, se desasocia y se elimina como miembro de la cuenta de administrador del CSPM de Security Hub.

El CSPM de Security Hub retiene los resultados archivados existentes de la cuenta durante 30 días. En el caso de un resultado correspondiente a un control, el cálculo de los 30 días se basa en el valor del campo `UpdatedAt` del resultado. Para otro tipo de resultado, el cálculo se basa en el valor del campo `UpdatedAt` o `ProcessedAt` del resultado, según cuál fecha sea más reciente. Al finalizar este periodo de 30 días, el CSPM de Security Hub elimina permanentemente el resultado de la cuenta.

El CSPM de Security Hub retiene los resultados activos existentes de la cuenta durante 90 días. En el caso de un resultado correspondiente a un control, el cálculo de los 90 días se basa en el valor del campo `UpdatedAt` del resultado. Para otro tipo de resultado, el cálculo se basa en el valor del campo `UpdatedAt` o `ProcessedAt` del resultado, según cuál fecha sea más reciente. Al finalizar

este periodo de 90 días, el CSPM de Security Hub elimina permanentemente el resultado de la cuenta.

Para retener los resultados existentes por un periodo más largo, puede exportarlos a un bucket de S3. Puedes hacerlo mediante una acción personalizada con una EventBridge regla de Amazon. Para obtener más información, consulte Uso EventBridge para respuesta y remediación automatizadas.

> **Important**
>
> En el caso de los clientes registradosAWS GovCloud (US) Regions, haz una copia de seguridad de los datos de tu póliza y otros recursos de la cuenta y los borra antes de cerrarla. No tendrá acceso a los recursos ni datos después de cerrar la cuenta.

Para obtener más información, consulte Cerrar una Cuenta de AWS en la Guía de referencia de AWS Account Management

Descripción de la agregación entre regiones en el CSPM de Security Hub

> **Note**
>
> La región de agregación ahora se denomina región de origen. Algunas operaciones de la API del CSPM de Security Hub aún utilizan el término anterior región de agregación.

Al utilizar la agregación entre regiones en AWS Security Hub CSPM, puede agregar hallazgos, encontrar actualizaciones, información, estados de cumplimiento de controles y puntajes de seguridad de varias regiones de origen Regiones de AWS a una sola. A continuación, puede administrar todos estos datos desde la región de origen.

Supongamos que establece este de EE. UU.(norte de Virginia) como región de origen y oeste de EE. UU. (Oregón) y oeste de EE. UU. (norte de California) como regiones vinculadas. Al ver la página Resultados en Este de EE. UU. (Norte de Virginia), verá los resultados de las tres regiones. Las actualizaciones de esos resultados también se reflejan en las tres regiones.

> **Note**
>
> EnAWS GovCloud (US), la agregación entre regiones solo se admite para los hallazgos, las actualizaciones de búsquedas y la información de todos los países. AWS GovCloud (US) En concreto, solo puede agregar hallazgos, actualizaciones e información entre AWS GovCloud (US-East) y AWS GovCloud (US-West). En las regiones de China, solo se admite agregación entre regiones de los resultados, las actualizaciones de resultados y los hallazgos de las regiones de China. En concreto, solo puede agregar resultados, actualizaciones de resultados y hallazgos entre China (Pekín) y China (Ningxia).

Si un control está activado en una región vinculada pero deshabilitado en la región de origen, podrá ver el estado de conformidad del control desde la región de origen, pero no podrá habilitar ni deshabilitar ese control desde la región de origen. La única excepción es si se utiliza la configuración centralizada. Si utiliza la configuración centralizada, el administrador delegado del CSPM de Security Hub puede configurar controles en la región principal y en las regiones vinculadas desde la región principal.

Si ha establecido una región de origen, las puntuaciones de seguridad tienen en cuenta los estados de control en todas las regiones vinculadas. Para ver las puntuaciones de seguridad y los estados de cumplimiento entre regiones, agregue los siguientes permisos al rol de IAM que usa el CSPM de Security Hub:

- `ListSecurityControlDefinitions`
- `BatchGetStandardsControlAssociations`
- `BatchUpdateStandardsControlAssociations`

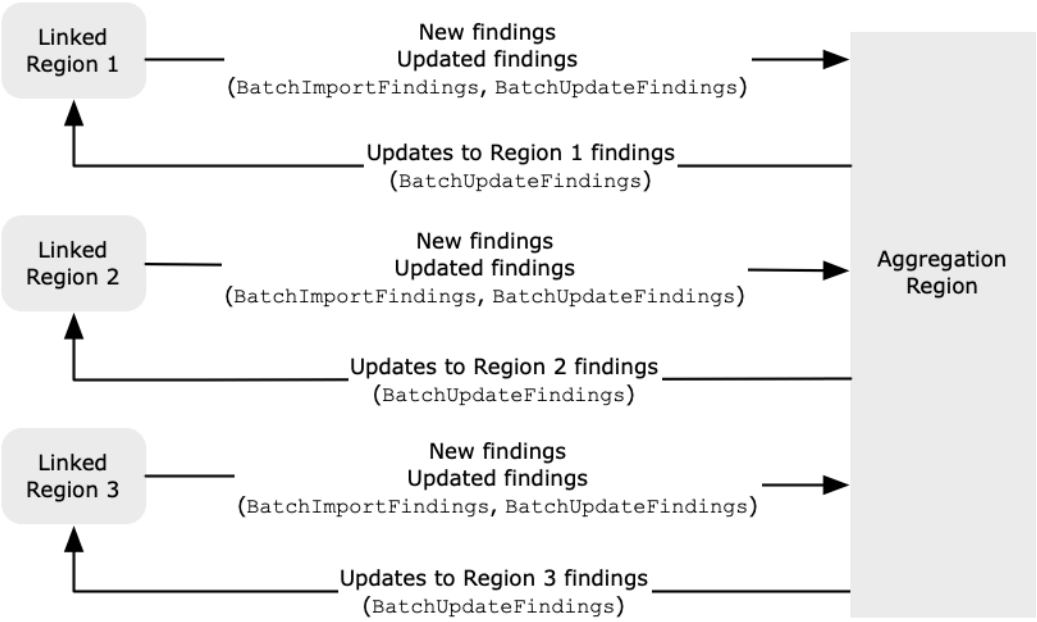
Tipos de datos que se agregan

Cuando la agregación entre regiones está habilitada con una o más regiones vinculadas, el CSPM de Security Hub replica los siguientes datos desde las regiones vinculadas hacia la región de origen. Esto ocurre en todas las cuentas que tienen habilitada la agregación entre regiones.

- Hallazgos
- Información
- Estados de control de la conformidad

- Puntuaciones de seguridad

Además de los nuevos datos que aparecen en la lista anterior, el CSPM de Security Hub también replica las actualizaciones a estos datos entre las regiones vinculadas y la región de origen. Las actualizaciones que se producen en una región vinculada se replican en la región de origen. Las actualizaciones que se producen en la región de origen se replican de vuelta en la región vinculada. Si hay actualizaciones contradictorias en la región de origen y en la región vinculada, se utiliza la actualización más reciente.



Cross-Region la agregación no aumenta el coste del Security Hub CSPM. No se le cobrará nada cuando el CSPM de Security Hub replique nuevos datos o actualizaciones.

En la región de origen, la página Resumen ofrece una vista de los resultados activos en las regiones vinculadas. Para más información, consulte Visualización de un resumen de los resultados entre regiones por gravedad. Otros paneles de la página Resumen que analizan los resultados también muestran información de todas las regiones vinculadas.

Las puntuaciones de seguridad en la región de origen se calculan comparando el número de controles aprobados con el número de controles habilitados en todas las regiones vinculadas. Además, si un control está activado en al menos una región vinculada, estará visible en las páginas de detalles de las normas de seguridad de la región de origen. El estado de cumplimiento de los controles en las páginas de detalles de las normas refleja los resultados de las regiones vinculadas. Si un control de seguridad asociado a un control falla en una o más regiones vinculadas, el estado de conformidad de ese control aparece como Con fallos en las páginas de detalles de las normas de la

región de origen. El número de controles de seguridad incluye los resultados de todas las regiones vinculadas.

El CSPM de Security Hub solo agrega datos de las regiones en las que haya alguna cuenta que tenga el CSPM de Security Hub habilitado. El CSPM de Security Hub no se habilita automáticamente para ninguna cuenta en función de la configuración de agregación entre regiones.

Es posible activar la agregación entre regiones sin seleccionar ninguna región vinculada. En este caso, no se replican los datos.

Agregación de cuentas de administrador y de miembros

La agregación entre regiones se configura mediante cuentas independientes, cuentas de miembros y cuentas de administrador. Si un administrador realiza la configuración, la presencia de la cuenta de administrador es esencial para que la agregación entre regiones funcione en las cuentas administradas. Si la cuenta de administrador se elimina o se desvincula de una cuenta de miembro, se detiene la agregación entre regiones para la cuenta de miembro. Esto se cumple incluso si la cuenta tenía activada la agregación entre regiones antes de que se iniciara la asociación administrador-miembro.

Cuando una cuenta de administrador habilita la agregación entre regiones, el CSPM de Security Hub replica en la región de origen los datos que la cuenta de administrador genera en todas las regiones vinculadas. Además, el CSPM de Security Hub identifica las cuentas de miembro asociadas a ese administrador, y cada una de estas hereda la configuración de agregación entre regiones del administrador. El CSPM de Security Hub replica en la región de origen los datos que una cuenta de miembro genera en todas las regiones vinculadas.

El administrador puede acceder a los resultados de seguridad y administrarlos desde todas las cuentas de miembros de las regiones administradas. Sin embargo, como administrador del CSPM de Security Hub, debe iniciar sesión en la región de origen para ver los datos agregados de todas las cuentas de miembro y las regiones vinculadas.

Como cuenta de miembro del CSPM de Security Hub, debe iniciar sesión en la región de origen para ver los datos agregados de la cuenta desde todas las regiones vinculadas. Las cuentas de miembros no tienen permisos para ver los datos de otras cuentas de miembros.

Una cuenta de administrador puede invitar manualmente a las cuentas de los miembros o actuar como administradora delegada de una organización con la que esté integrada. AWS Organizations En el caso de una cuenta de miembro invitada de forma manual, el administrador debe invitar a

la cuenta de la región de origen y de todas las regiones vinculadas para que la agregación entre regiones funcione. Además, la cuenta de miembro debe tener habilitado el CSPM de Security Hub en la región de origen y en todas las regiones vinculadas para que el administrador pueda ver los resultados de la cuenta de miembro. Si no utiliza la región de origen para otros fines, puede desactivar los estándares e integraciones del CSPM de Security Hub en esa región para evitar cargos.

Si tiene pensado utilizar la agregación entre regiones y posee varias cuentas de administrador, se recomienda que siga estas prácticas:

- Cada cuenta de administrador tiene cuentas de miembro diferentes.
- Cada cuenta de administrador tiene las mismas cuentas de miembro en todas las regiones.
- Cada cuenta de administrador utiliza una región de origen diferente.

> **Note**
>
> Para entender el impacto de la agregación entre regiones en la configuración centralizada, consulte Impacto de la configuración centralizada en la agregación entre regiones.

Impacto de la configuración centralizada en la agregación entre regiones

La configuración central es una función opcional de AWS Security Hub CSPM que puede utilizar si se integra con. AWS Organizations Con la configuración centralizada, la cuenta de administrador delegado puede configurar el servicio CSPM de Security Hub, así como los estándares y controles, para las cuentas y las unidades organizativas (UO) de la organización. Para configurar cuentas y unidades organizativas, el administrador delegado crea políticas de configuración del CSPM de Security Hub. Las políticas de configuración se pueden utilizar para definir si el CSPM de Security Hub está habilitado o desactivado, así como qué estándares y controles se habilitan. El administrador delegado asocia las políticas de configuración a cuentas, unidades organizativas específicas o a la raíz (toda la organización).

El administrador delegado puede crear y administrar políticas de configuración para la organización solo desde la región de origen. Además, las políticas de configuración entran en vigor en la región de origen y en todas las regiones vinculadas. No puede crear una política de configuración que se aplique exclusivamente a algunas regiones vinculadas. Para obtener información sobre la agregación entre regiones, consulte agregación. Cross-Region

Para utilizar la configuración centralizada, debe designar una región de origen. Si lo desea, puede elegir una o más regiones como regiones vinculadas. También puede optar por designar una región de origen sin ninguna región vinculada.

Cambiar la configuración de la agregación entre regiones puede afectar a las políticas de configuración. Al agregar una región vinculada, las políticas de configuración se aplican en esa región. Si la región es una región opcional, debe estar habilitada para que las políticas de configuración se apliquen allí. Por el contrario, al eliminar una región vinculada, las políticas de configuración dejan de tener efecto en esa región. En esa región, las cuentas mantienen la configuración que tenían cuando se eliminó la región vinculada. Puede cambiar esa configuración, pero debe hacerlo por separado en cada cuenta y región.

Si elimina o cambia la región de origen, se eliminarán las políticas de configuración y las asociaciones de políticas. Ya no podrá utilizar la configuración centralizada ni crear políticas de configuración en ninguna región. Las cuentas mantienen la configuración que tenían antes de que se cambiara o eliminara la región de origen. Puede cambiar esa configuración en cualquier momento, pero, como ya no utiliza la configuración centralizada, la configuración debe modificarse por separado en cada cuenta y región. Puede utilizar la configuración centralizada y volver a crear políticas de configuración si designa una nueva región de origen.

Para obtener más información acerca de la configuración centralizada, consulte Descripción de la configuración central en el CSPM de Security Hub.

Habilitación de agregación entre regiones

> **Note**
>
> La región de agregación ahora se denomina región de origen. Algunas operaciones de la API del CSPM de Security Hub aún utilizan el término anterior región de agregación.

Debe habilitar la agregación entre regiones desde la Región de AWS que desee designar como región de origen.

Para habilitar la agregación entre regiones, cree un recurso del CSPM de Security Hub que se denomina agregador de resultados. El recurso del agregador de resultados especifica su región de origen y las regiones vinculadas (si las hubiera).

No puedes usar una región Región de AWS que esté deshabilitada de forma predeterminada como región de origen. Para obtener una lista de regiones que están deshabilitadas de forma predeterminada, consulte Habilitar una región en la Referencia general de AWS.

Cuando activa la agregación entre regiones, puede especificar una o más regiones vinculadas si lo desea. También puede elegir si desea vincular automáticamente las nuevas regiones cuando el CSPM de Security Hub comience a admitirlas y usted ya se haya suscrito a estas.

Security Hub CSPM console

Cómo habilitar la agregación entre regiones

1. Abra la consola CSPM de AWS Security Hub en. https://console.aws.amazon.com/securityhub/
2. Con el Región de AWS selector, inicie sesión en la región que desee usar como región de agregación.
3. En el menú de navegación del CSPM de Security Hub, seleccione Configuración y, a continuación, Regiones.
4. En Agregación de resultados, elija Configuración de la agregación de resultados.

   De forma predeterminada, la región de origen aparece como Sin región de agregación.
5. En Región de agregación, seleccione la opción para designar la región actual como región de origen.
6. De forma opcional, en Regiones vinculadas, seleccione las regiones desde las que desea agregar datos.
7. Para agregar automáticamente los datos de nuevas regiones de la partición a medida que el CSPM de Security Hub las admita y usted se suscriba a ellas, seleccione Vincular futuras regiones.
8. Seleccione Save.

Security Hub CSPM API

Desde la región que desee utilizar como región de origen, use la operación `CreateFindingAggregator` de la API del CSPM de Security Hub. Si usa elAWS CLI, ejecute el comando create-finding-aggregator.

En `RegionLinkingMode`, elija una de las siguientes opciones:

- `ALL_REGIONS`: el CSPM de Security Hub agrega datos de todas las regiones. El CSPM de Security Hub también agrega datos de las nuevas regiones a medida que las admite y usted se suscribe a estas.
- `ALL_REGIONS_EXCEPT_SPECIFIED`: el CSPM de Security Hub agrega datos de todas las regiones, excepto aquellas que desee excluir. El CSPM de Security Hub también agrega datos de las nuevas regiones a medida que las admite y usted se suscribe a estas. Utilice `Regions` para proporcionar la lista de regiones que se van a excluir de la agregación.
- `SPECIFIED_REGIONS`: el CSPM de Security Hub agrega datos de una lista seleccionada de regiones. El CSPM de Security Hub no agrega automáticamente los datos de las nuevas regiones. Se utiliza `Regions` para proporcionar la lista de regiones desde las que agregar.
- `NO_REGIONS`: el CSPM de Security Hub no agrega datos si no selecciona ninguna región vinculada.

En el siguiente ejemplo, se configura la agregación entre regiones. La región de origen es este de EE. UU. (norte de Virginia). Las regiones vinculadas son Oeste de EE. UU. (Norte de California) y Oeste de EE. UU. (Oregón). Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$ aws securityhub create-finding-aggregator --region us-east-1 --region-linking-
mode SPECIFIED_REGIONS --regions us-west-1 us-west-2
```

Revisión de la configuración de agregación entre regiones

> **Note**
>
> La región de agregación ahora se denomina región de origen. Algunas operaciones de la API del CSPM de Security Hub aún utilizan el término anterior región de agregación.

Puede ver la configuración actual de agregación entre regiones en AWS Security Hub CSPM desde cualquier lugar. Región de AWS La configuración incluye la región de origen, las regiones vinculadas (si las hay) y si se vinculan automáticamente las nuevas regiones a medida que el CSPM de Security Hub las admita.

Las cuentas de miembro pueden ver la configuración de agregación entre regiones que configuró la cuenta de administrador.

Elija su método preferido y siga estos pasos para ver su configuración actual de agregación entre regiones.

Security Hub CSPM console

Para ver la configuración de agregación entre regiones (consola)

1. Abra la consola CSPM de AWS Security Hub en. https://console.aws.amazon.com/securityhub/
2. En el panel de navegación, elija Configuración y, luego, la pestaña Regiones.

Si la agregación entre regiones no está habilitada, la pestaña Regiones muestra la opción para habilitar la agregación entre regiones. Solo las cuentas de administrador y las cuentas independientes pueden habilitar la agregación entre regiones.

Si la agregación entre regiones está habilitada, la pestaña Regiones muestra la siguiente información:

- La región de origen
- Si se debe agregar de forma automática los resultados, la información, los estados de los controles y las puntuaciones de seguridad provenientes de las nuevas regiones que el CSPM de Security Hub admite y a las que usted se suscribe.
- La lista de regiones vinculadas (si se selecciona alguna)

Security Hub CSPM API

Para revisar la configuración de agregación entre regiones (API del CSPM de Security Hub)

Use la operación `GetFindingAggregator` de la API del CSPM de Security Hub. Si usa elAWS CLI, ejecute el comando get-finding-aggregator.

Al realizar la solicitud, proporcione el ARN del agregador de resultados. Para obtener el ARN del agregador de resultados, utilice la operación `ListFindingAggregators` o el comando list-finding-aggregators.

El siguiente ejemplo muestra la configuración de agregación entre regiones para el ARN del agregador de resultados especificado. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad

```
$aws securityhub get-finding-aggregator --finding-aggregator-
arn arn:aws:securityhub:us-east-1:222222222222:finding-aggregator/123e4567-
e89b-12d3-a456-426652340000
```

Actualización de la configuración de agregación entre regiones

> **Note**
>
> La región de agregación ahora se denomina región de origen. Algunas operaciones de la API del CSPM de Security Hub aún utilizan el término anterior región de agregación.

Puede actualizar su configuración actual de agregación entre regiones en AWS Security Hub CSPM cambiando las regiones vinculadas o la región de origen actual. También puede cambiar si desea agregar automáticamente los datos de los nuevos Regiones de AWS que sean compatibles con el CSPM de Security Hub.

Los cambios en la agregación entre regiones no se implementan en una región opcional hasta que habilite la región en su Cuenta de AWS. Las regiones que AWS se introdujeron el 20 de marzo de 2019 o con posterioridad son regiones que se suscriben de forma voluntaria.

Cuando dejas de agregar datos de una región vinculada, AWS Security Hub CSPM no elimina ningún dato agregado existente de esa región al que se pueda acceder en la región de origen.

No puede usar los procedimientos de actualización de esta sección para cambiar la región de origen. Para cambiar la región de origen, se debe hacer lo siguiente:

1. Detenga la agregación entre regiones. Para obtener instrucciones, consulte the section called “Detención de la agregación”.
2. Cambie a la región que desea que sea la nueva región de origen.
3. Habilitación de agregación entre regiones. Para obtener instrucciones, consulte the section called “Habilitación de agregación”.

Debe actualizar la configuración de agregación entre regiones desde la región de origen actual.

Security Hub CSPM console

Para cambiar las regiones vinculadas

1. Abra la consola CSPM de AWS Security Hub en. https://console.aws.amazon.com/securityhub/

   Inicie sesión en la región de agregación actual.
2. En el menú de navegación del CSPM de Security Hub, seleccione Configuración y, a continuación, Regiones.
3. Para la opción Agregación de resultados, seleccione Editar.
4. Para la opción Regiones vinculadas, actualice las regiones vinculadas seleccionadas.
5. Si es necesario, cambie la selección de Vincular regiones futuras. Esta configuración determina si el CSPM de Security Hub vincula automáticamente las nuevas regiones a medida que las admite y usted se suscribe a ellas.
6. Seleccione Save.

Security Hub CSPM API

Utilice la operación `UpdateFindingAggregator`. Si usa elAWS CLI, ejecute el comando update-finding-aggregator. Para identificar el agregador de resultados, debe proporcionar el ARN de este. Para obtener el ARN del agregador de resultados, utilice la operación `ListFindingAggregators` o el comando list-finding-aggregators.

Si el modo de enlace es `ALL_REGIONS_EXCEPT_SPECIFIED` o `SPECIFIED_REGIONS`, puede cambiar la lista de regiones excluidas o incluidas. Si quiere cambiar el modo de enlace de regiones a `NO_REGIONS`, no debe proporcionar una lista de regiones.

Al cambiar la lista de regiones excluidas o incluidas, debe proporcionar la lista completa con las actualizaciones. Por ejemplo, supongamos que actualmente agrega los resultados de Este de EE. UU. (Ohio) y desea agregar también los resultados de Oeste de EE. UU. (Oregón). Debe proporcionar una lista de `Regions` que contenga tanto el este de EE. UU. (Ohio) como el oeste de EE. UU. (Oregón).

En el siguiente ejemplo, se actualiza la agregación entre regiones para las regiones seleccionadas. El comando se ejecuta desde la región de origen actual, que es este de EE. UU. (norte de Virginia). Las regiones vinculadas son Oeste de EE. UU. (Norte de California) y Oeste

de EE. UU. (Oregón). Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
aws securityhub update-finding-aggregator --region us-east-1 --finding-
aggregator-arn arn:aws:securityhub:us-east-1:222222222222:finding-
aggregator/123e4567-e89b-12d3-a456-426652340000 --region-linking-mode
 SPECIFIED_REGIONS --regions us-west-1 us-west-2
```

Detención de la agregación entre regiones

> **Note**
>
> La región de agregación ahora se denomina región de origen. Algunas operaciones de la API del CSPM de Security Hub aún utilizan el término anterior región de agregación.

Si no quieres que AWS Security Hub CSPM agregue datos, puedes eliminar tu agregador de búsquedas. Como alternativa, puedes conservar tu agregador de búsquedas pero no vincular ninguno Regiones de AWS a la región de origen actualizando el agregador existente al modo de enlace. `NO_REGIONS`

Para cambiar su región de origen, debe eliminar su agregador de resultados actual y crear uno nuevo.

Al eliminar el agregador de resultados, el CSPM de Security Hub deja de agregar datos. No elimina ningún dato agregado existente de la región de origen.

Para eliminar el agregador de resultados (consola)

Puede eliminar su agregador de resultados únicamente desde la región de origen actual.

En las regiones distintas de la región de origen, el panel Agregación de resultados en la consola del CSPM de Security Hub muestra un mensaje en el que se indica que debe editar la configuración en la región de origen. Seleccione este mensaje para mostrar un enlace para cambiar a la región de origen.

Security Hub CSPM console

Para detener la agregación entre regiones (consola)

1. Abra la consola CSPM de AWS Security Hub en. https://console.aws.amazon.com/securityhub/
2. Asegúrese de que haya iniciado sesión en su región de origen actual.
3. En el menú de navegación del CSPM de Security Hub, seleccione Configuración y, a continuación, Regiones.
4. En Agregación de resultados, seleccione Editar.
5. En Región de agregación, elija Sin región de agregación.
6. Seleccione Save.
7. En el cuadro de diálogo de confirmación, en el campo de confirmación, escriba **`Confirm`**.
8. Elija Confirmar.

Security Hub CSPM API

Use la operación `DeleteFindingAggregator` de la API del CSPM de Security Hub. Si está utilizando elAWS CLI, ejecute el `delete-finding-aggregator`comando.

Para identificar el agregador de resultados que va a eliminar, proporcione el ARN de este. Para obtener el ARN del agregador de resultados, utilice la operación `ListFindingAggregators` o el comando `list-finding-aggregators`.

En el siguiente ejemplo, se elimina el agregador de resultados. El comando se ejecuta desde la región de origen actual, que es este de EE. UU. (norte de Virginia). Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$aws securityhub delete-finding-aggregator arn:aws:securityhub:us-
east-1:222222222222:finding-aggregator/123e4567-e89b-12d3-a456-426652340000 --
region us-east-1
```

Descripción de los estándares de seguridad en el CSPM de Security Hub

En AWS Security Hub CSPM, un estándar de seguridad es un conjunto de requisitos que se basan en los marcos normativos, las mejores prácticas del sector o las políticas de la empresa. Para obtener información sobre los estándares que admite actualmente el CSPM de Security Hub, incluidos los controles de seguridad que se aplican a cada uno, consulte Referencia de estándares para el CSPM de Security Hub.

Cuando habilita un estándar, el CSPM de Security Hub habilita automáticamente todos los controles que se aplican a ese estándar. El CSPM de Security Hub ejecuta después las comprobaciones de seguridad correspondientes a esos controles, lo que genera resultados del CSPM de Security Hub. Puede desactivar controles individuales y volver a habilitarlos cuando sea necesario. También puede desactivar un estándar por completo. Si desactiva un estándar, el CSPM de Security Hub deja de ejecutar comprobaciones de seguridad respecto a los controles asociados a ese estándar. En ese caso, ya no se generan resultados para esos controles.

Además de los resultados, el CSPM de Security Hub genera un puntaje de seguridad para cada estándar que habilite. El puntaje se basa en el estado de los controles que se aplican al estándar. Si configura una región de agregación, el puntaje de seguridad de un estándar refleja el estado de los controles en todas las regiones vinculadas. Si es el administrador del CSPM de Security Hub para una organización, el puntaje refleja el estado de los controles de todas las cuentas de la organización. Para obtener más información, consulte Calcular las puntuaciones de seguridad.

Para revisar y administrar los estándares, puede usar la consola del CSPM de Security Hub o la API del CSPM de Security Hub. En la consola, la página Estándares de seguridad muestra todos los estándares de seguridad que el CSPM de Security Hub admite actualmente. Esta página incluye una descripción de cada estándar y el estado actual del estándar. Si habilita un estándar, también puede usar esta página para acceder a detalles adicionales del estándar. Por ejemplo, puede revisar lo siguiente:

- El puntaje de seguridad actual del estándar.
- Las estadísticas agregadas de los controles que se aplican al estándar.
- La lista de controles que se aplican al estándar y que están habilitados actualmente, incluido el estado de cumplimiento de cada control.
- La lista de controles que se aplican al estándar pero que están desactivados actualmente.

Para un análisis más detallado, puede filtrar y ordenar los datos y profundizar en los detalles de los controles individuales que se aplican al estándar.

Puede habilitar los estándares de forma individual para una sola cuenta y. Región de AWS Sin embargo, para ahorrar tiempo y evitar desviaciones de configuración en entornos con múltiples cuentas y regiones, recomendamos usar una configuración centralizada para habilitar y administrar los estándares. Con una configuración centralizada, el administrador delegado del CSPM de Security Hub puede crear políticas que definan cómo configurar un estándar en varias cuentas y regiones.

Temas

- Referencia de estándares para el CSPM de Security Hub
- Habilitación de un estándar de seguridad
- Revisión de los detalles de un estándar de seguridad
- Desactivación de estándares de seguridad habilitados automáticamente
- Deshabilitación de un estándar de seguridad

Referencia de estándares para el CSPM de Security Hub

En AWS Security Hub CSPM, un estándar de seguridad es un conjunto de requisitos que se basa en los marcos normativos, las mejores prácticas del sector o las políticas de la empresa. El CSPM de Security Hub asigna estos requisitos a controles y ejecuta comprobaciones de seguridad respecto a estos para verificar si se cumplen los requisitos del estándar. Cada estándar incluye varios controles.

El CSPM de Security Hub admite actualmente los siguientes estándares:

- AWS Mejores prácticas de seguridad fundamentales: Desarrollado por profesionales del sector AWS y por profesionales del sector, este estándar es una recopilación de las mejores prácticas de seguridad para las organizaciones, independientemente del sector o el tamaño. Proporciona un conjunto de controles que detectan cuándo usted Cuentas de AWS y sus recursos se desvían de las prácticas recomendadas de seguridad. También ofrece orientación prescriptiva sobre cómo mejorar y mantener la posición de seguridad.
- Mejores prácticas de seguridad de la IA: desarrollada por expertos en AWS seguridad, esta norma proporciona un conjunto seleccionado de controles que detectan si los recursos de IA desplegados no se ajustan a las prácticas recomendadas de seguridad. Le ayuda a identificar las áreas en las que sus cargas de trabajo de IA se desvían de las configuraciones de seguridad recomendadas, y abarca ámbitos como el aislamiento de la red, el cifrado, la ubicación de las VPC y AWS KMS el uso de claves.

- AWS Etiquetado de recursos: desarrollado por Security Hub CSPM, este estándar puede ayudarlo a determinar si sus recursos tienen etiquetas. AWS Una etiqueta es un par clave-valor que actúa como metadatos para un recurso. AWS Las etiquetas pueden ayudarlo a identificar, clasificar, administrar y buscar recursos. AWS Por ejemplo, puede usar etiquetas para categorizar recursos por finalidad, propietario o entorno.
- CIS AWS Foundations Benchmark: desarrollado por el Center for Internet Security (CIS), este estándar proporciona pautas de configuración seguras para AWS. Especifica un conjunto de directrices de configuración de seguridad y prácticas recomendadas para un subconjunto de Servicios de AWS recursos, haciendo hincapié en los parámetros básicos, comprobables e independientes de la arquitectura. Las directrices incluyen procedimientos claros, paso a paso, para la implementación y la evaluación.
- Revisión 5 de NIST SP 800-53: este estándar se alinea con los requisitos del National Institute of Standards and Technology (NIST) para proteger la confidencialidad, la integridad y la disponibilidad de los sistemas de información y de los recursos críticos. El marco asociado generalmente se aplica a U.S las agencias federales u organizaciones que trabajan con las agencias federales o los sistemas de información U.S. No obstante, las organizaciones privadas también pueden usar estos requisitos como marco de orientación.
- Revisión 2 del NIST SP 800-171: esta norma se ajusta a las recomendaciones y requisitos de seguridad del NIST para proteger la confidencialidad de la información no clasificada controlada (CUI) en los sistemas y organizaciones que no forman parte del gobierno federal. U.S La CUI es información que no cumple con los criterios gubernamentales de clasificación, pero que se considera confidencial y es creada o poseída por el gobierno federal u otras entidades en nombre del gobierno federal U.S. U.S
- PCI DSS: este estándar se alinea con el marco de cumplimiento del Estándar de seguridad de datos de la industria de tarjetas de pago (PCI-DSS), definido por el PCI Security Standards Council (SSC). El marco proporciona un conjunto de reglas y directrices para manejar de forma segura la información de tarjetas de crédito y de débito. El marco se aplica, por lo general, a organizaciones que almacenan, tratan o transmiten datos de titulares de tarjetas.
- Service-managed estándar, AWS Control Tower — Este estándar le ayuda a configurar los controles de detección proporcionados por Security Hub CSPM desde. AWS Control Tower AWS Control Tower ofrece una forma sencilla de configurar y administrar un entorno de AWS cuentas múltiples, siguiendo las mejores prácticas prescriptivas.

Los estándares y controles del CSPM de Security Hub no garantizan el cumplimiento de marcos normativos ni de auditorías. En su lugar, proporcionan una forma de evaluar y supervisar el estado

de los recursos y Cuentas de AWS . Recomendamos habilitar cada estándar que resulte pertinente para las necesidades de su negocio, su sector o su caso de uso.

Los controles individuales se pueden aplicar a más de un estándar. Si habilita varios estándares, recomendamos habilitar también los resultados consolidados de controles. Si hace esto, el CSPM de Security Hub genera un único resultado por cada control, incluso si el control se aplica a más de un estándar. Si no activa los resultados consolidados de controles, el CSPM de Security Hub genera un resultado independiente por cada estándar habilitado al que se aplique un control. Por ejemplo, si habilita dos estándares y un control se aplica a ambos, recibe dos resultados separados para el control, uno por cada estándar. Si habilita los resultados consolidados de controles, recibe un único resultado para el control. Para obtener más información, consulte Resultados de control consolidados.

Referencia detallada por estándar

- AWS Estándar fundamental de mejores prácticas de seguridad en Security Hub (CSPM)
- Estándar de mejores prácticas de seguridad de IA en Security Hub (CSPM)
- AWS Estándar de etiquetado de recursos en Security Hub CSPM
- CIS AWS Aspectos básicos y comparativos del CSPM de Security Hub
- Revisión 5 de NIST SP 800-53 en el CSPM de Security Hub
- Revisión 2 de NIST SP 800-171 en el CSPM de Security Hub
- PCI DSS en el CSPM de Security Hub
- Service-managed estándares en Security Hub CSPM

AWS Estándar fundamental de mejores prácticas de seguridad en Security Hub (CSPM)

Desarrollado por profesionales del sector AWS y por profesionales del sector, el estándar AWS Fundational Security Best Practices (FSBP) es una recopilación de las mejores prácticas de seguridad para las organizaciones, independientemente del sector o tamaño de la organización. Proporciona un conjunto de controles que detectan cuándo Cuentas de AWS y los recursos se desvían de las mejores prácticas de seguridad. También ofrece directrices prescriptivas sobre cómo mejorar y mantener la posición de seguridad de la organización.

En AWS Security Hub CSPM, el estándar AWS fundamental de prácticas recomendadas de seguridad incluye controles que evalúan de forma continua sus cargas y las de trabajo, Cuentas de AWS y ayudan a identificar las áreas que se desvían de las prácticas recomendadas de seguridad.

Los controles incluyen las mejores prácticas de seguridad para los recursos de varios Servicios de AWS. A cada control se le asigna una categoría que refleja la función de seguridad a la que se aplica el control. Para ver la lista de categorías y obtener más detalles, consulte Categorías de controles.

Controles que se aplican al estándar

En la siguiente lista se especifican los controles de CSPM AWS de Security Hub que se aplican al estándar AWS fundamental de prácticas recomendadas de seguridad (v1.0.0). Para revisar los detalles de un control, seleccione el control.

[Account.1] La información de contacto de seguridad debe proporcionarse para unCuenta de AWS

[ACM.1] ACM-issued Los certificados importados y renovados deben renovarse después de un período de tiempo específico

[ACM.2] Los certificados RSA gestionados por ACM deben utilizar una longitud de clave de al menos 2048 bits

[APIGateway.1] El registro de ejecución de API y REST de WebSocket API Gateway deben estar habilitados.

[APIGateway.2] Las etapas de la API REST de API Gateway deben configurarse para usar certificados SSL para la autenticación de backend

[APIGateway.3] Las etapas de la API REST de API Gateway deben tener AWS X-Ray rastreo habilitado

[APIGateway.4] API Gateway debe estar asociada a una ACL web de WAF

[APIGateway.5] Los datos de la caché de la API REST de API Gateway deben cifrarse en reposo

[APIGateway.8] Las rutas de API Gateway deben especificar un tipo de autorización

[APIGateway.9] El registro de acceso debe configurarse para las etapas V2 de API Gateway

[APIGateway.10] Las integraciones de API Gateway V2 deben usar HTTPS para las conexiones privadas

[APIGateway.11] Los nombres de dominio de API Gateway deben usar las políticas de seguridad recomendadas

[AppSync.1]AWS AppSyncLas cachés de las API deben estar cifradas en reposo

[AppSync.2]AWS AppSyncdebe tener habilitado el registro a nivel de campo

[AppSync.5]AWS AppSyncLas API de GraphQL no deben autenticarse con claves de API

[AppSync.6]AWS AppSyncLas cachés de las API deben cifrarse en tránsito

[Athena.4] Los grupos de trabajo de Athena deberían tener habilitado el registro

[AutoScaling.1] Los grupos de Auto Scaling asociados a un balanceador de cargas deben usar comprobaciones de estado del ELB

[AutoScaling.2] El grupo Amazon EC2 Auto Scaling debe cubrir varias zonas de disponibilidad

[AutoScaling.3] Las configuraciones de lanzamiento grupal de Auto Scaling deberían configurar las instancias EC2 para que requieran la versión 2 del Servicio de Metadatos de Instancia (IMDSv2)

[Autoscaling.5] Las instancias de Amazon EC2 lanzadas mediante configuraciones de lanzamiento grupal de Auto Scaling no deben tener direcciones IP públicas

[AutoScaling.6] Los grupos de Auto Scaling deben usar varios tipos de instancias en múltiples zonas de disponibilidad

[AutoScaling.9] Los grupos de Amazon EC2 Auto Scaling deben utilizar las plantillas de lanzamiento de Amazon EC2

[Backup.1]AWS Backuplos puntos de recuperación deben estar cifrados en reposo

[BedrockAgentCore.1] Los AgentCore tiempos de ejecución de Bedrock deben configurarse con el modo de red VPC

[BedrockAgentCore.2] Bedrock AgentCore Gateways debería requerir autorización para las solicitudes entrantes

[BedrockAgentCore.5] Los navegadores AgentCore personalizados de Bedrock no deberían usar el modo de red pública

[BedrockAgentCore.6] Los navegadores AgentCore personalizados de Bedrock deberían tener habilitada la grabación de sesiones

[CloudFormation.3] las CloudFormation pilas deben tener habilitada la protección de terminación

[CloudFormation.4] las CloudFormation pilas deben tener funciones de servicio asociadas

[CloudFront.1] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado

[CloudFront.3] CloudFront las distribuciones deben requerir el cifrado durante el tránsito

[CloudFront.4] CloudFront las distribuciones deben tener configurada la conmutación por error de origen

[CloudFront.5] CloudFront las distribuciones deben tener habilitado el registro

[CloudFront.6] CloudFront las distribuciones deben tener WAF activado

[CloudFront.7] CloudFront las distribuciones deben usar certificados personalizados SSL/TLS

[CloudFront.8] CloudFront las distribuciones deben usar el SNI para atender las solicitudes HTTPS

[CloudFront.9] CloudFront las distribuciones deben cifrar el tráfico para convertirlo en orígenes personalizados

[CloudFront.10] CloudFront las distribuciones no deben usar protocolos SSL obsoletos entre ubicaciones de borde y orígenes personalizados

[CloudFront.12] CloudFront las distribuciones no deben apuntar a orígenes de S3 inexistentes

[CloudFront.13] CloudFront las distribuciones deben usar el control de acceso al origen

[CloudFront.15] CloudFront las distribuciones deben usar la política de seguridad TLS recomendada

[CloudFront.16] CloudFront las distribuciones deben usar el control de acceso de origen para los orígenes de las URL de las funciones de Lambda

[CloudFront.17] CloudFront las distribuciones deben usar grupos de claves confiables para las URL y cookies firmadas

[CloudTrail.1] CloudTrail debe estar habilitado y configurado con al menos un registro multirregional que incluya eventos de administración de lectura y escritura

[CloudTrail.2] CloudTrail debe tener activado el cifrado en reposo

[CloudTrail.4] La validación del archivo de CloudTrail registro debe estar habilitada

[CloudTrail.5] los CloudTrail senderos deben estar integrados con Amazon CloudWatch Logs

[CodeBuild.1] Las URL del repositorio fuente de CodeBuild Bitbucket no deben contener credenciales confidenciales

[CodeBuild.2] las variables de entorno CodeBuild del proyecto no deben contener credenciales de texto claro

[CodeBuild.3] Los registros de CodeBuild S3 deben estar cifrados

[CodeBuild.4] los entornos de CodeBuild proyectos deben tener un registroAWS ConfigDuración

[CodeBuild.7] las exportaciones de grupos de CodeBuild informes deben cifrarse en reposo

[Cognito.2] Los grupos de identidades de Cognito no deben permitir identidades no autenticadas

[Cognito.3] Las políticas de contraseñas para los grupos de usuarios de Cognito deben tener configuraciones sólidas

[Cognito.4] Los grupos de usuarios de Cognito deben tener activada la protección contra amenazas y el modo de aplicación con todas las funciones para la autenticación personalizada

[Cognito.5] La MFA debe estar habilitada para los grupos de usuarios de Cognito

[Cognito.6] Los grupos de usuarios de Cognito deben tener habilitada la protección contra la eliminación

[Config.1] AWS Config deben estar habilitados y usar la función vinculada al servicio para el registro de recursos

[Connect.2] Las instancias de Connect Customer deben tener el CloudWatch registro habilitado

[DataFirehose.1] Los flujos de entrega de Firehose deben cifrarse en reposo

[DataSync.1] DataSync las tareas deberían tener el registro activado

[DMS.1] Las instancias de replicación de Database Migration Service no deben ser públicas

[DMS.6] Las instancias de replicación de DMS deben tener habilitada la actualización automática de las versiones secundarias

[DMS.7] Las tareas de replicación del DMS para la base de datos de destino deben tener el registro habilitado

[DMS.8] Las tareas de replicación del DMS para la base de datos de origen deben tener el registro activado

[DMS.9] Los puntos finales del DMS deben usar SSL

[DMS.10] Los puntos finales de DMS para las bases de datos de Neptune deben tener habilitada la autorización de IAM

[DMS.11] Los puntos finales de DMS para MongoDB deben tener un mecanismo de autenticación habilitado

[DMS.12] Los puntos finales de DMS para Redis OSS deben tener el TLS habilitado

[DMS.13] Las instancias de replicación de DMS deben configurarse para usar varias zonas de disponibilidad

[DocumentDB.1] Los clústeres de Amazon DocumentDB deben cifrarse en reposo

[DocumentDB.2] Los clústeres de Amazon DocumentDB deben tener un período de retención de copias de seguridad adecuado

[DocumentDB.3] Las instantáneas de clústeres manuales de Amazon DocumentDB no deben ser públicas

[DocumentDB.4] Los clústeres de Amazon DocumentDB deben publicar los registros de auditoría en Logs CloudWatch

[DocumentDB.5] Los clústeres de Amazon DocumentDB deben tener habilitada la protección contra eliminaciones

[DocumentDB.6] Los clústeres de Amazon DocumentDB deben cifrarse en tránsito

[DynamoDB.1] Las tablas de DynamoDB deberían escalar automáticamente la capacidad en función de la demanda

[DynamoDB.2] Las tablas de DynamoDB deben tener habilitada la recuperación puntual

[DynamoDB.3] Los clústeres de DynamoDB Accelerator (DAX) deben cifrarse en reposo

[DynamoDB.6] Las tablas de DynamoDB deben tener habilitada la protección de eliminación

[DynamoDB.7] Los clústeres de DynamoDB Accelerator deben cifrarse en tránsito

[EC2.1] Las instantáneas de Amazon EBS no deben configurarse para que se puedan restaurar públicamente

[EC2.2] Los grupos de seguridad predeterminados de VPC no deben permitir el tráfico entrante o saliente

[EC2.3] Los volúmenes adjuntos de Amazon EBS deben cifrarse en reposo

[EC2.4] Las instancias EC2 detenidas deben eliminarse después de un período de tiempo específico

[EC2.6] El registro de flujo de VPC debe estar habilitado en todas las VPC

[EC2.7] El cifrado predeterminado de EBS debe estar habilitado

[EC2.8] Las instancias EC2 deben utilizar la versión 2 del servicio de metadatos de instancia (IMDSv2)

[EC2.9] Las instancias de Amazon EC2 no deben tener una dirección IPv4 pública

[EC2.10] Amazon EC2 debe configurarse para utilizar los puntos de enlace de VPC que se crean para el servicio Amazon EC2

[EC2.15] Las subredes de Amazon EC2 no deben asignar automáticamente direcciones IP públicas

[EC2.16] Se deben eliminar las listas de control de acceso a la red no utilizadas

[EC2.17] Las instancias de Amazon EC2 no deben usar varios ENI

[EC2.18] Los grupos de seguridad solo deben permitir el tráfico entrante sin restricciones en los puertos autorizados

[EC2.19] Los grupos de seguridad no deben permitir el acceso irrestricto a los puertos de alto riesgo

[EC2.20] Ambos túneles VPN para un AWS Site-to-Site La conexión VPN debería estar activa

[EC2.21] Las ACL de red no deberían permitir la entrada desde la versión 0.0.0. 0/0 al puerto 22 o al puerto 3389

[EC2.23] Amazon EC2 Transit Gateways no debe aceptar automáticamente las solicitudes de adjuntos de VPC

[EC2.24] No se deben utilizar los tipos de instancias paravirtuales de Amazon EC2

[EC2.25] Las plantillas de lanzamiento de Amazon EC2 no deben asignar direcciones IP públicas a las interfaces de red

[EC2.51] Los puntos finales EC2 Client VPN deben tener habilitado el registro de conexiones de clientes

[EC2.55] Las VPC deben configurarse con un punto final de interfaz para la API de ECR

[EC2.56] Las VPC deben configurarse con un punto final de interfaz para Docker Registry

[EC2.57] Las VPC deben configurarse con un punto final de interfaz para Systems Manager

[EC2.58] Las VPC deben configurarse con un punto final de interfaz para los contactos de Systems Manager Incident Manager

[EC2.60] Las VPC deben configurarse con un punto final de interfaz para Systems Manager Incident Manager

[EC2.170] Las plantillas de lanzamiento de EC2 deben utilizar la versión 2 del servicio de metadatos de instancias (IMDSv2)

[EC2.171] Las conexiones VPN de EC2 deberían tener el registro habilitado

[EC2.172] La configuración de acceso público del bloque de VPC de EC2 debería bloquear el tráfico de la puerta de enlace de Internet

[EC2.173] Las solicitudes de EC2 Spot Fleet con parámetros de lanzamiento deberían permitir el cifrado de los volúmenes de EBS adjuntos

[EC2.180] Las interfaces de red EC2 deberían tener habilitada source/destination la verificación

[EC2.181] Las plantillas de lanzamiento de EC2 deberían permitir el cifrado de los volúmenes de EBS adjuntos

[EC2.182] La configuración de bloqueo de acceso público debe estar habilitada para las instantáneas de Amazon EBS

[EC2.183] Las conexiones VPN de EC2 deben utilizar el protocolo IKEv2

[ECR.1] Los repositorios privados de ECR deben tener configurado el escaneo de imágenes

[ECR.2] Los repositorios privados de ECR deben tener configurada la inmutabilidad de etiquetas

[ECR.3] Los repositorios de ECR deben tener configurada al menos una política de ciclo de vida

[ECS.2] Los servicios de ECS no deberían tener direcciones IP públicas asignadas automáticamente

[ECS.3] Las definiciones de tareas de ECS no deben compartir el espacio de nombres del proceso del host

[ECS.4] Los contenedores ECS deben ejecutarse sin privilegios

[ECS.5] Las definiciones de tareas de ECS deben configurar los contenedores para que se limiten al acceso de solo lectura a los sistemas de archivos raíz

[ECS.8] Los secretos no deben transmitirse como variables de entorno de contenedores

[ECS.9] Las definiciones de tareas de ECS deben tener una configuración de registro

[ECS.10] Los servicios Fargate de ECS deberían ejecutarse en la última versión de la plataforma Fargate

[ECS.12] Los clústeres de ECS deben usar Container Insights

[ECS.16] Los conjuntos de tareas de ECS no deben asignar automáticamente direcciones IP públicas

[ECS.18] Las definiciones de tareas de ECS deben utilizar el cifrado en tránsito para los volúmenes de EFS

[ECS.19] Los proveedores de capacidad de ECS deberían tener habilitada la protección de terminación gestionada

[ECS.20] Las definiciones de tareas de ECS deben configurar a los usuarios no root en las definiciones de contenedores de Linux

[ECS.21] Las definiciones de tareas de ECS deberían configurar a los usuarios no administradores en las definiciones de contenedores de Windows

[EFS.1] Elastic File System debe configurarse para cifrar los datos de los archivos en reposo mediante AWS KMS

[EFS.2] Los volúmenes de Amazon EFS deben figurar en los planes de copia de seguridad

[EFS.3] Los puntos de acceso EFS deben exigir un directorio raíz

[EFS.4] Los puntos de acceso EFS deben exigir la identidad del usuario

[] Los sistemas de archivos EFS deben tener habilitadas las copias de seguridad automáticas EFS.7

[EFS.8] Los sistemas de archivos EFS deben cifrarse en reposo

[EKS.1] Los puntos finales del clúster EKS no deben ser de acceso público

[EKS.2] Los clústeres de EKS deben ejecutarse en una versión de Kubernetes compatible

[EKS.3] Los clústeres de EKS deben usar secretos de Kubernetes cifrados

[EKS.8] Los clústeres de EKS deben tener habilitado el registro de auditoría

[EKS.9] Los grupos de nodos de EKS deben ejecutarse en una versión de Kubernetes compatible

[ElastiCache.1] ElastiCache (Redis OSS) los clústeres deben tener habilitadas las copias de seguridad automáticas

[ElastiCache.2] ElastiCache los clústeres deberían tener habilitadas las actualizaciones automáticas de las versiones secundarias

[ElastiCache.3] los grupos de ElastiCache replicación deberían tener habilitada la conmutación por error automática

[ElastiCache.4] los grupos de ElastiCache replicación deben cifrarse en reposo

[ElastiCache.5] los grupos de ElastiCache replicación deben cifrarse en tránsito

[ElastiCache.6] ElastiCache (Redis OSS) Los grupos de replicación de versiones anteriores deberían tener habilitada la autenticación de Redis OSS

[ElastiCache.7] los ElastiCache clústeres no deben usar el grupo de subredes predeterminado

[ElasticBeanstalk.1] Los entornos de Elastic Beanstalk deberían tener habilitados los informes de estado mejorados

[ElasticBeanstalk.2] Las actualizaciones de la plataforma gestionada de Elastic Beanstalk deben estar habilitadas

[ElasticBeanstalk.3] Elastic Beanstalk debería transmitir los registros a CloudWatch

[ELB.1] El balanceador de carga de aplicaciones debe configurarse para redirigir todas las solicitudes HTTP a HTTPS

[ELB.2] Los balanceadores de carga clásicos con SSL/HTTPS oyentes deben usar un certificado proporcionado por AWS Gestor de certificados

[ELB.3] Los oyentes de Classic Load Balancer deben configurarse con terminación HTTPS o TLS

[ELB.4] El balanceador de carga de aplicaciones debe configurarse para eliminar los encabezados http no válidos

[ELB.5] El registro de los balanceadores de carga clásicos y de aplicaciones debería estar activado

[ELB.6] Los balanceadores de cargas de aplicaciones, puertas de enlace y red deben tener habilitada la protección contra eliminaciones

[ELB.7] Los balanceadores de carga clásicos deben tener activado el drenaje de conexiones

[ELB.8] Los balanceadores de carga clásicos con receptores SSL deben usar una política de seguridad predefinida que sea sólida AWS Config Duración

[ELB.9] Los balanceadores de carga clásicos deben tener habilitado el balanceo de cargas entre zonas

[ELB.10] El balanceador de carga clásico debe abarcar varias zonas de disponibilidad

[ELB.12] El balanceador de carga de aplicaciones debe configurarse con el modo defensivo o de mitigación de desincronización más estricto

[ELB.13] Los balanceadores de carga de aplicaciones, redes y puertas de enlace deben abarcar varias zonas de disponibilidad

[ELB.14] El balanceador de carga clásico debe configurarse con el modo defensivo o de mitigación de desincronización más estricto

[ELB.17] Los balanceadores de cargas de aplicaciones y redes con oyentes deben usar las políticas de seguridad recomendadas

[ELB.18] Los oyentes del balanceador de cargas de red y aplicaciones deben usar protocolos seguros para cifrar los datos en tránsito

[ELB.21] Los grupos destinatarios de Application and Network Load Balancer deben utilizar protocolos de control de estado cifrados

[ELB.22] Los grupos objetivo del ELB deben usar protocolos de transporte cifrados

[EMR.1] Los nodos principales del clúster de Amazon EMR no deben tener direcciones IP públicas

[EMR.2] La configuración de acceso público del bloque Amazon EMR debe estar habilitada

[EMR.3] Las configuraciones de seguridad de Amazon EMR deben cifrarse en reposo

[EMR.4] Las configuraciones de seguridad de Amazon EMR deben cifrarse en tránsito

[ES.1] Los dominios de Elasticsearch deben tener habilitado el cifrado en reposo

[ES.2] Los dominios de Elasticsearch no deben ser de acceso público

[ES.3] Los dominios de Elasticsearch deben cifrar los datos enviados entre nodos

[ES.4] Debería estar habilitado el registro de errores de dominio de Elasticsearch en Logs CloudWatch

[ES.5] Los dominios de Elasticsearch deben tener habilitado el registro de auditoría

[ES.6] Los dominios de Elasticsearch deben tener al menos tres nodos de datos

[ES.7] Los dominios de Elasticsearch deben configurarse con al menos tres nodos maestros dedicados

[ES.8] Las conexiones a los dominios de Elasticsearch deben cifrarse con la política de seguridad TLS más reciente

[EventBridge.3] los autobuses de eventos EventBridge personalizados deben tener adjunta una política basada en los recursos

[FSx.1] FSx para sistemas de archivos OpenZFS debe configurarse para copiar etiquetas en copias de seguridad y volúmenes

[FSx.2] Los sistemas de archivos FSx for Lustre deben configurarse para copiar etiquetas a las copias de seguridad

[FSx.3] FSx para sistemas de archivos OpenZFS debe configurarse para su implementación Multi-AZ

[FSx.4] FSx para sistemas de archivos NetApp ONTAP debe configurarse para su implementación Multi-AZ

[FSx.5] Los sistemas de archivos FSx for Windows File Server deben configurarse para Multi-AZ su implementación

[Glue.3]AWS GlueLas transformaciones de aprendizaje automático deben cifrarse en reposo

[Glue.4]AWS GlueLos trabajos de Spark deberían ejecutarse en versiones compatibles deAWS Glue

[GuardDuty.1] GuardDuty debería estar activado

[GuardDuty.5] La monitorización del registro de auditoría de GuardDuty EKS debe estar habilitada

[GuardDuty.6] GuardDuty La protección Lambda debe estar habilitada

[GuardDuty.7] La monitorización del tiempo de ejecución de GuardDuty EKS debe estar habilitada

[GuardDuty.8] La protección contra GuardDuty malware para EC2 debe estar habilitada

[GuardDuty.9] La protección GuardDuty RDS debe estar habilitada

[GuardDuty.10] La protección GuardDuty S3 debe estar habilitada

[GuardDuty.11] La monitorización del GuardDuty tiempo de ejecución debe estar habilitada

[GuardDuty.12] La monitorización del tiempo de ejecución de GuardDuty ECS debe estar habilitada

[GuardDuty.13] La monitorización del tiempo de ejecución de GuardDuty EC2 debe estar habilitada

[IAM.1] Las políticas de IAM no deberían permitir todos los privilegios administrativos «*»

[IAM.2] Los usuarios de IAM no deberían tener políticas de IAM adjuntas

[IAM.3] Las claves de acceso de los usuarios de IAM deben rotarse cada 90 días o menos

[IAM.4] La clave de acceso del usuario raíz de IAM no debería existir

[IAM.5] La MFA debe estar habilitada para todos los usuarios de IAM que tengan una contraseña de consola

[IAM.6] La MFA de hardware debe estar habilitada para el usuario root

[IAM.7] Las políticas de contraseñas para los usuarios de IAM deben tener configuraciones sólidas

[IAM.8] Se deben eliminar las credenciales de usuario de IAM no utilizadas

[IAM.21] Las políticas de IAM gestionadas por el cliente que cree no deberían permitir acciones comodín en los servicios

[Inspector.1] El escaneo EC2 de Amazon Inspector debe estar activado

[Inspector.2] El escaneo ECR de Amazon Inspector debe estar activado

[Inspector.3] El escaneo de código Lambda de Amazon Inspector Lambda debe estar activado

[Inspector.4] El escaneo estándar de Amazon Inspector Lambda debe estar activado

[Kinesis.1] Las transmisiones de Kinesis deben cifrarse en reposo

[Kinesis.3] Las transmisiones de Kinesis deben tener un período de retención de datos adecuado

[KMS.1] Las políticas gestionadas por los clientes de IAM no deberían permitir acciones de descifrado en todas las claves de KMS

[KMS.2] Los directores de IAM no deberían tener políticas integradas de IAM que permitan realizar acciones de descifrado en todas las claves de KMS

[KMS.3]AWS KMS keysno se debe eliminar involuntariamente

[KMS.5] Las claves KMS no deben ser de acceso público

[Lambda.1] Las políticas de las funciones de Lambda deberían prohibir el acceso público

[Lambda.2] Las funciones de Lambda deben usar los tiempos de ejecución compatibles

[Lambda.5] Las funciones de VPC Lambda deben funcionar en varias zonas de disponibilidad

[Macie.1] Amazon Macie debería estar activado

[Macie.2] La detección automática de datos confidenciales por parte de Macie debería estar habilitada

[MQ.2] Los corredores de ActiveMQ deben transmitir los registros de auditoría a CloudWatch

[MSK.1] Los clústeres de MSK deben cifrarse en tránsito entre los nodos de intermediación

[MSK.3] Los conectores MSK Connect deben estar cifrados en tránsito

[MSK.4] Los clústeres de MSK deben tener el acceso público deshabilitado

[MSK.5] Los conectores MSK deben tener el registro activado

[MSK.6] Los clústeres de MSK deberían deshabilitar el acceso no autenticado

[Neptune.1] Los clústeres de bases de datos de Neptune deben cifrarse en reposo

[Neptune.2] Los clústeres de bases de datos de Neptune deberían publicar registros de auditoría en Logs CloudWatch

[Neptune.3] Las instantáneas del clúster de base de datos de Neptune no deben ser públicas

[Neptune.4] Los clústeres de base de datos de Neptune deben tener habilitada la protección contra eliminación

[Neptune.5] Los clústeres de Neptune DB deberían tener habilitadas las copias de seguridad automatizadas

[Neptune.6] Las instantáneas del clúster de base de datos de Neptune deben cifrarse en reposo

[Neptune.7] Los clústeres de base de datos de Neptune deben tener habilitada la autenticación de bases de datos de IAM

[Neptune.8] Los clústeres de bases de datos de Neptune deben configurarse para copiar etiquetas a las instantáneas

[NetworkFirewall.2] El registro de Network Firewall debe estar habilitado

[NetworkFirewall.3] Las políticas de Network Firewall deben tener asociado al menos un grupo de reglas

[NetworkFirewall.4] La acción sin estado predeterminada para las políticas de Network Firewall debe ser eliminar o reenviar paquetes completos

[NetworkFirewall.5] La acción sin estado predeterminada para las políticas de Network Firewall debe ser eliminar o reenviar paquetes fragmentados

[NetworkFirewall.6] El grupo de reglas de Stateless Network Firewall no debe estar vacío

[NetworkFirewall.9] Los firewalls de Network Firewall deben tener habilitada la protección de eliminación

[NetworkFirewall.10] Los firewalls de Network Firewall deben tener habilitada la protección contra cambios de subred

[Opensearch.1] OpenSearch los dominios deben tener activado el cifrado en reposo

[Opensearch.2] OpenSearch los dominios no deben ser de acceso público

[Opensearch.3] OpenSearch los dominios deben cifrar los datos enviados entre nodos

[Opensearch.4] El registro de errores de OpenSearch dominio en Logs debe estar habilitado CloudWatch

[Opensearch.5] OpenSearch los dominios deben tener activado el registro de auditoría

[Opensearch.6] OpenSearch los dominios deben tener al menos tres nodos de datos

[Opensearch.7] OpenSearch los dominios deben tener habilitado un control de acceso detallado

[Opensearch.8] Las conexiones a los OpenSearch dominios deben cifrarse con la última política de seguridad de TLS

[Opensearch.10] OpenSearch los dominios deben tener instalada la última actualización de software

[PCA.1]AWS Privada CALa autoridad emisora de certificados raíz debe estar deshabilitada

[Route53.2] Las zonas alojadas públicas de Route 53 deberían registrar las consultas de DNS

[RDS.1] La instantánea de RDS debe ser privada

[RDS.2] Las instancias de base de datos de RDS deben prohibir el acceso público, según lo determine la configuración PubliclyAccessible

[RDS.3] Las instancias de base de datos de RDS deben tener habilitado el cifrado en reposo

[RDS.4] Las instantáneas de clústeres de RDS y las instantáneas de bases de datos deben cifrarse en reposo

[RDS.5] Las instancias de base de datos de RDS deben configurarse con varias zonas de disponibilidad

[RDS.6] Se debe configurar una supervisión mejorada para las instancias de base de datos de RDS

[RDS.7] Los clústeres de RDS deben tener habilitada la protección contra eliminaciones

[RDS.8] Las instancias de base de datos de RDS deben tener habilitada la protección contra eliminaciones

[RDS.9] Las instancias de base de datos de RDS deben publicar los registros en Logs CloudWatch

[RDS.10] La autenticación de IAM debe configurarse para las instancias de RDS

[RDS.11] Las instancias de RDS deben tener habilitadas las copias de seguridad automáticas

[RDS.12] La autenticación de IAM debe configurarse para los clústeres de RDS

[RDS.13] Las actualizaciones automáticas de las versiones secundarias de RDS deben estar habilitadas

[RDS.14] Los clústeres de Amazon Aurora deben tener habilitado el retroceso

[RDS.15] Los clústeres de bases de datos de RDS deben configurarse para varias zonas de disponibilidad

[RDS.16] Los clústeres de bases de datos de Aurora deben configurarse para copiar las etiquetas a las instantáneas de bases de datos

[RDS.17] Las instancias de base de datos de RDS deben configurarse para copiar las etiquetas de las instantáneas

[RDS.19] Las suscripciones de notificación de eventos de RDS existentes deben configurarse para los eventos críticos del clúster

[RDS.20] Las suscripciones de notificación de eventos de RDS existentes deben configurarse para los eventos críticos de las instancias de bases de datos

[RDS.21] Se debe configurar una suscripción a las notificaciones de eventos de RDS para los eventos de grupos de parámetros de base de datos críticos

[RDS.22] Se debe configurar una suscripción a las notificaciones de eventos de RDS para los eventos críticos de grupos de seguridad de bases de datos

[RDS.23] Las instancias de RDS no deben usar el puerto predeterminado de un motor de base de datos

[RDS.24] Los clústeres de bases de datos de RDS deben usar un nombre de usuario de administrador personalizado

[RDS.25] Las instancias de bases de datos de RDS deben usar un nombre de usuario de administrador personalizado

[RDS.27] Los clústeres de bases de datos de RDS deben cifrarse en reposo

[RDS.34] Los clústeres de bases de datos Aurora MySQL deben publicar los registros de auditoría en Logs CloudWatch

[RDS.35] Los clústeres de bases de datos de RDS deben tener habilitada la actualización automática de versiones secundarias

[RDS.36] Las instancias de base de datos de RDS para PostgreSQL deben publicar los registros en Logs CloudWatch

[RDS.37] Los clústeres de bases de datos de Aurora PostgreSQL deben publicar los registros en Logs CloudWatch

[RDS.40] Las instancias de base de datos de RDS para SQL Server deben publicar los registros en Logs CloudWatch

[RDS.41] Las instancias de base de datos de RDS para SQL Server deben cifrarse en tránsito

[RDS.42] Las instancias de base de datos de RDS para MariaDB deben publicar los registros en Logs CloudWatch

[RDS.43] Los proxies de bases de datos de RDS deben requerir el cifrado TLS para las conexiones

[RDS.44] Las instancias de base de datos de RDS para MariaDB deben cifrarse durante el tránsito

[RDS.45] Los clústeres de bases de datos Aurora MySQL deben tener habilitado el registro de auditoría

[RDS.46] Las instancias de base de datos de RDS no deben implementarse en subredes públicas con rutas a pasarelas de Internet

[RDS.47] Los clústeres de bases de datos de RDS para PostgreSQL deben configurarse para copiar las etiquetas a las instantáneas de bases de datos

[RDS.48] Los clústeres de bases de datos de RDS para MySQL deben configurarse para copiar etiquetas a las instantáneas de bases de datos

[RDS.50] Los clústeres de bases de datos de RDS deben tener un período de retención de copias de seguridad suficiente

[RDS.51] Los clústeres globales de RDS deben ejecutarse en una versión compatible de Aurora MySQL

[Redshift.1] Los clústeres de Amazon Redshift deberían prohibir el acceso público

[Redshift.2] Las conexiones a los clústeres de Amazon Redshift deben cifrarse en tránsito

[Redshift.3] Los clústeres de Amazon Redshift deben tener habilitadas las instantáneas automáticas

[Redshift.4] Los clústeres de Amazon Redshift deben tener habilitado el registro de auditoría

[Redshift.6] Amazon Redshift debería tener habilitadas las actualizaciones automáticas a las versiones principales

[Redshift.7] Los clústeres de Redshift deberían utilizar un enrutamiento de VPC mejorado

[Redshift.8] Los clústeres de Amazon Redshift no deben usar el nombre de usuario de administrador predeterminado

[Redshift.10] Los clústeres de Redshift deben cifrarse en reposo

[Redshift.15] Los grupos de seguridad de Redshift deberían permitir la entrada en el puerto del clúster solo desde orígenes restringidos

[Redshift.18] Los clústeres de Redshift deberían tener Multi-AZ las implementaciones habilitadas

[RedshiftServerless.1] Los grupos de trabajo sin servidor de Amazon Redshift deberían utilizar un enrutamiento de VPC mejorado

[RedshiftServerless.2] Las conexiones a los grupos de trabajo sin servidor de Redshift deberían ser obligatorias para usar SSL

[RedshiftServerless.3] Los grupos de trabajo sin servidor de Redshift deberían prohibir el acceso público

[RedshiftServerless.5] Los espacios de nombres Redshift Serverless no deben usar el nombre de usuario de administrador predeterminado

[RedshiftServerless.6] Los espacios de nombres Redshift Serverless deberían exportar los registros a los registros CloudWatch

[S3.1] Los cubos de uso general de S3 deben tener habilitada la configuración de bloqueo del acceso público

[S3.2] Los cubos de uso general de S3 deberían bloquear el acceso de lectura pública

[S3.3] Los cubos S3 de uso general deberían bloquear el acceso público a la escritura

[S3.5] Los cubos de uso general de S3 deberían requerir que las solicitudes usen TLS

[S3.6] Las políticas de bucket de uso general de S3 deberían restringir el acceso a otros Cuentas de AWS

[S3.8] Los cubos de uso general de S3 deben bloquear el acceso público

[S3.9] Los cubos de uso general de S3 deben tener habilitado el registro de acceso al servidor

[S3.12] Las ACL no deben usarse para administrar el acceso de los usuarios a los cubos de uso general de S3

[S3.13] Los cubos de uso general de S3 deben tener configuraciones de ciclo de vida

[S3.19] Los puntos de acceso S3 deben tener habilitada la configuración de bloqueo de acceso público

[S3.24] Los puntos de Multi-Region acceso S3 deben tener habilitada la configuración de bloqueo del acceso público

[S3.25] Los buckets de directorio de S3 deben tener configuraciones de ciclo de vida

[SageMaker.1] Las instancias de Amazon SageMaker Notebook no deberían tener acceso directo a Internet

[SageMaker.2] las instancias de SageMaker cuadernos deben lanzarse en una VPC personalizada

[SageMaker.3] Los usuarios no deben tener acceso root a las instancias de los SageMaker cuadernos

[SageMaker.4] Las variantes de producción de SageMaker terminales deben tener un recuento inicial de instancias superior a 1

SageMaker Los modelos [SageMaker.5] deben tener habilitado el aislamiento de red

[SageMaker.8] las instancias de SageMaker notebooks deben ejecutarse en plataformas compatibles

[SageMaker.9] las definiciones de trabajos de calidad de los SageMaker datos deben tener habilitado el cifrado del tráfico entre contenedores

[SageMaker.10] Las definiciones de trabajos de explicabilidad del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores

[SageMaker.11] las definiciones de trabajos SageMaker de calidad de los datos deben tener habilitado el aislamiento de red

[SageMaker.12] las definiciones de trabajo basadas en el sesgo del SageMaker modelo deben tener habilitado el aislamiento de red

[SageMaker.13] las definiciones de trabajos de calidad del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores

[SageMaker.14] los programas SageMaker de monitoreo deben tener habilitado el aislamiento de la red

[SageMaker.15] Las definiciones de trabajo basadas en el sesgo del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores

SageMaker Los modelos [SageMaker.16] deben usar un registro privado en la VPC para los contenedores principales

[SageMaker.17] SageMaker Las tiendas offline de los grupos de funciones deben cifrarse con AWS KMS claves

[SageMaker.19] SageMaker los modelos deben usar un registro privado en la VPC para las canalizaciones de inferencia de varios contenedores

[SecretsManager.1] Los secretos de Secrets Manager deberían tener habilitada la rotación automática

[SecretsManager.2] Los secretos de Secrets Manager configurados con rotación automática deberían girar correctamente

[SecretsManager.3] Eliminar los secretos de Secrets Manager no utilizados

[SecretsManager.4] Los secretos de Secrets Manager deben rotarse en un número específico de días

[ServiceCatalog.1] Las carteras de Service Catalog deben compartirse dentro de unAWSsolo una organización

[SES.3] Los conjuntos de configuración de SES deben tener el TLS habilitado para enviar correos electrónicos

[SNS.4] Las políticas de acceso a los temas de SNS no deberían permitir el acceso público

[SQS.1] Las colas de Amazon SQS deben cifrarse en reposo

[SQS.3] Las políticas de acceso a las colas de SQS no deberían permitir el acceso público

[SSM.1] Las instancias de Amazon EC2 deben administrarse medianteAWS Systems Manager

[SSM.2] Las instancias de Amazon EC2 administradas por Systems Manager deben tener el estado de conformidad con los parches de CONFORMIDAD CON LOS PARCHES tras la instalación de un parche

[SSM.3] Las instancias de Amazon EC2 administradas por Systems Manager deben tener el estado de conformidad de la asociación de COMPLIANT

[SSM.4] Los documentos SSM no deben ser públicos

[SSM.6] SSM Automation debería tener el registro habilitado CloudWatch

[SSM.7] Los documentos SSM deben tener habilitada la configuración de bloqueo para compartir en público

[StepFunctions.1] Step Functions indica que las máquinas deben tener el registro activado

[Transfer.2] Los servidores Transfer Family no deben usar el protocolo FTP para la conexión de puntos finales

[Transfer.3] Los conectores Transfer Family deben tener habilitado el registro

[WAF.1]AWS WAFEl registro de ACL web global clásico debe estar habilitado

[WAF.2]AWS WAFLas reglas regionales clásicas deben tener al menos una condición

[WAF.3]AWS WAFLos grupos de reglas regionales clásicos deben tener al menos una regla

[WAF.4]AWS WAFLas ACL web regionales clásicas deben tener al menos una regla o grupo de reglas

[WAF.6]AWS WAFLas reglas globales clásicas deben tener al menos una condición

[WAF.7]AWS WAFLos grupos de reglas globales clásicos deben tener al menos una regla

[WAF.8]AWS WAFLas ACL web globales clásicas deben tener al menos una regla o grupo de reglas

[WAF.10]AWS WAFLas ACL web deben tener al menos una regla o grupo de reglas

[WAF.12]AWS WAFlas reglas deben tener CloudWatch las métricas habilitadas

[WorkSpaces.1] los volúmenes de WorkSpaces usuarios deben cifrarse en reposo

[WorkSpaces.2] los volúmenes WorkSpaces raíz deben cifrarse en reposo

Estándar de mejores prácticas de seguridad de IA en Security Hub (CSPM)

El estándar de mejores prácticas de seguridad de la IA es un conjunto de controles de seguridad automatizados que detectan si los recursos de IA desplegados no se ajustan a las prácticas recomendadas de seguridad. Desarrollado por expertos en AWS seguridad, este estándar proporciona un conjunto seleccionado de controles que ayudan a identificar las áreas en las que las cargas de trabajo de la IA se desvían de las configuraciones de seguridad recomendadas.

En AWS Security Hub CSPM, el estándar de mejores prácticas de seguridad de la IA incluye controles que evalúan tus recursos de forma continua. Los controles abarcan los dominios de seguridad, incluidos, entre otros, el aislamiento de la red, el cifrado en reposo y en tránsito, la ubicación de las VPC, el uso de AWS KMS claves y los requisitos de registro privado. A cada control se le asigna una categoría que refleja la función de seguridad a la que se aplica el control. Para ver la lista de categorías y obtener más detalles, consulte Categorías de controles en el CSPM de Security Hub.

El estándar de mejores prácticas de seguridad de la IA tiene el siguiente nombre de recurso de Amazon (ARN):`arn:aws:securityhub:`*`region`*`::standards/ai-security-best-practices/v/1.0.0`, donde *`region`* está el código de región correspondiente al correspondiente. Región de AWS También puede utilizar el GetEnabledStandards funcionamiento de la API CSPM de Security Hub para recuperar el ARN de un estándar que esté activado actualmente.

Controles que se aplican al estándar

En la siguiente lista se especifican los controles CSPM de AWS Security Hub que se aplican al estándar de prácticas recomendadas de seguridad de la IA (v1.0.0). Para revisar los detalles de un control, seleccione el control.

- [Bedrock.1] Las fuentes de datos de Amazon Bedrock deben cifrarse de forma gestionada por el clienteAWS KMSclaves

- [BedrockAgentCore.1] Los AgentCore tiempos de ejecución de Bedrock deben configurarse con el modo de red VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways debería requerir autorización para las solicitudes entrantes
- [BedrockAgentCore.3] Bedrock AgentCore Memory debe estar cifrada y gestionada por el clienteAWS KMSclaves
- [BedrockAgentCore.4] Bedrock AgentCore Gateway debe cifrarse de forma que sea gestionada por el clienteAWS KMSclaves
- [BedrockAgentCore.5] Los navegadores AgentCore personalizados de Bedrock no deberían usar el modo de red pública
- [BedrockAgentCore.6] Los navegadores AgentCore personalizados de Bedrock deberían tener habilitada la grabación de sesiones
- [BedrockAgentCore.7] Los intérpretes de código AgentCore personalizados de Bedrock deben usar una configuración de red privada
- [SageMaker.1] Las instancias de Amazon SageMaker Notebook no deberían tener acceso directo a Internet
- [SageMaker.2] las instancias de SageMaker cuadernos deben lanzarse en una VPC personalizada
- [SageMaker.3] Los usuarios no deben tener acceso root a las instancias de los SageMaker cuadernos
- [SageMaker.4] Las variantes de producción de SageMaker terminales deben tener un recuento inicial de instancias superior a 1
- SageMaker Los modelos [SageMaker.5] deben tener habilitado el aislamiento de red
- [SageMaker.8] las instancias de SageMaker notebooks deben ejecutarse en plataformas compatibles
- [SageMaker.9] las definiciones de trabajos de calidad de los SageMaker datos deben tener habilitado el cifrado del tráfico entre contenedores
- [SageMaker.10] Las definiciones de trabajos de explicabilidad del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores
- [SageMaker.11] las definiciones de trabajos SageMaker de calidad de los datos deben tener habilitado el aislamiento de red
- [SageMaker.12] las definiciones de trabajo basadas en el sesgo del SageMaker modelo deben tener habilitado el aislamiento de red

- [SageMaker.13] las definiciones de trabajos de calidad del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores
- [SageMaker.14] los programas SageMaker de monitoreo deben tener habilitado el aislamiento de la red
- [SageMaker.15] Las definiciones de trabajo basadas en el sesgo del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores
- SageMaker Los modelos [SageMaker.16] deben usar un registro privado en la VPC para los contenedores principales
- [SageMaker.17] SageMaker Las tiendas offline de los grupos de funciones deben cifrarse con AWS KMS claves
- [SageMaker.18] las tiendas en línea de grupos de SageMaker funciones con almacenamiento estándar deben cifrarse con AWS KMS claves
- [SageMaker.19] SageMaker los modelos deben usar un registro privado en la VPC para las canalizaciones de inferencia de varios contenedores
- [SageMaker.20] explicabilidad del SageMaker modelo: las definiciones de los trabajos deben tener habilitado el aislamiento de red
- [SageMaker.21] las instancias de SageMaker cuadernos deben cifrarse y gestionarse por el cliente AWS KMS claves
- [SageMaker.22] los programas SageMaker de monitoreo deben tener habilitado el cifrado del tráfico entre contenedores
- [SageMaker.23] los experimentos de SageMaker inferencia deben tener el volumen de almacenamiento de instancias cifrado y gestionado por el cliente AWS KMS claves
- [SageMaker.24] los experimentos de SageMaker inferencia deben tener el almacenamiento de datos cifrado y gestionado por el cliente AWS KMS claves
- [SageMaker.25] las definiciones de trabajos de calidad del SageMaker modelo deben tener habilitado el aislamiento de red

AWS Estándar de etiquetado de recursos en Security Hub CSPM

El estándar AWS de etiquetado de recursos, desarrollado por AWS Security Hub CSPM, le ayuda a determinar si a sus AWS recursos les faltan etiquetas. Las etiquetas son pares clave-valor que actúan como metadatos para organizar los recursos. AWS En la mayoría de los recursos de AWS , puede agregar etiquetas al recurso cuando lo crea o después de crearlo. Entre los ejemplos de recursos se incluyen CloudFront las distribuciones de Amazon, las instancias de Amazon Elastic

Compute Cloud (Amazon EC2) y los secretos en. AWS Secrets Manager Las etiquetas pueden ayudarlo a administrar, identificar, organizar, buscar y filtrar AWS los recursos.

Cada etiqueta de tiene dos partes:

- Una clave de etiqueta, por ejemplo, `CostCenter`, `Environment`, o `Project`. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.
- Un valor de etiqueta, por ejemplo, `111122223333` o `Production`. Al igual que las claves de etiquetas, los valores de las etiquetas distinguen entre mayúsculas y minúsculas.

Utilice etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Para obtener información sobre cómo agregar etiquetas a AWS los recursos, consulta la Guía del usuario del editor de etiquetas y AWS recursos para etiquetar recursos.

Para cada control que se aplique al estándar de etiquetado de AWS recursos de Security Hub CSPM, si lo desea, puede usar el parámetro compatible para especificar las claves de etiqueta que desea que compruebe el control. Si no especifica ninguna clave de etiqueta, el control verifica únicamente la existencia de al menos una clave de etiqueta y falla si un recurso no tiene ninguna.

Antes de habilitar el estándar AWS de etiquetado de recursos, es importante habilitar y configurar el registro de recursos. AWS Config Al configurar el registro de recursos, asegúrese también de habilitarlo para todos los tipos de AWS recursos que se comprueban mediante los controles que se aplican a la norma. De lo contrario, es posible que el CSPM de Security Hub no pueda evaluar los recursos adecuados ni generar los resultados precisos para los controles aplicables al estándar. Para obtener más información, incluida una lista de los tipos de recursos que se deben registrar, consulte AWS ConfigRecursos necesarios para los hallazgos de control.

Tras habilitar el estándar de etiquetado de AWS recursos, empezará a recibir información sobre los controles que se aplican al estándar. Tenga en cuenta que Security Hub CSPM puede tardar hasta 18 horas en generar los resultados de los controles que utilizan la misma regla AWS Config vinculada a un servicio que los controles que se aplican a otros estándares habilitados. Para obtener más información, consulte Programación para ejecutar comprobaciones de seguridad.

El estándar AWS de etiquetado de recursos tiene el siguiente nombre de recurso de Amazon (ARN):`arn:aws:securityhub:`*`region`*`::standards/aws-resource-tagging-standard/v/1.0.0`, donde *`region`* es el código de región aplicable. Región de AWS También puede utilizar el GetEnabledStandards funcionamiento de la API CSPM de Security Hub para recuperar el ARN de un estándar que esté activado actualmente.

> **Note**
>
> El estándar de etiquetado de recursos de AWS no está disponible en las regiones de Asia-Pacífico (Nueva Zelanda) y Asia-Pacífico (Taipéi).

Controles que se aplican al estándar

La siguiente lista especifica qué controles CSPM de AWS Security Hub se aplican al estándar de etiquetado de AWS recursos (v1.0.0). Para revisar los detalles de un control, seleccione el control.

- [ACM.3] Los certificados ACM deben estar etiquetados
- [Amplify.1] Las aplicaciones Amplify deben estar etiquetadas
- [Amplify.2] Amplify branches debe estar etiquetado
- [AppConfig.1]AWS AppConfiglas aplicaciones deben estar etiquetadas
- [AppConfig.2]AWS AppConfiglos perfiles de configuración deben estar etiquetados
- [AppConfig.3]AWS AppConfiglos entornos deben estar etiquetados
- [AppConfig.4]AWS AppConfiglas asociaciones de extensiones deben estar etiquetadas
- [AppFlow.1] AppFlow Los flujos de Amazon deben estar etiquetados
- [AppRunner.1] Los servicios de App Runner deben estar etiquetados
- [AppRunner.2] Los conectores VPC de App Runner deben estar etiquetados
- [AppSync.4]AWS AppSyncLas API de GraphQL deben estar etiquetadas
- [Athena.2] Los catálogos de datos de Athena deben estar etiquetados
- [Athena.3] Los grupos de trabajo de Athena deben estar etiquetados
- [AutoScaling.10] Los grupos de Auto Scaling de EC2 deben estar etiquetados
- [Backup.2]AWS Backuplos puntos de recuperación deben estar etiquetados
- [Backup.3]AWS Backuplas bóvedas deben estar etiquetadas
- [Backup.4]AWS Backuplos planes de informes deben estar etiquetados
- [Backup.5]AWS Backuplos planes de respaldo deben estar etiquetados
- [Batch.1] Las colas de trabajos por lotes deben estar etiquetadas
- [Batch.2] Las políticas de programación de lotes deben estar etiquetadas
- [Batch.3] Los entornos de procesamiento por lotes deben etiquetarse

- [Batch.4] Las propiedades de los recursos de cómputo en los entornos de cómputo por lotes gestionados deben estar etiquetadas
- [CloudFormation.2] las CloudFormation pilas deben estar etiquetadas
- [CloudFront.14] CloudFront las distribuciones deben estar etiquetadas
- [CloudTrail.9] las CloudTrail rutas deben estar etiquetadas
- [CodeArtifact.1] CodeArtifact los repositorios deben estar etiquetados
- [CodeGuruProfiler.1] Los grupos CodeGuru de creación de perfiles de Profiler deben estar etiquetados
- [CodeGuruReviewer.1] Las asociaciones de repositorios de CodeGuru Reviewer deben estar etiquetadas
- [Connect.1] Los tipos de objetos de los perfiles de clientes de Amazon Connect deben estar etiquetados
- [DataSync.2] DataSync las tareas deben estar etiquetadas
- [Detective.1] Los gráficos de comportamiento de los detectives deben estar etiquetados
- [DMS.2] Los certificados DMS deben estar etiquetados
- [DMS.3] Las suscripciones a eventos de DMS deben estar etiquetadas
- [DMS.4] Las instancias de replicación de DMS deben estar etiquetadas
- [DMS.5] Los grupos de subredes de replicación del DMS deben estar etiquetados
- [DynamoDB.5] Las tablas de DynamoDB deben estar etiquetadas
- [EC2.33] Los archivos adjuntos de la pasarela de tránsito EC2 deben estar etiquetados
- [EC2.34] Las tablas de rutas de la pasarela de tránsito EC2 deben estar etiquetadas
- [EC2.35] Las interfaces de red EC2 deben estar etiquetadas
- [EC2.36] Las pasarelas de clientes de EC2 deben estar etiquetadas
- [EC2.37] Las direcciones IP elásticas de EC2 deben estar etiquetadas
- [EC2.38] Las instancias EC2 deben estar etiquetadas
- [EC2.39] Las pasarelas de Internet EC2 deben estar etiquetadas
- [EC2.40] Las pasarelas NAT EC2 deben estar etiquetadas
- [EC2.41] Las ACL de la red EC2 deben estar etiquetadas
- [EC2.42] Las tablas de rutas de EC2 deben estar etiquetadas
- [EC2.43] Los grupos de seguridad de EC2 deben estar etiquetados

- [EC2.44] Las subredes EC2 deben estar etiquetadas
- [EC2.45] Los volúmenes EC2 deben estar etiquetados
- [EC2.46] Las Amazon VPC deben estar etiquetadas
- [EC2.47] Los servicios de punto final de Amazon VPC deben estar etiquetados
- [EC2.48] Los registros de flujo de Amazon VPC deben estar etiquetados
- [EC2.49] Las conexiones de emparejamiento de Amazon VPC deben estar etiquetadas
- [EC2.50] Las pasarelas VPN de EC2 deben estar etiquetadas
- [EC2.52] Las pasarelas de tránsito EC2 deben estar etiquetadas
- [EC2.174] Los conjuntos de opciones DHCP de EC2 deben estar etiquetados
- [EC2.175] Las plantillas de lanzamiento de EC2 deben estar etiquetadas
- [EC2.176] Las listas de prefijos de EC2 deben estar etiquetadas
- [EC2.177] Las sesiones de réplica de tráfico de EC2 deben etiquetarse
- [EC2.178] Los filtros espejo de tráfico EC2 deben estar etiquetados
- [EC2.179] Los objetivos del espejo de tráfico de EC2 deben estar etiquetados
- [ECR.4] Los repositorios públicos de ECR deben etiquetarse
- [ECS.13] Los servicios de ECS deben estar etiquetados
- [ECS.14] Los clústeres de ECS deben etiquetarse
- [ECS.15] Las definiciones de las tareas de ECS deben estar etiquetadas
- [EFS.5] Los puntos de acceso EFS deben estar etiquetados
- [] Los clústeres de EKS deben etiquetarse EKS.6
- [EKS.7] Las configuraciones del proveedor de identidad de EKS deben etiquetarse
- [ES.9] Los dominios de Elasticsearch deben etiquetarse
- [EventBridge.2] los autobuses de EventBridge eventos deben estar etiquetados
- [FraudDetector.1] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.2] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas
- [FraudDetector.3] Los resultados de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.4] Las variables de Amazon Fraud Detector deben estar etiquetadas
- [GlobalAccelerator.1] Los aceleradores de Global Accelerator deben estar etiquetados
- [Glue.1]AWS Gluelos trabajos deben estar etiquetados

- GuardDuty Los filtros [GuardDuty.2] deben estar etiquetados
- [GuardDuty.3] Los GuardDuty IPSets deben estar etiquetados
- [GuardDuty.4] GuardDuty los detectores deben estar etiquetados
- [IAM.23] Los analizadores de IAM Access Analyzer deben estar etiquetados
- [IAM.24] Las funciones de IAM deben estar etiquetadas
- [IAM.25] Los usuarios de IAM deben estar etiquetados
- [IoT.1]AWS IoT Device Defenderlos perfiles de seguridad deben estar etiquetados
- [IoT.2]AWS IoT Corelas acciones de mitigación deben estar etiquetadas
- [IoT.3]AWS IoT Corelas dimensiones deben estar etiquetadas
- [IoT.4]AWS IoT Corelos autorizadores deben estar etiquetados
- [IoT.5]AWS IoT CoreLos alias de los roles deben estar etiquetados
- [IoT.6]AWS IoT Corelas políticas deben estar etiquetadas
- [IoTSiteWise.1]AWSLos modelos SiteWise de activos de IoT deben estar etiquetados
- [IoTSiteWise.2]AWS SiteWise Los paneles de IoT deben estar etiquetados
- [IoTSiteWise.3]AWS SiteWise Las pasarelas de IoT deben estar etiquetadas
- [IoTSiteWise.4]AWS SiteWise Los portales de IoT deben estar etiquetados
- [IoTSiteWise.5]AWS SiteWise Los proyectos de IoT deben estar etiquetados
- [IoTTwinMaker.1]AWSLos trabajos de TwinMaker sincronización de IoT deben estar etiquetados
- [IoTTwinMaker.2]AWS TwinMaker Los espacios de trabajo de IoT deben estar etiquetados
- [IoTTwinMaker.3]AWS TwinMaker Las escenas de IoT deben estar etiquetadas
- [IoTTwinMaker.4]AWS TwinMaker Las entidades de IoT deben estar etiquetadas
- [IoTWireless.1]AWSLos grupos de multidifusión de IoT Wireless deben estar etiquetados
- [IoTWireless.2]AWSLos perfiles de servicio de IoT Wireless deben estar etiquetados
- [IoTWireless.3]AWSLas tareas de IoT FUOTA deben estar etiquetadas
- [IVS.1] Los pares de teclas de reproducción IVS deben estar etiquetados
- [IVS.2] Las configuraciones de grabación de IVS deben estar etiquetadas
- [IVS.3] Los canales IVS deben estar etiquetados
- [Keyspaces.1] Los espacios clave de Amazon Keyspaces deben estar etiquetados
- [Kinesis.2] Las transmisiones de Kinesis deben estar etiquetadas

- [Lambda.6] Las funciones de Lambda deben estar etiquetadas
- [MQ.4] Los corredores de Amazon MQ deben estar etiquetados
- [NetworkFirewall.7] Los firewalls de Network Firewall deben estar etiquetados
- [NetworkFirewall.8] Las políticas de firewall de Network Firewall deben estar etiquetadas
- [Opensearch.9] OpenSearch los dominios deben estar etiquetados
- [PCA.2]AWSLas autoridades de certificación de CA privadas deben estar etiquetadas
- [RDS.28] Los clústeres de bases de datos de RDS deben etiquetarse
- [RDS.29] Las instantáneas del clúster de bases de datos de RDS deben etiquetarse
- [RDS.30] Las instancias de base de datos de RDS deben etiquetarse
- [RDS.31] Los grupos de seguridad de la base de datos de RDS deben etiquetarse
- [RDS.32] Las instantáneas de la base de datos de RDS deben etiquetarse
- [RDS.33] Los grupos de subredes de bases de datos de RDS deben etiquetarse
- [Redshift.11] Los clústeres de Redshift deben estar etiquetados
- [Redshift.12] Las suscripciones a notificaciones de eventos de Redshift deben estar etiquetadas
- [Redshift.13] Las instantáneas del clúster de Redshift deben estar etiquetadas
- [Redshift.14] Los grupos de subredes del clúster de Redshift deben estar etiquetados
- [Redshift.17] Los grupos de parámetros del clúster de Redshift deben estar etiquetados
- [Route53.1] Los controles de salud de Route 53 deben estar etiquetados
- [SageMaker.6] las configuraciones de imagen de la SageMaker aplicación deben estar etiquetadas
- [SageMaker.7] SageMaker las imágenes deben estar etiquetadas
- [SecretsManager.5] Los secretos de Secrets Manager deben estar etiquetados
- [SES.1] Las listas de contactos de SES deben estar etiquetadas
- [SES.2] Los conjuntos de configuración de SES deben estar etiquetados
- [SNS.3] Los temas de SNS deben estar etiquetados
- [SQS.2] Las colas de SQS deben estar etiquetadas
- [SSM.5] Los documentos SSM deben estar etiquetados
- [StepFunctions.2] Las actividades de Step Functions deben estar etiquetadas
- [Transfer.1]AWS Transfer Familylos flujos de trabajo deben estar etiquetados
- [Transfer.4] Los acuerdos Transfer Family deben estar etiquetados

- [Transfer.5] Los certificados Transfer Family deben estar etiquetados
- [Transfer.6] Los conectores Transfer Family deben estar etiquetados
- [Transfer.7] Los perfiles de Transfer Family deben estar etiquetados

CIS AWS Aspectos básicos y comparativos del CSPM de Security Hub

El Center for Internet Security (CIS) AWS Foundations Benchmark sirve como un conjunto de mejores prácticas de configuración de seguridad para AWS. Estas mejores prácticas aceptadas por la industria le proporcionan procedimientos de implementación y evaluación claros y paso a paso. Desde sistemas operativos hasta servicios en la nube y dispositivos de red, los controles de este punto de referencia le ayudan a proteger los sistemas específicos que utiliza su organización.

AWS Security Hub CSPM es compatible con las versiones 5.0.0, 3.0.0, 1.4.0 y 1.2.0 de CIS AWS Foundations Benchmark. Esta página enumera los controles de seguridad que admite cada versión. También ofrece una comparación entre las versiones.

CIS AWS Foundations Benchmark, versión 5.0.0

Security Hub CSPM es compatible con la versión 5.0.0 (v5.0.0) del CIS Foundations Benchmark. AWS El CSPM de Security Hub cumple los requisitos de la certificación de software de seguridad de CIS y ha recibido dicha certificación para los siguientes indicadores de referencia de CIS:

- CIS Benchmark para CIS AWS Foundations Benchmark, v5.0.0, nivel 1
- CIS Benchmark para CIS AWS Foundations Benchmark, v5.0.0, nivel 2

Controles que se aplican al CIS AWS Versión 5.0.0 de Foundations Benchmark

[Account.1] La información de contacto de seguridad debe proporcionarse para unCuenta de AWS

[CloudTrail.1] CloudTrail debe estar habilitado y configurado con al menos un registro multirregional que incluya eventos de administración de lectura y escritura

[CloudTrail.2] CloudTrail debe tener activado el cifrado en reposo

[CloudTrail.4] La validación del archivo de CloudTrail registro debe estar habilitada

[CloudTrail.7] Asegúrese de que el registro de acceso al bucket de S3 esté habilitado en el CloudTrail bucket de S3

[Config.1] AWS Config deben estar habilitados y usar la función vinculada al servicio para el registro de recursos

[EC2.2] Los grupos de seguridad predeterminados de VPC no deben permitir el tráfico entrante o saliente

[EC2.6] El registro de flujo de VPC debe estar habilitado en todas las VPC

[EC2.7] El cifrado predeterminado de EBS debe estar habilitado

[EC2.8] Las instancias EC2 deben utilizar la versión 2 del servicio de metadatos de instancia (IMDSv2)

[EC2.21] Las ACL de red no deberían permitir la entrada desde la versión 0.0.0. 0/0 al puerto 22 o al puerto 3389

[EC2.53] Los grupos de seguridad de EC2 no deberían permitir la entrada desde la versión 0.0.0. 0/0 a los puertos de administración remota del servidor

[EC2.54] Los grupos de seguridad de EC2 no deberían permitir la entrada desde: :/0 a los puertos de administración remota del servidor

[EFS.1] Elastic File System debe configurarse para cifrar los datos de los archivos en reposo mediante AWS KMS

[EFS.8] Los sistemas de archivos EFS deben cifrarse en reposo

[IAM.2] Los usuarios de IAM no deberían tener políticas de IAM adjuntas

[IAM.3] Las claves de acceso de los usuarios de IAM deben rotarse cada 90 días o menos

[IAM.4] La clave de acceso del usuario raíz de IAM no debería existir

[IAM.5] La MFA debe estar habilitada para todos los usuarios de IAM que tengan una contraseña de consola

[IAM.6] La MFA de hardware debe estar habilitada para el usuario root

[IAM.9] La MFA debe estar habilitada para el usuario root

[IAM.15] Asegúrese de que la política de contraseñas de IAM exija una longitud de contraseña mínima de 14 o más

[IAM.16] Asegúrese de que la política de contraseñas de IAM impida la reutilización de contraseñas

[IAM.18] Asegúrese de que se haya creado una función de soporte para gestionar los incidentes conAWS Support

[IAM.22] Se deben eliminar las credenciales de usuario de IAM que no se hayan utilizado durante 45 días

[IAM.26] SSL/TLS Los certificados caducados gestionados en IAM deben eliminarse

[IAM.27] Las identidades de IAM no deberían tener la AWSCloudShellFullAccess política adjunta

[IAM.28] El analizador de acceso externo de IAM Access Analyzer debe estar habilitado

[KMS.4]AWS KMSla rotación de claves debe estar habilitada

[RDS.2] Las instancias de base de datos de RDS deben prohibir el acceso público, según lo determine la configuración PubliclyAccessible

[RDS.3] Las instancias de base de datos de RDS deben tener habilitado el cifrado en reposo

[RDS.5] Las instancias de base de datos de RDS deben configurarse con varias zonas de disponibilidad

[RDS.13] Las actualizaciones automáticas de las versiones secundarias de RDS deben estar habilitadas

[RDS.15] Los clústeres de bases de datos de RDS deben configurarse para varias zonas de disponibilidad

[S3.1] Los cubos de uso general de S3 deben tener habilitada la configuración de bloqueo del acceso público

[S3.5] Los cubos de uso general de S3 deberían requerir que las solicitudes usen TLS

[S3.8] Los cubos de uso general de S3 deben bloquear el acceso público

[S3.20] Los cubos de uso general de S3 deben tener habilitada la eliminación de MFA

[S3.22] Los cubos de uso general de S3 deben registrar los eventos de escritura a nivel de objeto

[S3.23] Los cubos de uso general de S3 deben registrar los eventos de lectura a nivel de objeto

CIS AWS Foundations Benchmark versión 3.0.0

Security Hub CSPM es compatible con la versión 3.0.0 (v3.0.0) del CIS Foundations Benchmark. AWS El CSPM de Security Hub cumple los requisitos de la certificación de software de seguridad de CIS y ha recibido dicha certificación para los siguientes indicadores de referencia de CIS:

- CIS Benchmark para CIS AWS Foundations Benchmark, v3.0.0, nivel 1
- CIS Benchmark para CIS AWS Foundations Benchmark, v3.0.0, nivel 2

Controles que se aplican al CIS AWS Versión 3.0.0 de Foundations Benchmark

[Account.1] La información de contacto de seguridad debe proporcionarse para unCuenta de AWS

[CloudTrail.1] CloudTrail debe estar habilitado y configurado con al menos un registro multirregional que incluya eventos de administración de lectura y escritura

[CloudTrail.2] CloudTrail debe tener activado el cifrado en reposo

[CloudTrail.4] La validación del archivo de CloudTrail registro debe estar habilitada

[CloudTrail.7] Asegúrese de que el registro de acceso al bucket de S3 esté habilitado en el CloudTrail bucket de S3

[Config.1] AWS Config deben estar habilitados y usar la función vinculada al servicio para el registro de recursos

[EC2.2] Los grupos de seguridad predeterminados de VPC no deben permitir el tráfico entrante o saliente

[EC2.6] El registro de flujo de VPC debe estar habilitado en todas las VPC

[EC2.7] El cifrado predeterminado de EBS debe estar habilitado

[EC2.8] Las instancias EC2 deben utilizar la versión 2 del servicio de metadatos de instancia (IMDSv2)

[EC2.21] Las ACL de red no deberían permitir la entrada desde la versión 0.0.0. 0/0 al puerto 22 o al puerto 3389

[EC2.53] Los grupos de seguridad de EC2 no deberían permitir la entrada desde la versión 0.0.0. 0/0 a los puertos de administración remota del servidor

[EC2.54] Los grupos de seguridad de EC2 no deberían permitir la entrada desde: :/0 a los puertos de administración remota del servidor

[EFS.1] Elastic File System debe configurarse para cifrar los datos de los archivos en reposo mediante AWS KMS

[IAM.2] Los usuarios de IAM no deberían tener políticas de IAM adjuntas

[IAM.3] Las claves de acceso de los usuarios de IAM deben rotarse cada 90 días o menos

[IAM.4] La clave de acceso del usuario raíz de IAM no debería existir

[IAM.5] La MFA debe estar habilitada para todos los usuarios de IAM que tengan una contraseña de consola

[IAM.6] La MFA de hardware debe estar habilitada para el usuario root

[IAM.9] La MFA debe estar habilitada para el usuario root

[IAM.15] Asegúrese de que la política de contraseñas de IAM exija una longitud de contraseña mínima de 14 o más

[IAM.16] Asegúrese de que la política de contraseñas de IAM impida la reutilización de contraseñas

[IAM.18] Asegúrese de que se haya creado una función de soporte para gestionar los incidentes conAWS Support

[IAM.22] Se deben eliminar las credenciales de usuario de IAM que no se hayan utilizado durante 45 días

[IAM.26] SSL/TLS Los certificados caducados gestionados en IAM deben eliminarse

[IAM.27] Las identidades de IAM no deberían tener la AWSCloudShellFullAccess política adjunta

[IAM.28] El analizador de acceso externo de IAM Access Analyzer debe estar habilitado

[KMS.4]AWS KMSla rotación de claves debe estar habilitada

[RDS.2] Las instancias de base de datos de RDS deben prohibir el acceso público, según lo determine la configuración PubliclyAccessible

[RDS.3] Las instancias de base de datos de RDS deben tener habilitado el cifrado en reposo

[RDS.13] Las actualizaciones automáticas de las versiones secundarias de RDS deben estar habilitadas

[S3.1] Los cubos de uso general de S3 deben tener habilitada la configuración de bloqueo del acceso público

[S3.5] Los cubos de uso general de S3 deberían requerir que las solicitudes usen TLS

[S3.8] Los cubos de uso general de S3 deben bloquear el acceso público

[S3.20] Los cubos de uso general de S3 deben tener habilitada la eliminación de MFA

[S3.22] Los cubos de uso general de S3 deben registrar los eventos de escritura a nivel de objeto

[S3.23] Los cubos de uso general de S3 deben registrar los eventos de lectura a nivel de objeto

CIS AWS Foundations Benchmark versión 1.4.0

Security Hub CSPM es compatible con la versión 1.4.0 (v1.4.0) del CIS Foundations Benchmark. AWS

Controles que se aplican al CIS AWS Versión 1.4.0 de Foundations Benchmark

[CloudTrail.1] CloudTrail debe estar habilitado y configurado con al menos un registro multirregional que incluya eventos de administración de lectura y escritura

[CloudTrail.2] CloudTrail debe tener activado el cifrado en reposo

[CloudTrail.4] La validación del archivo de CloudTrail registro debe estar habilitada

[CloudTrail.5] los CloudTrail senderos deben estar integrados con Amazon CloudWatch Logs

[CloudTrail.6] Asegúrese de que el depósito de S3 que se utiliza para almacenar CloudTrail los registros no sea de acceso público

[CloudTrail.7] Asegúrese de que el registro de acceso al bucket de S3 esté habilitado en el CloudTrail bucket de S3

[CloudWatch.1] Debe existir un registro, un filtro métrico y una alarma para el uso del usuario «raíz»

[CloudWatch.4] Asegúrese de que haya un registro, un filtro métrico y una alarma para los cambios en las políticas de IAM

[CloudWatch.5] Asegúrese de que existan un registro, un filtro métrico y una alarma para los cambios CloudTrail de configuración

[CloudWatch.6] Asegúrese de que existan un registro métrico, un filtro y una alarma para Consola de administración de AWS errores de autenticación

[CloudWatch.7] Asegúrese de que haya un registro, un filtro métrico y una alarma para deshabilitar o programar la eliminación de las claves administradas por el cliente

[CloudWatch.8] Asegúrese de que haya un registro, un filtro métrico y una alarma para los cambios en la política de buckets de S3

[CloudWatch.9] Asegúrese de que existan un registro métrico, un filtro y una alarma para AWS Config cambios de configuración

[CloudWatch.10] Asegúrese de que haya un registro, un filtro métrico y una alarma para los cambios en los grupos de seguridad

[CloudWatch.11] Asegúrese de que existan un filtro métrico de registro y una alarma para los cambios en las listas de control de acceso a la red (NACL)

[CloudWatch.12] Asegúrese de que haya un registro, un filtro métrico y una alarma para detectar los cambios en las pasarelas de red

[CloudWatch.13] Asegúrese de que haya un registro, un filtro métrico y una alarma para los cambios en la tabla de rutas

[CloudWatch.14] Asegúrese de que haya un registro, un filtro métrico y una alarma para los cambios en la VPC

[Config.1] AWS Config deben estar habilitados y usar la función vinculada al servicio para el registro de recursos

[EC2.2] Los grupos de seguridad predeterminados de VPC no deben permitir el tráfico entrante o saliente

[EC2.6] El registro de flujo de VPC debe estar habilitado en todas las VPC

[EC2.7] El cifrado predeterminado de EBS debe estar habilitado

[EC2.21] Las ACL de red no deberían permitir la entrada desde la versión 0.0.0. 0/0 al puerto 22 o al puerto 3389

[IAM.1] Las políticas de IAM no deberían permitir todos los privilegios administrativos «*»

[IAM.3] Las claves de acceso de los usuarios de IAM deben rotarse cada 90 días o menos

[IAM.4] La clave de acceso del usuario raíz de IAM no debería existir

[IAM.5] La MFA debe estar habilitada para todos los usuarios de IAM que tengan una contraseña de consola

[IAM.6] La MFA de hardware debe estar habilitada para el usuario root

[IAM.9] La MFA debe estar habilitada para el usuario root

[IAM.15] Asegúrese de que la política de contraseñas de IAM exija una longitud de contraseña mínima de 14 o más

[IAM.16] Asegúrese de que la política de contraseñas de IAM impida la reutilización de contraseñas

[IAM.18] Asegúrese de que se haya creado una función de soporte para gestionar los incidentes conAWS Support

[IAM.22] Se deben eliminar las credenciales de usuario de IAM que no se hayan utilizado durante 45 días

[KMS.4]AWS KMSla rotación de claves debe estar habilitada

[RDS.3] Las instancias de base de datos de RDS deben tener habilitado el cifrado en reposo

[S3.1] Los cubos de uso general de S3 deben tener habilitada la configuración de bloqueo del acceso público

[S3.5] Los cubos de uso general de S3 deberían requerir que las solicitudes usen TLS

[S3.8] Los cubos de uso general de S3 deben bloquear el acceso público

[S3.20] Los cubos de uso general de S3 deben tener habilitada la eliminación de MFA

CIS AWS Foundations Benchmark versión 1.2.0

Security Hub CSPM es compatible con la versión 1.2.0 (v1.2.0) del CIS Foundations Benchmark. AWS El CSPM de Security Hub cumple los requisitos de la certificación de software de seguridad de CIS y ha recibido dicha certificación para los siguientes indicadores de referencia de CIS:

- CIS Benchmark para CIS AWS Foundations Benchmark, v1.2.0, nivel 1

- CIS Benchmark para CIS AWS Foundations Benchmark, v1.2.0, nivel 2

Controles que se aplican al CIS AWS Versión 1.2.0 de Foundations Benchmark

[CloudTrail.1] CloudTrail debe estar habilitado y configurado con al menos un registro multirregional que incluya eventos de administración de lectura y escritura

[CloudTrail.2] CloudTrail debe tener activado el cifrado en reposo

[CloudTrail.4] La validación del archivo de CloudTrail registro debe estar habilitada

[CloudTrail.5] los CloudTrail senderos deben estar integrados con Amazon CloudWatch Logs

[CloudTrail.6] Asegúrese de que el depósito de S3 que se utiliza para almacenar CloudTrail los registros no sea de acceso público

[CloudTrail.7] Asegúrese de que el registro de acceso al bucket de S3 esté habilitado en el CloudTrail bucket de S3

[CloudWatch.1] Debe existir un registro, un filtro métrico y una alarma para el uso del usuario «raíz»

[CloudWatch.2] Asegúrese de que existan un registro, un filtro métrico y una alarma para las llamadas a la API no autorizadas

[CloudWatch.3] Asegúrese de que haya un registro, un filtro métrico y una alarma para iniciar sesión en la consola de administración sin MFA

[CloudWatch.4] Asegúrese de que haya un registro, un filtro métrico y una alarma para los cambios en las políticas de IAM

[CloudWatch.5] Asegúrese de que existan un registro, un filtro métrico y una alarma para los cambios CloudTrail de configuración

[CloudWatch.6] Asegúrese de que existan un registro métrico, un filtro y una alarma para Consola de administración de AWS errores de autenticación

[CloudWatch.7] Asegúrese de que haya un registro, un filtro métrico y una alarma para deshabilitar o programar la eliminación de las claves administradas por el cliente

[CloudWatch.8] Asegúrese de que haya un registro, un filtro métrico y una alarma para los cambios en la política de buckets de S3

[CloudWatch.9] Asegúrese de que existan un registro métrico, un filtro y una alarma para AWS Config cambios de configuración

[CloudWatch.10] Asegúrese de que haya un registro, un filtro métrico y una alarma para los cambios en los grupos de seguridad

[CloudWatch.11] Asegúrese de que existan un filtro métrico de registro y una alarma para los cambios en las listas de control de acceso a la red (NACL)

[CloudWatch.12] Asegúrese de que haya un registro, un filtro métrico y una alarma para detectar los cambios en las pasarelas de red

[CloudWatch.13] Asegúrese de que haya un registro, un filtro métrico y una alarma para los cambios en la tabla de rutas

[CloudWatch.14] Asegúrese de que haya un registro, un filtro métrico y una alarma para los cambios en la VPC

[Config.1] AWS Config deben estar habilitados y usar la función vinculada al servicio para el registro de recursos

[EC2.2] Los grupos de seguridad predeterminados de VPC no deben permitir el tráfico entrante o saliente

[EC2.6] El registro de flujo de VPC debe estar habilitado en todas las VPC

[EC2.13] Los grupos de seguridad no deberían permitir la entrada desde la versión 0.0.0. 0/0 o: :/0 al puerto 22

[EC2.14] Los grupos de seguridad no deberían permitir la entrada desde la versión 0.0.0. 0/0 o: :/0 al puerto 3389

[IAM.1] Las políticas de IAM no deberían permitir todos los privilegios administrativos «*»

[IAM.2] Los usuarios de IAM no deberían tener políticas de IAM adjuntas

[IAM.3] Las claves de acceso de los usuarios de IAM deben rotarse cada 90 días o menos

[IAM.4] La clave de acceso del usuario raíz de IAM no debería existir

[IAM.5] La MFA debe estar habilitada para todos los usuarios de IAM que tengan una contraseña de consola

[IAM.6] La MFA de hardware debe estar habilitada para el usuario root

[IAM.8] Se deben eliminar las credenciales de usuario de IAM no utilizadas

[IAM.9] La MFA debe estar habilitada para el usuario root

[IAM.11] Asegúrese de que la política de contraseñas de IAM requiera al menos una letra mayúscula

[IAM.12] Asegúrese de que la política de contraseñas de IAM requiera al menos una letra minúscula

[IAM.13] Asegúrese de que la política de contraseñas de IAM requiera al menos un símbolo

[IAM.14] Asegúrese de que la política de contraseñas de IAM requiera al menos un número

[IAM.15] Asegúrese de que la política de contraseñas de IAM exija una longitud de contraseña mínima de 14 o más

[IAM.16] Asegúrese de que la política de contraseñas de IAM impida la reutilización de contraseñas

[IAM.17] Asegúrese de que la política de contraseñas de IAM haga caducar las contraseñas en un plazo de 90 días o menos

[IAM.18] Asegúrese de que se haya creado una función de soporte para gestionar los incidentes conAWS Support

[KMS.4]AWS KMSla rotación de claves debe estar habilitada

Comparación de versiones para CIS AWS Foundations Benchmark

En esta sección se resumen las diferencias entre las versiones específicas de Center for Internet Security (CIS) AWS Foundations Benchmark: v5.0.0, v3.0.0, v1.4.0 y v1.2.0. AWS Security Hub CSPM es compatible con cada una de estas versiones del CIS Foundations Benchmark. AWS Sin embargo, recomendamos usar la versión 5.0.0 para mantener actualizadas las prácticas recomendadas de seguridad. Puede tener habilitadas varias versiones de los estándares de CIS AWS Foundations Benchmark al mismo tiempo. Para obtener información sobre cómo habilitar estándares, consulte Habilitación de un estándar de seguridad. Si desea actualizar a la versión 5.0.0, habilítela antes de desactivar una versión anterior. Esto evita deficiencias en las comprobaciones de seguridad. Si utiliza la integración de Security Hub con CSPM AWS Organizations y quiere habilitarla por lotes en varias cuentas, le recomendamos que utilice una configuración central. ???

Asignación de los controles a los requisitos del CIS en cada versión

Comprenda qué controles admite cada versión de CIS AWS Foundations Benchmark.

ID y título de control	Requisito de CIS v5.0.0	Requisito del CIS v3.0.0	Requisito del CIS v1.4.0	Requisito del CIS v1.2.0
[Account.1] La información de contacto de seguridad debe proporcionarse para unCuenta de AWS	1.2	1.2	1.2	1.18
[CloudTrail.1] CloudTrail debe estar habilitado y configura do con al menos un registro multirregional que incluya eventos de administración de lectura y escritura	3.1	3.1	3.1	2.1
[CloudTrail.2] CloudTrail debe tener activado el cifrado en reposo	3.5	3.5	3.7	2.7
[CloudTrail.4] La validación del archivo de CloudTrail registro debe estar habilitada	3.2	3.2	3.2	2.2
[CloudTrail.5] los CloudTrai l senderos deben estar integrados con Amazon CloudWatch Logs	No compatibl e: el CIS eliminó este requisito	No compatibl e: el CIS eliminó este requisito	3.4	2.4
[CloudTrail.6] Asegúrese de que el depósito de S3 que se utiliza para almacenar CloudTrail los registros no sea de acceso público	No compatibl e: el CIS eliminó este requisito	No compatibl e: el CIS eliminó este requisito	3.3	2.3
[CloudTrail.7] Asegúrese de que el registro de acceso al bucket de S3 esté habilitado en el CloudTrail bucket de S3	3.4	3.4	3.6	2.6

ID y título de control	Requisito de CIS v5.0.0	Requisito del CIS v3.0.0	Requisito del CIS v1.4.0	Requisito del CIS v1.2.0
[CloudWatch.1] Debe existir un registro, un filtro métrico y una alarma para el uso del usuario «raíz»	No compatible: comprobación manual	No compatible: comprobación manual	4.3	3.3
[CloudWatch.2] Asegúrese de que existan un registro, un filtro métrico y una alarma para las llamadas a la API no autorizadas	No compatible: comprobación manual	No compatible: comprobación manual	No compatible: comprobación manual	3.1
[CloudWatch.3] Asegúrese de que haya un registro, un filtro métrico y una alarma para iniciar sesión en la consola de administración sin MFA	No compatible: comprobación manual	No compatible: comprobación manual	No compatible: comprobación manual	3.2
[CloudWatch.4] Asegúrese de que haya un registro, un filtro métrico y una alarma para los cambios en las políticas de IAM	No compatible: comprobación manual	No compatible: comprobación manual	4.4	3.4
[CloudWatch.5] Asegúrese de que existan un registro, un filtro métrico y una alarma para los cambios CloudTrail de configuración	No compatible: comprobación manual	No compatible: comprobación manual	4.5	3.5
[CloudWatch.6] Asegúrese de que existan un registro métrico, un filtro y una alarma para Consola de administración de AWS errores de autenticación	No compatible: comprobación manual	No compatible: comprobación manual	4.6	3.6

ID y título de control	Requisito de CIS v5.0.0	Requisito del CIS v3.0.0	Requisito del CIS v1.4.0	Requisito del CIS v1.2.0
[CloudWatch.7] Asegúrese de que haya un registro, un filtro métrico y una alarma para deshabilitar o programar la eliminación de las claves administradas por el cliente	No compatible: comprobación manual	No compatible: comprobación manual	4.7	3.7
[CloudWatch.8] Asegúrese de que haya un registro, un filtro métrico y una alarma para los cambios en la política de buckets de S3	No compatible: comprobación manual	No compatible: comprobación manual	4.8	3.8
[CloudWatch.9] Asegúrese de que existan un registro métrico, un filtro y una alarma para AWS Config cambios de configuración	No compatible: comprobación manual	No compatible: comprobación manual	4.9	3.9
[CloudWatch.10] Asegúrese de que haya un registro, un filtro métrico y una alarma para los cambios en los grupos de seguridad	No compatible: comprobación manual	No compatible: comprobación manual	4,10	3,10
[CloudWatch.11] Asegúrese de que existan un filtro métrico de registro y una alarma para los cambios en las listas de control de acceso a la red (NACL)	No compatible: comprobación manual	No compatible: comprobación manual	4,11	3,11

ID y título de control	Requisito de CIS v5.0.0	Requisito del CIS v3.0.0	Requisito del CIS v1.4.0	Requisito del CIS v1.2.0
[CloudWatch.12] Asegúrese de que haya un registro, un filtro métrico y una alarma para detectar los cambios en las pasarelas de red	No compatible: comprobación manual	No compatible: comprobación manual	4,12	3,12
[CloudWatch.13] Asegúrese de que haya un registro, un filtro métrico y una alarma para los cambios en la tabla de rutas	No compatible: comprobación manual	No compatible: comprobación manual	4,13	3.13
[CloudWatch.14] Asegúrese de que haya un registro, un filtro métrico y una alarma para los cambios en la VPC	No compatible: comprobación manual	No compatible: comprobación manual	4,14	3,14
[Config.1] AWS Config deben estar habilitados y usar la función vinculada al servicio para el registro de recursos	3.3	3.3	3.5	2,5
[EC2.2] Los grupos de seguridad predeterminados de VPC no deben permitir el tráfico entrante o saliente	5.5	5.4	5.3	4.3
[EC2.6] El registro de flujo de VPC debe estar habilitado en todas las VPC	3.7	3.7	3.9	2.9
[EC2.7] El cifrado predeterminado de EBS debe estar habilitado	5.1.1	2.2.1	2.2.1	No compatible

ID y título de control	Requisito de CIS v5.0.0	Requisito del CIS v3.0.0	Requisito del CIS v1.4.0	Requisito del CIS v1.2.0
[EC2.8] Las instancias EC2 deben utilizar la versión 2 del servicio de metadatos de instancia (IMDSv2)	5.7	5.6	No admitido	No admitido
[EC2.13] Los grupos de seguridad no deberían permitir la entrada desde la versión 0.0.0. 0/0 o: :/0 al puerto 22	No compatible: se sustituyó por los requisitos 5.3 y 5.4	No compatible: se sustituyó por los requisitos 5.2 y 5.3	No compatible: se sustituyó por los requisitos 5.2 y 5.3	4.1
[EC2.14] Los grupos de seguridad no deberían permitir la entrada desde la versión 0.0.0. 0/0 o: :/0 al puerto 3389	No compatible: se sustituyó por los requisitos 5.3 y 5.4	No compatible: se sustituyó por los requisitos 5.2 y 5.3	No compatible: se sustituyó por los requisitos 5.2 y 5.3	4.2
[EC2.21] Las ACL de red no deberían permitir la entrada desde la versión 0.0.0. 0/0 al puerto 22 o al puerto 3389	5.2	5.1	5.1	No compatible
[EC2.53] Los grupos de seguridad de EC2 no deberían permitir la entrada desde la versión 0.0.0. 0/0 a los puertos de administración remota del servidor	5.3	5.2	No admitido	No admitido
[EC2.54] Los grupos de seguridad de EC2 no deberían permitir la entrada desde: :/0 a los puertos de administración remota del servidor	5.4	5.3	No admitido	No admitido

ID y título de control	Requisito de CIS v5.0.0	Requisito del CIS v3.0.0	Requisito del CIS v1.4.0	Requisito del CIS v1.2.0
[EFS.1] Elastic File System debe configurarse para cifrar los datos de los archivos en reposo mediante AWS KMS	2.3.1	2.4.1	No admitido	No admitido
[EFS.8] Los sistemas de archivos EFS deben cifrarse en reposo	2.3.1	No admitido	No admitido	No admitido
[IAM.1] Las políticas de IAM no deberían permitir todos los privilegios administrativos «*»	No admitido	No admitido	1.16	1,22
[IAM.2] Los usuarios de IAM no deberían tener políticas de IAM adjuntas	1.14	1.15	No compatible	1.16
[IAM.3] Las claves de acceso de los usuarios de IAM deben rotarse cada 90 días o menos	1.13	1.14	1.14	1.4
[IAM.4] La clave de acceso del usuario raíz de IAM no debería existir	1.3	1.4	1.4	1.12
[IAM.5] La MFA debe estar habilitada para todos los usuarios de IAM que tengan una contraseña de consola	1.9	1.10	1.10	1.2
[IAM.6] La MFA de hardware debe estar habilitada para el usuario root	1.5	1.6	1.6	1.14

ID y título de control	Requisito de CIS v5.0.0	Requisito del CIS v3.0.0	Requisito del CIS v1.4.0	Requisito del CIS v1.2.0
[IAM.8] Se deben eliminar las credenciales de usuario de IAM no utilizadas	No se admite: consulte [IAM.22] Se deben eliminar las credenciales de usuario de IAM que no se hayan utilizado durante 45 días en su lugar	No se admite: consulte [IAM.22] Se deben eliminar las credenciales de usuario de IAM que no se hayan utilizado durante 45 días en su lugar	No se admite: consulte [IAM.22] Se deben eliminar las credenciales de usuario de IAM que no se hayan utilizado durante 45 días en su lugar	1.3
[IAM.9] La MFA debe estar habilitada para el usuario root	1.4	1.5	1.5	1.13
[IAM.11] Asegúrese de que la política de contraseñas de IAM requiera al menos una letra mayúscula	No compatible: el CIS eliminó este requisito	No compatible: el CIS eliminó este requisito	No compatible: el CIS eliminó este requisito	1.5
[IAM.12] Asegúrese de que la política de contraseñas de IAM requiera al menos una letra minúscula	No compatible: el CIS eliminó este requisito	No compatible: el CIS eliminó este requisito	No compatible: el CIS eliminó este requisito	1.6
[IAM.13] Asegúrese de que la política de contraseñas de IAM requiera al menos un símbolo	No compatible: el CIS eliminó este requisito	No compatible: el CIS eliminó este requisito	No compatible: el CIS eliminó este requisito	1.7

ID y título de control	Requisito de CIS v5.0.0	Requisito del CIS v3.0.0	Requisito del CIS v1.4.0	Requisito del CIS v1.2.0
[IAM.14] Asegúrese de que la política de contraseñas de IAM requiera al menos un número	No compatible: el CIS eliminó este requisito	No compatible: el CIS eliminó este requisito	No compatible: el CIS eliminó este requisito	1.8
[IAM.15] Asegúrese de que la política de contraseñas de IAM exija una longitud de contraseña mínima de 14 o más	1.7	1.8	1.8	1.9
[IAM.16] Asegúrese de que la política de contraseñas de IAM impida la reutilización de contraseñas	1.8	1.9	1.9	1.10
[IAM.17] Asegúrese de que la política de contraseñas de IAM haga caducar las contraseñas en un plazo de 90 días o menos	No compatible: el CIS eliminó este requisito	No compatible: el CIS eliminó este requisito	No compatible: el CIS eliminó este requisito	1.11
[IAM.18] Asegúrese de que se haya creado una función de soporte para gestionar los incidentes conAWS Support	1.16	1,17	1,17	1.2
[IAM.20] Evite el uso del usuario root	No compatible: el CIS eliminó este requisito	No compatible: el CIS eliminó este requisito	No compatible: el CIS eliminó este requisito	1.1

ID y título de control	Requisito de CIS v5.0.0	Requisito del CIS v3.0.0	Requisito del CIS v1.4.0	Requisito del CIS v1.2.0
[IAM.22] Se deben eliminar las credenciales de usuario de IAM que no se hayan utilizado durante 45 días	1.11	1.12	1.12	No compatible: el CIS agregó este requisito en versiones posteriores
[IAM.26] SSL/TLS Los certificados caducados gestionados en IAM deben eliminarse	1,18	1,19	No compatible: el CIS agregó este requisito en versiones posteriores	No compatible: el CIS agregó este requisito en versiones posteriores
[IAM.27] Las identidades de IAM no deberían tener la AWSCloudShellFullAccess política adjunta	1,21	1,22	No compatible: el CIS agregó este requisito en versiones posteriores	No compatible: el CIS agregó este requisito en versiones posteriores
[IAM.28] El analizador de acceso externo de IAM Access Analyzer debe estar habilitado	1,19	1,20	No compatible: el CIS agregó este requisito en versiones posteriores	No compatible: el CIS agregó este requisito en versiones posteriores
[KMS.4]AWS KMSla rotación de claves debe estar habilitada	3.6	3.6	3.8	2.8
[Macie.1] Amazon Macie debería estar activado	No compatible: comprobación manual	No compatible: comprobación manual	No compatible: comprobación manual	No compatible: comprobación manual

ID y título de control	Requisito de CIS v5.0.0	Requisito del CIS v3.0.0	Requisito del CIS v1.4.0	Requisito del CIS v1.2.0
[RDS.2] Las instancias de base de datos de RDS deben prohibir el acceso público, según lo determine la configuración PubliclyAccessible	2.2.3	2.3.3	No compatible: el CIS agregó este requisito en versiones posteriores	No compatible: el CIS agregó este requisito en versiones posteriores
[RDS.3] Las instancias de base de datos de RDS deben tener habilitado el cifrado en reposo	2.2.1	2.3.1	2.3.1	No compatible: el CIS agregó este requisito en versiones posteriores
[RDS.5] Las instancias de base de datos de RDS deben configurarse con varias zonas de disponibilidad	2.2.4	No compatible: el CIS agregó este requisito en versiones posteriores	No compatible: el CIS agregó este requisito en versiones posteriores	No compatible: el CIS agregó este requisito en versiones posteriores
[RDS.13] Las actualizaciones automáticas de las versiones secundarias de RDS deben estar habilitadas	2.2.2	2.3.2	No compatible: el CIS agregó este requisito en versiones posteriores	No compatible: el CIS agregó este requisito en versiones posteriores
[RDS.15] Los clústeres de bases de datos de RDS deben configurarse para varias zonas de disponibilidad	2.2.4	No compatible: el CIS agregó este requisito en versiones posteriores	No compatible: el CIS agregó este requisito en versiones posteriores	No compatible: el CIS agregó este requisito en versiones posteriores

ID y título de control	Requisito de CIS v5.0.0	Requisito del CIS v3.0.0	Requisito del CIS v1.4.0	Requisito del CIS v1.2.0
[S3.1] Los cubos de uso general de S3 deben tener habilitada la configuración de bloqueo del acceso público	2.1.4	2.1.4	2.1.5	No compatible: el CIS agregó este requisito en versiones posteriores
[S3.5] Los cubos de uso general de S3 deberían requerir que las solicitudes usen TLS	2.1.1	2.1.1	2.1.2	No compatible: el CIS agregó este requisito en versiones posteriores
[S3.8] Los cubos de uso general de S3 deben bloquear el acceso público	2.1.4	2.1.4	2.1.5	No compatible: el CIS agregó este requisito en versiones posteriores
[S3.20] Los cubos de uso general de S3 deben tener habilitada la eliminación de MFA	2.1.2	2.1.2	2.1.3	No compatible: el CIS agregó este requisito en versiones posteriores

ARN para CIS AWS Principios y puntos de referencia

Cuando habilita una o más versiones del CIS AWS Foundations Benchmark, comienza a recibir los resultados en el formato de evaluación de AWS seguridad (ASFF). En el ASFF, cada versión utiliza el siguiente nombre de recurso de Amazon (ARN):

CIS AWS Foundations Benchmark v5.0.0

```
arn:aws:securityhub:region::standards/cis-aws-foundations-benchmark/
v/5.0.0
```

CIS AWS Foundations Benchmark v3.0.0

```
arn:aws:securityhub:region::standards/cis-aws-foundations-benchmark/
v/3.0.0
```

CIS AWS Foundations Benchmark v1.4.0

```
arn:aws:securityhub:region::standards/cis-aws-foundations-benchmark/
v/1.4.0
```

CIS AWS Foundations Benchmark v1.2.0

```
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0
```

Puede utilizar la operación GetEnabledStandards de la API del CSPM de Security Hub para averiguar el ARN de un estándar habilitado.

Los valores anteriores son para `StandardsArn`. Sin embargo, `StandardsSubscriptionArn` hace referencia al recurso de suscripción estándar que el CSPM de Security Hub crea cuando se suscribe a un estándar mediante una llamada a BatchEnableStandards en una región.

> **Note**
>
> Cuando se habilita una versión de CIS AWS Foundations Benchmark, Security Hub CSPM puede tardar hasta 18 horas en detectar los controles que utilizan la misma regla AWS Config vinculada a los servicios que los controles habilitados en otros estándares habilitados. Para obtener más información sobre el programa para generar resultados de control, consulte Programación para ejecutar comprobaciones de seguridad.

Los campos de resultados serán diferentes si activa los resultados de los controles consolidados. Para obtener más información sobre estas diferencias, consulte Impacto de la consolidación en los campos y valores ASFF. Para ver ejemplos de los resultados de los controles, consulte Ejemplos de resultados de controles.

Requisitos del CIS que no se admiten en el CSPM de Security Hub

Como se indica en la tabla anterior, el CSPM de Security Hub no admite todos los requisitos del CIS en todas las versiones del CIS Foundations Benchmark. AWS Muchos de los requisitos no compatibles solo se pueden evaluar de forma manual al revisar el estado de los recursos de AWS .

Revisión 5 de NIST SP 800-53 en el CSPM de Security Hub

La publicación especial 800-53 del NIST, revisión 5 (NIST SP 800-53 Rev. 5) es un marco de ciberseguridad y cumplimiento desarrollado por el Instituto Nacional de Estándares y Tecnología (NIST), una agencia que forma parte del. U.S Departamento de Comercio. Este marco de cumplimiento proporciona un catálogo de requisitos de seguridad y privacidad para proteger la confidencialidad, la integridad y la disponibilidad de los sistemas de información y los recursos críticos. U.S. Las agencias del gobierno federal y los contratistas deben cumplir con estos requisitos para proteger sus sistemas y organizaciones. Las organizaciones privadas también pueden usar estos requisitos de manera voluntaria como marco orientador para reducir el riesgo de ciberseguridad. Para obtener más información sobre el marco y sus requisitos, consulte NIST SP 800-53 Rev. 5 en el Centro de Recursos de Seguridad Informática de NIST.

AWS Security Hub CSPM proporciona controles de seguridad que admiten un subconjunto de los requisitos de la revisión 5 del SP 800-53 del NIST. Los controles realizan comprobaciones de seguridad automatizadas para determinados recursos. Servicios de AWS Para habilitar y administrar estos controles, puede habilitar el marco NIST SP 800-53 Revisión 5 como un estándar en el CSPM de Security Hub. Tenga en cuenta que los controles no admiten los requisitos de NIST SP 800-53 Revisión 5 que requieren comprobaciones manuales.

A diferencia de otros marcos, NIST SP 800-53 Revisión 5 no prescribe cómo se deben evaluar sus requisitos. En su lugar, el marco proporciona directrices. En el CSPM de Security Hub, el estándar NIST SP 800-53 Revisión 5 y sus controles representan la interpretación que hace el servicio de estas directrices.

Temas

- Configuración del registro de recursos para los controles que se aplican al estándar
- Cómo determinar qué controles se aplican al estándar

Configuración del registro de recursos para los controles que se aplican al estándar

Para optimizar la cobertura y la precisión de los hallazgos, es importante habilitar y configurar el registro de los recursos AWS Config antes de habilitar el estándar NIST SP 800-53, revisión 5, en

AWS Security Hub CSPM. Al configurar el registro de recursos, asegúrese también de habilitarlo para todos los tipos de AWS recursos que se comprueban mediante los controles que se aplican a la norma. Esto se aplica principalmente a los controles que tienen un tipo de programación activado por cambios. Sin embargo, algunos controles con un tipo de programación periódica también requieren el registro de recursos. Si el registro de recursos no está habilitado o no está configurado correctamente, es posible que el CSPM de Security Hub no pueda evaluar los recursos correspondientes ni generar resultados precisos para los controles que se aplican al estándar.

Para obtener información sobre cómo Security Hub CSPM utiliza el registro de recursos en AWS Config, consulte. Activación y configuración AWS Config para Security Hub CSPM Para obtener información sobre cómo configurar el registro de recursos en AWS Config, consulte Trabajar con el grabador de configuración en la Guía para AWS Config desarrolladores.

La siguiente tabla especifica los tipos de recursos que se deben registrar para los controles que se aplican al estándar NIST SP 800-53 Revisión 5 en el CSPM de Security Hub.

Servicio de AWS	Tipos de recurso
Amazon API Gateway	`AWS::ApiGateway::Stage`, `AWS::ApiGatewayV2::Stage`
AWS AppSync	`AWS::AppSync::GraphQLApi`
AWS Backup	`AWS::Backup::RecoveryPoint`
Amazon Bedrock AgentCore	`AWS::BedrockAgentCore::Gateway`, `AWS::BedrockAgentCore::Memory`
AWS Gestor de certificados (ACM)	`AWS::ACM::Certificate`
AWS CloudFormation	`AWS::CloudFormation::Stack`
Amazon CloudFront	`AWS::CloudFront::Distribution`
Amazon CloudWatch	`AWS::CloudWatch::Alarm`
AWS CodeBuild	`AWS::CodeBuild::Project`

Servicio de AWS	Tipos de recurso
AWS Database Migration Service (AWS DMS)	`AWS::DMS::Endpoint`, `AWS::DMS::ReplicationInstance`, `AWS::DMS::ReplicationTask`
Amazon DynamoDB	`AWS::DynamoDB::Table`
Amazon Elastic Compute Cloud (Amazon EC2)	`AWS::EC2::ClientVpnEndpoint`, `AWS::EC2::EIP`, `AWS::EC2::Instance`, `AWS::EC2::LaunchTemplate`, `AWS::EC2::NetworkAcl`, `AWS::EC2::NetworkInterface`, `AWS::EC2::SecurityGroup`, `AWS::EC2::Subnet`, `AWS::EC2::TransitGateway`, `AWS::EC2::VPNConnection`, `AWS::EC2::Volume`
Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup`, `AWS::AutoScaling::LaunchConfiguration`
Amazon Elastic Container Registry (Amazon ECR)	`AWS::ECR::Repository`
Amazon Elastic Container Service (Amazon ECS)	`AWS::ECS::Cluster`, `AWS::ECS::Service`, `AWS::ECS::TaskDefinition`
Amazon Elastic File System (Amazon EFS)	`AWS::EFS::AccessPoint`
Amazon Elastic Kubernetes Service (Amazon EKS)	`AWS::EKS::Cluster`
AWS Elastic Beanstalk	`AWS::ElasticBeanstalk::Environment`

Servicio de AWS	Tipos de recurso
Elastic Load Balancing	`AWS::ElasticLoadBalancing::LoadBalancer`, `AWS::ElasticLoadBalancingV2::Listener`, `AWS::ElasticLoadBalancingV2::LoadBalancer`
Amazon ElasticSearch	`AWS::Elasticsearch::Domain`
Amazon EMR	`AWS::EMR::SecurityConfiguration`
Amazon EventBridge	`AWS::Events::Endpoint`, `AWS::Events::EventBus`
AWS Glue	`AWS::Glue::Job`
AWS Identity and Access Management (IAM)	`AWS::IAM::Group`, `AWS::IAM::Policy`, `AWS::IAM::Role`, `AWS::IAM::User`
AWS Key Management Service (AWS KMS)	`AWS::KMS::Alias`, `AWS::KMS::Key`
Amazon Kinesis	`AWS::Kinesis::Stream`
AWS Lambda	`AWS::Lambda::Function`
Amazon Managed Streaming para Apache Kafka (Amazon MSK)	`AWS::MSK::Cluster`
Amazon MQ	`AWS::AmazonMQ::Broker`
AWS Network Firewall	`AWS::NetworkFirewall::Firewall`, `AWS::NetworkFirewall::FirewallPolicy`, `AWS::NetworkFirewall::RuleGroup`
Servicio Amazon OpenSearch	`AWS::OpenSearch::Domain`

Servicio de AWS	Tipos de recurso
Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBCluster`, `AWS::RDS::DBClusterSnapshot`, `AWS::RDS::DBInstance`, `AWS::RDS::DBSnapshot`, `AWS::RDS::EventSubscription`
Amazon Redshift	`AWS::Redshift::Cluster`, `AWS::Redshift::ClusterSubnetGroup`
Amazon Route 53	`AWS::Route53::HostedZone`
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::AccessPoint`, `AWS::S3::AccountPublicAccessBlock`, `AWS::S3::Bucket`
AWS Service Catalog	`AWS::ServiceCatalog::Portfolio`
Amazon Simple Notification Service (Amazon SNS)	`AWS::SNS::Topic`
Amazon Simple Queue Service (Amazon SQS)	`AWS::SQS::Queue`
Amazon EC2 Systems Manager (SSM)	`AWS::SSM::AssociationCompliance`, `AWS::SSM::ManagedInstanceInventory`, `AWS::SSM::PatchCompliance`
SageMaker Inteligencia artificial de Amazon	`AWS::SageMaker::FeatureGroup`, `AWS::SageMaker::NotebookInstance`
AWS Secrets Manager	`AWS::SecretsManager::Secret`
AWS Transfer Family	`AWS::Transfer::Connector`

Servicio de AWS	Tipos de recurso
AWS WAF	`AWS::WAF::Rule` , `AWS::WAF::RuleGroup` , `AWS::WAF::WebACL` , `AWS::WAFRegional::Rule` , `AWS::WAFRegional::RuleGroup` , `AWS::WAFRegional::WebACL` , `AWS::WAFv2::RuleGroup` , `AWS::WAFv2::WebACL`

Cómo determinar qué controles se aplican al estándar

En la siguiente lista se especifican los controles que cumplen con los requisitos de la revisión 5 del NIST SP 800-53 y se aplican al estándar NIST SP 800-53, revisión 5, de Security Hub CSPM. AWS Para ver los detalles sobre los requisitos específicos que admite un control, seleccione el control. Luego, consulte el campo Requisitos relacionados en los detalles del control. Este campo especifica cada requisito de NIST que admite el control. Si el campo no especifica un requisito concreto de NIST, el control no admite ese requisito.

- [Account.1] La información de contacto de seguridad debe proporcionarse para unCuenta de AWS
- [Account.2]Cuentas de AWSdebe formar parte de unAWS Organizationsorganización
- [ACM.1] ACM-issued Los certificados importados y renovados deben renovarse después de un período de tiempo específico
- [APIGateway.1] El registro de ejecución de API y REST de WebSocket API Gateway deben estar habilitados.
- [APIGateway.2] Las etapas de la API REST de API Gateway deben configurarse para usar certificados SSL para la autenticación de backend
- [APIGateway.3] Las etapas de la API REST de API Gateway deben tener AWS X-Ray rastreo habilitado
- [APIGateway.4] API Gateway debe estar asociada a una ACL web de WAF
- [APIGateway.5] Los datos de la caché de la API REST de API Gateway deben cifrarse en reposo
- [APIGateway.8] Las rutas de API Gateway deben especificar un tipo de autorización
- [APIGateway.9] El registro de acceso debe configurarse para las etapas V2 de API Gateway
- [AppSync.5]AWS AppSyncLas API de GraphQL no deben autenticarse con claves de API

- [AutoScaling.1] Los grupos de Auto Scaling asociados a un balanceador de cargas deben usar comprobaciones de estado del ELB
- [AutoScaling.2] El grupo Amazon EC2 Auto Scaling debe cubrir varias zonas de disponibilidad
- [AutoScaling.3] Las configuraciones de lanzamiento grupal de Auto Scaling deberían configurar las instancias EC2 para que requieran la versión 2 del Servicio de Metadatos de Instancia (IMDSv2)
- [Autoscaling.5] Las instancias de Amazon EC2 lanzadas mediante configuraciones de lanzamiento grupal de Auto Scaling no deben tener direcciones IP públicas
- [AutoScaling.6] Los grupos de Auto Scaling deben usar varios tipos de instancias en múltiples zonas de disponibilidad
- [AutoScaling.9] Los grupos de Amazon EC2 Auto Scaling deben utilizar las plantillas de lanzamiento de Amazon EC2
- [Backup.1]AWS Backuplos puntos de recuperación deben estar cifrados en reposo
- [BedrockAgentCore.3] Bedrock AgentCore Memory debe estar cifrada y gestionada por el clienteAWS KMSclaves
- [BedrockAgentCore.4] Bedrock AgentCore Gateway debe cifrarse de forma que sea gestionada por el clienteAWS KMSclaves
- [CloudFront.1] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado
- [CloudFront.3] CloudFront las distribuciones deben requerir el cifrado durante el tránsito
- [CloudFront.4] CloudFront las distribuciones deben tener configurada la conmutación por error de origen
- [CloudFront.5] CloudFront las distribuciones deben tener habilitado el registro
- [CloudFront.6] CloudFront las distribuciones deben tener WAF activado
- [CloudFront.7] CloudFront las distribuciones deben usar certificados personalizados SSL/TLS
- [CloudFront.8] CloudFront las distribuciones deben usar el SNI para atender las solicitudes HTTPS
- [CloudFront.9] CloudFront las distribuciones deben cifrar el tráfico para convertirlo en orígenes personalizados
- [CloudFront.10] CloudFront las distribuciones no deben usar protocolos SSL obsoletos entre ubicaciones de borde y orígenes personalizados
- [CloudFront.12] CloudFront las distribuciones no deben apuntar a orígenes de S3 inexistentes
- [CloudTrail.1] CloudTrail debe estar habilitado y configurado con al menos un registro multirregional que incluya eventos de administración de lectura y escritura

- [CloudTrail.2] CloudTrail debe tener activado el cifrado en reposo
- [CloudTrail.4] La validación del archivo de CloudTrail registro debe estar habilitada
- [CloudTrail.5] los CloudTrail senderos deben estar integrados con Amazon CloudWatch Logs
- [CloudTrail.10] Los almacenes de datos de eventos de CloudTrail Lake deben estar cifrados y gestionados por el clienteAWS KMS keys
- [CloudWatch.15] CloudWatch las alarmas deben tener configuradas acciones específicas
- [CloudWatch.16] los grupos de CloudWatch registros deben conservarse durante un período de tiempo específico
- [CloudWatch.17] las acciones CloudWatch de alarma deben estar activadas
- [CodeBuild.1] Las URL del repositorio fuente de CodeBuild Bitbucket no deben contener credenciales confidenciales
- [CodeBuild.2] las variables de entorno CodeBuild del proyecto no deben contener credenciales de texto claro
- [CodeBuild.3] Los registros de CodeBuild S3 deben estar cifrados
- [CodeBuild.4] los entornos de CodeBuild proyectos deben tener un registroAWS ConfigDuración
- [Config.1] AWS Config deben estar habilitados y usar la función vinculada al servicio para el registro de recursos
- [DataFirehose.1] Los flujos de entrega de Firehose deben cifrarse en reposo
- [DMS.1] Las instancias de replicación de Database Migration Service no deben ser públicas
- [DMS.6] Las instancias de replicación de DMS deben tener habilitada la actualización automática de las versiones secundarias
- [DMS.7] Las tareas de replicación del DMS para la base de datos de destino deben tener el registro habilitado
- [DMS.8] Las tareas de replicación del DMS para la base de datos de origen deben tener el registro activado
- [DMS.9] Los puntos finales del DMS deben usar SSL
- [DMS.10] Los puntos finales de DMS para las bases de datos de Neptune deben tener habilitada la autorización de IAM
- [DMS.11] Los puntos finales de DMS para MongoDB deben tener un mecanismo de autenticación habilitado
- [DMS.12] Los puntos finales de DMS para Redis OSS deben tener el TLS habilitado
- [DocumentDB.1] Los clústeres de Amazon DocumentDB deben cifrarse en reposo

- [DocumentDB.2] Los clústeres de Amazon DocumentDB deben tener un período de retención de copias de seguridad adecuado
- [DocumentDB.3] Las instantáneas de clústeres manuales de Amazon DocumentDB no deben ser públicas
- [DocumentDB.4] Los clústeres de Amazon DocumentDB deben publicar los registros de auditoría en Logs CloudWatch
- [DocumentDB.5] Los clústeres de Amazon DocumentDB deben tener habilitada la protección contra eliminaciones
- [DynamoDB.1] Las tablas de DynamoDB deberían escalar automáticamente la capacidad en función de la demanda
- [DynamoDB.2] Las tablas de DynamoDB deben tener habilitada la recuperación puntual
- [DynamoDB.3] Los clústeres de DynamoDB Accelerator (DAX) deben cifrarse en reposo
- [DynamoDB.4] Las tablas de DynamoDB deben estar presentes en un plan de respaldo
- [DynamoDB.6] Las tablas de DynamoDB deben tener habilitada la protección de eliminación
- [DynamoDB.7] Los clústeres de DynamoDB Accelerator deben cifrarse en tránsito
- [EC2.1] Las instantáneas de Amazon EBS no deben configurarse para que se puedan restaurar públicamente
- [EC2.2] Los grupos de seguridad predeterminados de VPC no deben permitir el tráfico entrante o saliente
- [EC2.3] Los volúmenes adjuntos de Amazon EBS deben cifrarse en reposo
- [EC2.4] Las instancias EC2 detenidas deben eliminarse después de un período de tiempo específico
- [EC2.6] El registro de flujo de VPC debe estar habilitado en todas las VPC
- [EC2.7] El cifrado predeterminado de EBS debe estar habilitado
- [EC2.8] Las instancias EC2 deben utilizar la versión 2 del servicio de metadatos de instancia (IMDSv2)
- [EC2.9] Las instancias de Amazon EC2 no deben tener una dirección IPv4 pública
- [EC2.10] Amazon EC2 debe configurarse para utilizar los puntos de enlace de VPC que se crean para el servicio Amazon EC2
- [EC2.12] Deben eliminarse las EIP de Amazon EC2 no utilizadas
- [EC2.13] Los grupos de seguridad no deberían permitir la entrada desde la versión 0.0.0. 0/0 o: :/0 al puerto 22

- [EC2.15] Las subredes de Amazon EC2 no deben asignar automáticamente direcciones IP públicas
- [EC2.16] Se deben eliminar las listas de control de acceso a la red no utilizadas
- [EC2.17] Las instancias de Amazon EC2 no deben usar varios ENI
- [EC2.18] Los grupos de seguridad solo deben permitir el tráfico entrante sin restricciones en los puertos autorizados
- [EC2.19] Los grupos de seguridad no deben permitir el acceso irrestricto a los puertos de alto riesgo
- [EC2.20] Ambos túneles VPN para un AWS Site-to-Site La conexión VPN debería estar activa
- [EC2.21] Las ACL de red no deberían permitir la entrada desde la versión 0.0.0. 0/0 al puerto 22 o al puerto 3389
- [EC2.23] Amazon EC2 Transit Gateways no debe aceptar automáticamente las solicitudes de adjuntos de VPC
- [EC2.24] No se deben utilizar los tipos de instancias paravirtuales de Amazon EC2
- [EC2.25] Las plantillas de lanzamiento de Amazon EC2 no deben asignar direcciones IP públicas a las interfaces de red
- [EC2.28] Los volúmenes de EBS deben estar cubiertos por un plan de respaldo
- [EC2.51] Los puntos finales EC2 Client VPN deben tener habilitado el registro de conexiones de clientes
- [EC2.55] Las VPC deben configurarse con un punto final de interfaz para la API de ECR
- [EC2.56] Las VPC deben configurarse con un punto final de interfaz para Docker Registry
- [EC2.57] Las VPC deben configurarse con un punto final de interfaz para Systems Manager
- [EC2.58] Las VPC deben configurarse con un punto final de interfaz para los contactos de Systems Manager Incident Manager
- [EC2.60] Las VPC deben configurarse con un punto final de interfaz para Systems Manager Incident Manager
- [ECR.1] Los repositorios privados de ECR deben tener configurado el escaneo de imágenes
- [ECR.2] Los repositorios privados de ECR deben tener configurada la inmutabilidad de etiquetas
- [ECR.3] Los repositorios de ECR deben tener configurada al menos una política de ciclo de vida
- [ECR.5] Los repositorios de ECR deben estar cifrados y ser gestionados por el cliente AWS KMS keys

- [ECS.2] Los servicios de ECS no deberían tener direcciones IP públicas asignadas automáticamente
- [ECS.3] Las definiciones de tareas de ECS no deben compartir el espacio de nombres del proceso del host
- [ECS.4] Los contenedores ECS deben ejecutarse sin privilegios
- [ECS.5] Las definiciones de tareas de ECS deben configurar los contenedores para que se limiten al acceso de solo lectura a los sistemas de archivos raíz
- [ECS.8] Los secretos no deben transmitirse como variables de entorno de contenedores
- [ECS.9] Las definiciones de tareas de ECS deben tener una configuración de registro
- [ECS.10] Los servicios Fargate de ECS deberían ejecutarse en la última versión de la plataforma Fargate
- [ECS.12] Los clústeres de ECS deben usar Container Insights
- [ECS.17] Las definiciones de tareas de ECS no deben usar el modo de red host
- [EFS.1] Elastic File System debe configurarse para cifrar los datos de los archivos en reposo mediante AWS KMS
- [EFS.2] Los volúmenes de Amazon EFS deben figurar en los planes de copia de seguridad
- [EFS.3] Los puntos de acceso EFS deben exigir un directorio raíz
- [EFS.4] Los puntos de acceso EFS deben exigir la identidad del usuario
- [EFS.6] Los destinos de montaje de EFS no deben asociarse a subredes que asignan direcciones IP públicas en el momento del lanzamiento
- [EKS.1] Los puntos finales del clúster EKS no deben ser de acceso público
- [EKS.2] Los clústeres de EKS deben ejecutarse en una versión de Kubernetes compatible
- [EKS.3] Los clústeres de EKS deben usar secretos de Kubernetes cifrados
- [EKS.8] Los clústeres de EKS deben tener habilitado el registro de auditoría
- [ElastiCache.1] ElastiCache (Redis OSS) los clústeres deben tener habilitadas las copias de seguridad automáticas
- [ElastiCache.2] ElastiCache los clústeres deberían tener habilitadas las actualizaciones automáticas de las versiones secundarias
- [ElastiCache.3] los grupos de ElastiCache replicación deberían tener habilitada la conmutación por error automática
- [ElastiCache.4] los grupos de ElastiCache replicación deben cifrarse en reposo
- [ElastiCache.5] los grupos de ElastiCache replicación deben cifrarse en tránsito

- [ElastiCache.6] ElastiCache (Redis OSS) Los grupos de replicación de versiones anteriores deberían tener habilitada la autenticación de Redis OSS
- [ElastiCache.7] los ElastiCache clústeres no deben usar el grupo de subredes predeterminado
- [ElasticBeanstalk.1] Los entornos de Elastic Beanstalk deberían tener habilitados los informes de estado mejorados
- [ElasticBeanstalk.2] Las actualizaciones de la plataforma gestionada de Elastic Beanstalk deben estar habilitadas
- [ELB.1] El balanceador de carga de aplicaciones debe configurarse para redirigir todas las solicitudes HTTP a HTTPS
- [ELB.2] Los balanceadores de carga clásicos con SSL/HTTPS oyentes deben usar un certificado proporcionado por AWS Gestor de certificados
- [ELB.3] Los oyentes de Classic Load Balancer deben configurarse con terminación HTTPS o TLS
- [ELB.4] El balanceador de carga de aplicaciones debe configurarse para eliminar los encabezados http no válidos
- [ELB.5] El registro de los balanceadores de carga clásicos y de aplicaciones debería estar activado
- [ELB.6] Los balanceadores de cargas de aplicaciones, puertas de enlace y red deben tener habilitada la protección contra eliminaciones
- [ELB.7] Los balanceadores de carga clásicos deben tener activado el drenaje de conexiones
- [ELB.8] Los balanceadores de carga clásicos con receptores SSL deben usar una política de seguridad predefinida que sea sólida AWS Config Duración
- [ELB.9] Los balanceadores de carga clásicos deben tener habilitado el balanceo de cargas entre zonas
- [ELB.10] El balanceador de carga clásico debe abarcar varias zonas de disponibilidad
- [ELB.12] El balanceador de carga de aplicaciones debe configurarse con el modo defensivo o de mitigación de desincronización más estricto
- [ELB.13] Los balanceadores de carga de aplicaciones, redes y puertas de enlace deben abarcar varias zonas de disponibilidad
- [ELB.14] El balanceador de carga clásico debe configurarse con el modo defensivo o de mitigación de desincronización más estricto
- [ELB.16] Los balanceadores de carga de aplicaciones deben estar asociados a un AWS WAF ACL web
- [ELB.17] Los balanceadores de cargas de aplicaciones y redes con oyentes deben usar las políticas de seguridad recomendadas

- [EMR.1] Los nodos principales del clúster de Amazon EMR no deben tener direcciones IP públicas
- [EMR.2] La configuración de acceso público del bloque Amazon EMR debe estar habilitada
- [EMR.3] Las configuraciones de seguridad de Amazon EMR deben cifrarse en reposo
- [EMR.4] Las configuraciones de seguridad de Amazon EMR deben cifrarse en tránsito
- [ES.1] Los dominios de Elasticsearch deben tener habilitado el cifrado en reposo
- [ES.2] Los dominios de Elasticsearch no deben ser de acceso público
- [ES.3] Los dominios de Elasticsearch deben cifrar los datos enviados entre nodos
- [ES.4] Debería estar habilitado el registro de errores de dominio de Elasticsearch en Logs CloudWatch
- [ES.5] Los dominios de Elasticsearch deben tener habilitado el registro de auditoría
- [ES.6] Los dominios de Elasticsearch deben tener al menos tres nodos de datos
- [ES.7] Los dominios de Elasticsearch deben configurarse con al menos tres nodos maestros dedicados
- [ES.8] Las conexiones a los dominios de Elasticsearch deben cifrarse con la política de seguridad TLS más reciente
- [EventBridge.3] los autobuses de eventos EventBridge personalizados deben tener adjunta una política basada en los recursos
- [EventBridge.4] los puntos finales EventBridge globales deberían tener habilitada la replicación de eventos
- [FSx.1] FSx para sistemas de archivos OpenZFS debe configurarse para copiar etiquetas en copias de seguridad y volúmenes
- [FSx.2] Los sistemas de archivos FSx for Lustre deben configurarse para copiar etiquetas a las copias de seguridad
- [Glue.4]AWS GlueLos trabajos de Spark deberían ejecutarse en versiones compatibles deAWS Glue
- [GuardDuty.1] GuardDuty debería estar activado
- [IAM.1] Las políticas de IAM no deberían permitir todos los privilegios administrativos «*»
- [IAM.2] Los usuarios de IAM no deberían tener políticas de IAM adjuntas
- [IAM.3] Las claves de acceso de los usuarios de IAM deben rotarse cada 90 días o menos
- [IAM.4] La clave de acceso del usuario raíz de IAM no debería existir
- [IAM.5] La MFA debe estar habilitada para todos los usuarios de IAM que tengan una contraseña de consola

- [IAM.6] La MFA de hardware debe estar habilitada para el usuario root
- [IAM.7] Las políticas de contraseñas para los usuarios de IAM deben tener configuraciones sólidas
- [IAM.8] Se deben eliminar las credenciales de usuario de IAM no utilizadas
- [IAM.9] La MFA debe estar habilitada para el usuario root
- [IAM.19] La MFA debe estar habilitada para todos los usuarios de IAM
- [IAM.21] Las políticas de IAM gestionadas por el cliente que cree no deberían permitir acciones comodín en los servicios
- [Kinesis.1] Las transmisiones de Kinesis deben cifrarse en reposo
- [KMS.1] Las políticas gestionadas por los clientes de IAM no deberían permitir acciones de descifrado en todas las claves de KMS
- [KMS.2] Los directores de IAM no deberían tener políticas integradas de IAM que permitan realizar acciones de descifrado en todas las claves de KMS
- [KMS.3]AWS KMS keysno se debe eliminar involuntariamente
- [KMS.4]AWS KMSla rotación de claves debe estar habilitada
- [Lambda.1] Las políticas de las funciones de Lambda deberían prohibir el acceso público
- [Lambda.2] Las funciones de Lambda deben usar los tiempos de ejecución compatibles
- [Lambda.3] Las funciones de Lambda deben estar en una VPC
- [Lambda.5] Las funciones de VPC Lambda deben funcionar en varias zonas de disponibilidad
- [Lambda.7] Las funciones de Lambda deberían tener AWS X-Ray el rastreo activo está habilitado
- [Macie.1] Amazon Macie debería estar activado
- [Macie.2] La detección automática de datos confidenciales por parte de Macie debería estar habilitada
- [MSK.1] Los clústeres de MSK deben cifrarse en tránsito entre los nodos de intermediación
- [MSK.2] Los clústeres de MSK deberían tener configurada una supervisión mejorada
- [MQ.2] Los corredores de ActiveMQ deben transmitir los registros de auditoría a CloudWatch
- [MQ.5] Los corredores de ActiveMQ deberían usar el modo de implementación active/standby
- [MQ.6] Los corredores de RabbitMQ deberían usar el modo de despliegue de clústeres
- [Neptune.1] Los clústeres de bases de datos de Neptune deben cifrarse en reposo
- [Neptune.2] Los clústeres de bases de datos de Neptune deberían publicar registros de auditoría en Logs CloudWatch

- [Neptune.3] Las instantáneas del clúster de base de datos de Neptune no deben ser públicas
- [Neptune.4] Los clústeres de base de datos de Neptune deben tener habilitada la protección contra eliminación
- [Neptune.5] Los clústeres de Neptune DB deberían tener habilitadas las copias de seguridad automatizadas
- [Neptune.6] Las instantáneas del clúster de base de datos de Neptune deben cifrarse en reposo
- [Neptune.7] Los clústeres de base de datos de Neptune deben tener habilitada la autenticación de bases de datos de IAM
- [Neptune.8] Los clústeres de bases de datos de Neptune deben configurarse para copiar etiquetas a las instantáneas
- [Neptune.9] Los clústeres de base de datos Neptune deben implementarse en varias zonas de disponibilidad
- [NetworkFirewall.1] Los firewalls de Network Firewall deben implementarse en varias zonas de disponibilidad
- [NetworkFirewall.2] El registro de Network Firewall debe estar habilitado
- [NetworkFirewall.3] Las políticas de Network Firewall deben tener asociado al menos un grupo de reglas
- [NetworkFirewall.4] La acción sin estado predeterminada para las políticas de Network Firewall debe ser eliminar o reenviar paquetes completos
- [NetworkFirewall.5] La acción sin estado predeterminada para las políticas de Network Firewall debe ser eliminar o reenviar paquetes fragmentados
- [NetworkFirewall.6] El grupo de reglas de Stateless Network Firewall no debe estar vacío
- [NetworkFirewall.9] Los firewalls de Network Firewall deben tener habilitada la protección de eliminación
- [NetworkFirewall.10] Los firewalls de Network Firewall deben tener habilitada la protección contra cambios de subred
- [Opensearch.1] OpenSearch los dominios deben tener activado el cifrado en reposo
- [Opensearch.2] OpenSearch los dominios no deben ser de acceso público
- [Opensearch.3] OpenSearch los dominios deben cifrar los datos enviados entre nodos
- [Opensearch.4] El registro de errores de OpenSearch dominio en Logs debe estar habilitado CloudWatch
- [Opensearch.5] OpenSearch los dominios deben tener activado el registro de auditoría

- [Opensearch.6] OpenSearch los dominios deben tener al menos tres nodos de datos
- [Opensearch.7] OpenSearch los dominios deben tener habilitado un control de acceso detallado
- [Opensearch.8] Las conexiones a los OpenSearch dominios deben cifrarse con la última política de seguridad de TLS
- [Opensearch.10] OpenSearch los dominios deben tener instalada la última actualización de software
- [Opensearch.11] OpenSearch los dominios deben tener al menos tres nodos principales dedicados
- [PCA.1]AWS Privada CALa autoridad emisora de certificados raíz debe estar deshabilitada
- [RDS.1] La instantánea de RDS debe ser privada
- [RDS.2] Las instancias de base de datos de RDS deben prohibir el acceso público, según lo determine la configuración PubliclyAccessible
- [RDS.3] Las instancias de base de datos de RDS deben tener habilitado el cifrado en reposo
- [RDS.4] Las instantáneas de clústeres de RDS y las instantáneas de bases de datos deben cifrarse en reposo
- [RDS.5] Las instancias de base de datos de RDS deben configurarse con varias zonas de disponibilidad
- [RDS.6] Se debe configurar una supervisión mejorada para las instancias de base de datos de RDS
- [RDS.7] Los clústeres de RDS deben tener habilitada la protección contra eliminaciones
- [RDS.8] Las instancias de base de datos de RDS deben tener habilitada la protección contra eliminaciones
- [RDS.9] Las instancias de base de datos de RDS deben publicar los registros en Logs CloudWatch
- [RDS.10] La autenticación de IAM debe configurarse para las instancias de RDS
- [RDS.11] Las instancias de RDS deben tener habilitadas las copias de seguridad automáticas
- [RDS.12] La autenticación de IAM debe configurarse para los clústeres de RDS
- [RDS.13] Las actualizaciones automáticas de las versiones secundarias de RDS deben estar habilitadas
- [RDS.14] Los clústeres de Amazon Aurora deben tener habilitado el retroceso
- [RDS.15] Los clústeres de bases de datos de RDS deben configurarse para varias zonas de disponibilidad
- [RDS.16] Los clústeres de bases de datos de Aurora deben configurarse para copiar las etiquetas a las instantáneas de bases de datos

- [RDS.17] Las instancias de base de datos de RDS deben configurarse para copiar las etiquetas de las instantáneas
- [RDS.19] Las suscripciones de notificación de eventos de RDS existentes deben configurarse para los eventos críticos del clúster
- [RDS.20] Las suscripciones de notificación de eventos de RDS existentes deben configurarse para los eventos críticos de las instancias de bases de datos
- [RDS.21] Se debe configurar una suscripción a las notificaciones de eventos de RDS para los eventos de grupos de parámetros de base de datos críticos
- [RDS.22] Se debe configurar una suscripción a las notificaciones de eventos de RDS para los eventos críticos de grupos de seguridad de bases de datos
- [RDS.23] Las instancias de RDS no deben usar el puerto predeterminado de un motor de base de datos
- [RDS.24] Los clústeres de bases de datos de RDS deben usar un nombre de usuario de administrador personalizado
- [RDS.25] Las instancias de bases de datos de RDS deben usar un nombre de usuario de administrador personalizado
- [RDS.26] Las instancias de base de datos de RDS deben protegerse mediante un plan de respaldo
- [RDS.27] Los clústeres de bases de datos de RDS deben cifrarse en reposo
- [RDS.34] Los clústeres de bases de datos Aurora MySQL deben publicar los registros de auditoría en Logs CloudWatch
- [RDS.35] Los clústeres de bases de datos de RDS deben tener habilitada la actualización automática de versiones secundarias
- [RDS.40] Las instancias de base de datos de RDS para SQL Server deben publicar los registros en Logs CloudWatch
- [RDS.42] Las instancias de base de datos de RDS para MariaDB deben publicar los registros en Logs CloudWatch
- [RDS.45] Los clústeres de bases de datos Aurora MySQL deben tener habilitado el registro de auditoría
- [Redshift.1] Los clústeres de Amazon Redshift deberían prohibir el acceso público
- [Redshift.2] Las conexiones a los clústeres de Amazon Redshift deben cifrarse en tránsito
- [Redshift.3] Los clústeres de Amazon Redshift deben tener habilitadas las instantáneas automáticas
- [Redshift.4] Los clústeres de Amazon Redshift deben tener habilitado el registro de auditoría

- [Redshift.6] Amazon Redshift debería tener habilitadas las actualizaciones automáticas a las versiones principales
- [Redshift.7] Los clústeres de Redshift deberían utilizar un enrutamiento de VPC mejorado
- [Redshift.8] Los clústeres de Amazon Redshift no deben usar el nombre de usuario de administrador predeterminado
- [Redshift.10] Los clústeres de Redshift deben cifrarse en reposo
- [RedshiftServerless.4] Los espacios de nombres de Redshift Serverless deben cifrarse y administrarse por el clienteAWS KMS keys
- [Route53.2] Las zonas alojadas públicas de Route 53 deberían registrar las consultas de DNS
- [S3.1] Los cubos de uso general de S3 deben tener habilitada la configuración de bloqueo del acceso público
- [S3.2] Los cubos de uso general de S3 deberían bloquear el acceso de lectura pública
- [S3.3] Los cubos S3 de uso general deberían bloquear el acceso público a la escritura
- [S3.5] Los cubos de uso general de S3 deberían requerir que las solicitudes usen TLS
- [S3.6] Las políticas de bucket de uso general de S3 deberían restringir el acceso a otros Cuentas de AWS
- [S3.7] Los cubos de uso general de S3 deben utilizar la replicación entre regiones
- [S3.8] Los cubos de uso general de S3 deben bloquear el acceso público
- [S3.9] Los cubos de uso general de S3 deben tener habilitado el registro de acceso al servidor
- [S3.10] Los cubos de uso general de S3 con el control de versiones habilitado deben tener configuraciones de ciclo de vida
- [S3.11] Los cubos de uso general de S3 deben tener habilitadas las notificaciones de eventos
- [S3.12] Las ACL no deben usarse para administrar el acceso de los usuarios a los cubos de uso general de S3
- [S3.13] Los cubos de uso general de S3 deben tener configuraciones de ciclo de vida
- [S3.14] Los cubos de uso general de S3 deben tener habilitado el control de versiones
- [S3.15] Los cubos de uso general de S3 deben tener activado el bloqueo de objetos
- [S3.17] Los cubos de uso general de S3 deben cifrarse en reposo con AWS KMS keys
- [S3.19] Los puntos de acceso S3 deben tener habilitada la configuración de bloqueo de acceso público
- [S3.20] Los cubos de uso general de S3 deben tener habilitada la eliminación de MFA

- [SageMaker.1] Las instancias de Amazon SageMaker Notebook no deberían tener acceso directo a Internet
- [SageMaker.2] las instancias de SageMaker cuadernos deben lanzarse en una VPC personalizada
- [SageMaker.3] Los usuarios no deben tener acceso root a las instancias de los SageMaker cuadernos
- [SageMaker.4] Las variantes de producción de SageMaker terminales deben tener un recuento inicial de instancias superior a 1
- [SageMaker.18] las tiendas en línea de grupos de SageMaker funciones con almacenamiento estándar deben cifrarse con AWS KMS claves
- [SecretsManager.1] Los secretos de Secrets Manager deberían tener habilitada la rotación automática
- [SecretsManager.2] Los secretos de Secrets Manager configurados con rotación automática deberían girar correctamente
- [SecretsManager.3] Eliminar los secretos de Secrets Manager no utilizados
- [SecretsManager.4] Los secretos de Secrets Manager deben rotarse en un número específico de días
- [ServiceCatalog.1] Las carteras de Service Catalog deben compartirse dentro de unAWSsolo una organización
- [SNS.1] Los temas de SNS deben cifrarse en reposo medianteAWS KMS
- [SQS.1] Las colas de Amazon SQS deben cifrarse en reposo
- [SSM.1] Las instancias de Amazon EC2 deben administrarse medianteAWS Systems Manager
- [SSM.2] Las instancias de Amazon EC2 administradas por Systems Manager deben tener el estado de conformidad con los parches de CONFORMIDAD CON LOS PARCHES tras la instalación de un parche
- [SSM.3] Las instancias de Amazon EC2 administradas por Systems Manager deben tener el estado de conformidad de la asociación de COMPLIANT
- [SSM.4] Los documentos SSM no deben ser públicos
- [Transfer.2] Los servidores Transfer Family no deben usar el protocolo FTP para la conexión de puntos finales
- [Transfer.3] Los conectores Transfer Family deben tener habilitado el registro
- [WAF.1]AWS WAFEl registro de ACL web global clásico debe estar habilitado
- [WAF.2]AWS WAFLas reglas regionales clásicas deben tener al menos una condición

- [WAF.3]AWS WAFLos grupos de reglas regionales clásicos deben tener al menos una regla
- [WAF.4]AWS WAFLas ACL web regionales clásicas deben tener al menos una regla o grupo de reglas
- [WAF.6]AWS WAFLas reglas globales clásicas deben tener al menos una condición
- [WAF.7]AWS WAFLos grupos de reglas globales clásicos deben tener al menos una regla
- [WAF.8]AWS WAFLas ACL web globales clásicas deben tener al menos una regla o grupo de reglas
- [WAF.10]AWS WAFLas ACL web deben tener al menos una regla o grupo de reglas
- [WAF.11]AWS WAFEl registro de ACL web debe estar habilitado
- [WAF.12]AWS WAFlas reglas deben tener CloudWatch las métricas habilitadas

Revisión 2 de NIST SP 800-171 en el CSPM de Security Hub

La publicación especial 800-171 del NIST, revisión 2 (NIST SP 800-171 Rev. 2) es un marco de ciberseguridad y cumplimiento desarrollado por el Instituto Nacional de Estándares y Tecnología (NIST), una agencia que forma parte del. U.S Departamento de Comercio. Este marco de cumplimiento proporciona los requisitos de seguridad recomendados para proteger la confidencialidad de la información no clasificada controlada en sistemas y organizaciones que no forman parte del gobierno federal U.S. La información controlada no clasificada (CUI) es información confidencial que no cumple los criterios del Gobierno para clasificarse, pero que igualmente se debe proteger. Se trata de información que se considera confidencial y que el U.S gobierno federal u otras entidades crean o poseen en su nombre U.S.

NIST SP 800-171 Revisión 2 define requisitos de seguridad recomendados para proteger la confidencialidad de la CUI cuando:

- La información se aloja en sistemas u organizaciones que no pertenecen al Gobierno federal;
- La organización no federal no recopila ni mantiene la información en nombre de una agencia federal, ni utiliza u opera un sistema en nombre de dicha agencia; y
- No existen requisitos de protección específicos establecidos por la ley habilitante, la normativa o una política federal aplicable a la categoría de CUI correspondiente, según figura en el Registro de CUI.

Los requisitos se aplican a todos los componentes de sistemas y organizaciones no federales que tratan, almacenan o transmiten CUI, o que proporcionan protección de seguridad para dichos

componentes. Para obtener más información, consulte NIST SP 800-171 Revisión 2 en el Centro de Recursos de Seguridad Informática del NIST.

AWS Security Hub (CSPM) proporciona controles de seguridad que cumplen con un subconjunto de los requisitos de la revisión 2 del SP 800-171 del NIST. Los controles realizan comprobaciones de seguridad automatizadas para determinados recursos. Servicios de AWS Para habilitar y administrar estos controles, puede habilitar el marco NIST SP 800-171 Revisión 2 como un estándar en el CSPM de Security Hub. Tenga en cuenta que los controles no admiten los requisitos de NIST SP 800-171 Revisión 2 que requieren comprobaciones manuales.

Temas

- Configuración del registro de recursos para los controles que se aplican al estándar
- Cómo determinar qué controles se aplican al estándar

Configuración del registro de recursos para los controles que se aplican al estándar

Para optimizar la cobertura y la precisión de los hallazgos, es importante habilitar y configurar el registro de recursos AWS Config antes de habilitar el estándar NIST SP 800-171, revisión 2, en AWS Security Hub CSPM. Al configurar el registro de recursos, asegúrese también de habilitarlo para todos los tipos de AWS recursos que se comprueban mediante los controles que se aplican a la norma. De lo contrario, es posible que el CSPM de Security Hub no pueda evaluar los recursos adecuados ni generar los resultados precisos para los controles aplicables al estándar.

Para obtener información sobre cómo Security Hub CSPM utiliza el registro de recursos en AWS Config, consulte. Activación y configuración AWS Config para Security Hub CSPM Para obtener información sobre cómo configurar el registro de recursos en AWS Config, consulte Trabajar con el grabador de configuración en la Guía para AWS Config desarrolladores.

La siguiente tabla especifica los tipos de recursos que se deben registrar para los controles que se aplican al estándar NIST SP 800-171 Revisión 2 en el CSPM de Security Hub.

Servicio de AWS	Tipos de recurso
AWS Gestor de certificados(ACM)	`AWS::ACM::Certificate`
Amazon API Gateway	`AWS::ApiGateway::Stage`
Amazon CloudFront	`AWS::CloudFront::Distribution`

Servicio de AWS	Tipos de recurso
Amazon CloudWatch	`AWS::CloudWatch::Alarm`
Amazon Elastic Compute Cloud (Amazon EC2)	`AWS::EC2::ClientVpnEndpoint`, `AWS::EC2::NetworkAcl`, `AWS::EC2::SecurityGroup`, `AWS::EC2::VPC`, `AWS::EC2::VPNConnection`
Elastic Load Balancing	`AWS::ElasticLoadBalancing::LoadBalancer`
AWS Identity and Access Management(IAM)	`AWS::IAM::Policy`, `AWS::IAM::User`
AWS Key Management Service (AWS KMS)	`AWS::KMS::Alias`, `AWS::KMS::Key`
AWS Network Firewall	`AWS::NetworkFirewall::FirewallPolicy`, `AWS::NetworkFirewall::RuleGroup`
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::Bucket`
Amazon Simple Notification Service (Amazon SNS)	`AWS::SNS::Topic`
AWS Systems Manager (SSM)	`AWS::SSM::PatchCompliance`
AWS WAF	`AWS::WAFv2::RuleGroup`

Cómo determinar qué controles se aplican al estándar

La siguiente lista especifica los controles que cumplen con los requisitos de la revisión 2 del NIST SP 800-171 y se aplican al estándar NIST SP 800-171, revisión 2, de Security Hub CSPM. AWS Para ver los detalles sobre los requisitos específicos que admite un control, seleccione el control. Luego, consulte el campo Requisitos relacionados en los detalles del control. Este campo especifica cada requisito de NIST que admite el control. Si el campo no especifica un requisito concreto de NIST, el control no admite ese requisito.

- [ACM.1] ACM-issued Los certificados importados y renovados deben renovarse después de un período de tiempo específico
- [APIGateway.2] Las etapas de la API REST de API Gateway deben configurarse para usar certificados SSL para la autenticación de backend
- [CloudFront.7] CloudFront las distribuciones deben usar certificados personalizados SSL/TLS
- [CloudFront.10] CloudFront las distribuciones no deben usar protocolos SSL obsoletos entre ubicaciones de borde y orígenes personalizados
- [CloudTrail.2] CloudTrail debe tener activado el cifrado en reposo
- [CloudTrail.3] Debe estar habilitada al menos una CloudTrail ruta
- [CloudTrail.4] La validación del archivo de CloudTrail registro debe estar habilitada
- [CloudWatch.1] Debe existir un registro, un filtro métrico y una alarma para el uso del usuario «raíz»
- [CloudWatch.2] Asegúrese de que existan un registro, un filtro métrico y una alarma para las llamadas a la API no autorizadas
- [CloudWatch.4] Asegúrese de que haya un registro, un filtro métrico y una alarma para los cambios en las políticas de IAM
- [CloudWatch.5] Asegúrese de que existan un registro, un filtro métrico y una alarma para los cambios CloudTrail de configuración
- [CloudWatch.6] Asegúrese de que existan un registro métrico, un filtro y una alarma para Consola de administración de AWS errores de autenticación
- [CloudWatch.7] Asegúrese de que haya un registro, un filtro métrico y una alarma para deshabilitar o programar la eliminación de las claves administradas por el cliente
- [CloudWatch.8] Asegúrese de que haya un registro, un filtro métrico y una alarma para los cambios en la política de buckets de S3
- [CloudWatch.9] Asegúrese de que existan un registro métrico, un filtro y una alarma para AWS Config cambios de configuración
- [CloudWatch.10] Asegúrese de que haya un registro, un filtro métrico y una alarma para los cambios en los grupos de seguridad
- [CloudWatch.11] Asegúrese de que existan un filtro métrico de registro y una alarma para los cambios en las listas de control de acceso a la red (NACL)
- [CloudWatch.12] Asegúrese de que haya un registro, un filtro métrico y una alarma para detectar los cambios en las pasarelas de red

- [CloudWatch.13] Asegúrese de que haya un registro, un filtro métrico y una alarma para los cambios en la tabla de rutas
- [CloudWatch.14] Asegúrese de que haya un registro, un filtro métrico y una alarma para los cambios en la VPC
- [CloudWatch.15] CloudWatch las alarmas deben tener configuradas acciones específicas
- [EC2.6] El registro de flujo de VPC debe estar habilitado en todas las VPC
- [EC2.10] Amazon EC2 debe configurarse para utilizar los puntos de enlace de VPC que se crean para el servicio Amazon EC2
- [EC2.13] Los grupos de seguridad no deberían permitir la entrada desde la versión 0.0.0. 0/0 o: :/0 al puerto 22
- [EC2.16] Se deben eliminar las listas de control de acceso a la red no utilizadas
- [EC2.18] Los grupos de seguridad solo deben permitir el tráfico entrante sin restricciones en los puertos autorizados
- [EC2.19] Los grupos de seguridad no deben permitir el acceso irrestricto a los puertos de alto riesgo
- [EC2.20] Ambos túneles VPN para un AWS Site-to-Site La conexión VPN debería estar activa
- [EC2.21] Las ACL de red no deberían permitir la entrada desde la versión 0.0.0. 0/0 al puerto 22 o al puerto 3389
- [EC2.51] Los puntos finales EC2 Client VPN deben tener habilitado el registro de conexiones de clientes
- [EFS.6] Los destinos de montaje de EFS no deben asociarse a subredes que asignan direcciones IP públicas en el momento del lanzamiento
- [ELB.2] Los balanceadores de carga clásicos con SSL/HTTPS oyentes deben usar un certificado proporcionado por AWS Gestor de certificados
- [ELB.3] Los oyentes de Classic Load Balancer deben configurarse con terminación HTTPS o TLS
- [ELB.8] Los balanceadores de carga clásicos con receptores SSL deben usar una política de seguridad predefinida que sea sólida AWS Config Duración
- [GuardDuty.1] GuardDuty debería estar activado
- [IAM.1] Las políticas de IAM no deberían permitir todos los privilegios administrativos «*»
- [IAM.2] Los usuarios de IAM no deberían tener políticas de IAM adjuntas
- [IAM.7] Las políticas de contraseñas para los usuarios de IAM deben tener configuraciones sólidas
- [IAM.8] Se deben eliminar las credenciales de usuario de IAM no utilizadas

- [IAM.10] Las políticas de contraseñas para los usuarios de IAM deben tener configuraciones sólidas
- [IAM.11] Asegúrese de que la política de contraseñas de IAM requiera al menos una letra mayúscula
- [IAM.12] Asegúrese de que la política de contraseñas de IAM requiera al menos una letra minúscula
- [IAM.13] Asegúrese de que la política de contraseñas de IAM requiera al menos un símbolo
- [IAM.14] Asegúrese de que la política de contraseñas de IAM requiera al menos un número
- [IAM.15] Asegúrese de que la política de contraseñas de IAM exija una longitud de contraseña mínima de 14 o más
- [IAM.16] Asegúrese de que la política de contraseñas de IAM impida la reutilización de contraseñas
- [IAM.18] Asegúrese de que se haya creado una función de soporte para gestionar los incidentes conAWS Support
- [IAM.19] La MFA debe estar habilitada para todos los usuarios de IAM
- [IAM.21] Las políticas de IAM gestionadas por el cliente que cree no deberían permitir acciones comodín en los servicios
- [IAM.22] Se deben eliminar las credenciales de usuario de IAM que no se hayan utilizado durante 45 días
- [NetworkFirewall.2] El registro de Network Firewall debe estar habilitado
- [NetworkFirewall.3] Las políticas de Network Firewall deben tener asociado al menos un grupo de reglas
- [NetworkFirewall.5] La acción sin estado predeterminada para las políticas de Network Firewall debe ser eliminar o reenviar paquetes fragmentados
- [NetworkFirewall.6] El grupo de reglas de Stateless Network Firewall no debe estar vacío
- [S3.5] Los cubos de uso general de S3 deberían requerir que las solicitudes usen TLS
- [S3.6] Las políticas de bucket de uso general de S3 deberían restringir el acceso a otros Cuentas de AWS
- [S3.9] Los cubos de uso general de S3 deben tener habilitado el registro de acceso al servidor
- [S3.11] Los cubos de uso general de S3 deben tener habilitadas las notificaciones de eventos
- [S3.14] Los cubos de uso general de S3 deben tener habilitado el control de versiones
- [S3.17] Los cubos de uso general de S3 deben cifrarse en reposo con AWS KMS keys

- [SNS.1] Los temas de SNS deben cifrarse en reposo medianteAWS KMS
- [SSM.2] Las instancias de Amazon EC2 administradas por Systems Manager deben tener el estado de conformidad con los parches de CONFORMIDAD CON LOS PARCHES tras la instalación de un parche
- [WAF.12]AWS WAFlas reglas deben tener CloudWatch las métricas habilitadas

PCI DSS en el CSPM de Security Hub

El Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS) es un marco de cumplimiento de terceros que proporciona un conjunto de reglas y directrices para manejar de forma segura la información de tarjetas de crédito y débito. El Consejo de Normas de Seguridad PCI (PCI SSC) crea y actualiza este marco.

AWS El CSPM de Security Hub proporciona un estándar PCI DSS que puede ayudarlo a cumplir con este marco de terceros. Puede utilizar este estándar para descubrir vulnerabilidades de seguridad en los recursos de AWS que gestionan los datos de los titulares de tarjetas. Recomendamos habilitar este estándar en Cuentas de AWS con recursos que almacenan, tratan o transmiten datos de titulares de tarjetas o información confidencial de autenticación. Las evaluaciones realizadas por el PCI SSC validaron este estándar.

El CSPM de Security Hub ofrece compatibilidad con PCI DSS v3.2.1 y PCI DSS v4.0.1. Recomendamos usar la versión v4.0.1 para mantenerse alineado con las prácticas recomendadas de seguridad más recientes. Puede tener ambas versiones del estándar habilitadas al mismo tiempo. Para obtener información sobre cómo habilitar estándares, consulte Habilitación de un estándar de seguridad. Si actualmente usa la versión v3.2.1 pero desea usar únicamente la v4.0.1, habilite primero la versión más reciente antes de desactivar la versión anterior. Esto evita deficiencias en las comprobaciones de seguridad. Si utiliza la integración de Security Hub con CSPM AWS Organizations y quiere habilitarla por lotes en varias cuentas, le recomendamos que utilice una configuración central para hacerlo. ???

Las siguientes secciones especifican qué controles se aplican a PCI DSS v3.2.1 y a PCI DSS v4.0.1.

Controles que se aplican a PCI DSS v3.2.1

La siguiente lista especifica qué controles del CSPM de Security Hub se aplican a PCI DSS v3.2.1. Para revisar los detalles de un control, seleccione el control.

[AutoScaling.1] Los grupos de Auto Scaling asociados a un balanceador de cargas deben usar comprobaciones de estado del ELB

[CloudTrail.2] CloudTrail debe tener activado el cifrado en reposo

[CloudTrail.3] Debe estar habilitada al menos una CloudTrail ruta

[CloudTrail.4] La validación del archivo de CloudTrail registro debe estar habilitada

[CloudTrail.5] los CloudTrail senderos deben estar integrados con Amazon CloudWatch Logs

[CloudWatch.1] Debe existir un registro, un filtro métrico y una alarma para el uso del usuario «raíz»

[CodeBuild.1] Las URL del repositorio fuente de CodeBuild Bitbucket no deben contener credenciales confidenciales

[CodeBuild.2] las variables de entorno CodeBuild del proyecto no deben contener credenciales de texto claro

[Config.1] AWS Config deben estar habilitados y usar la función vinculada al servicio para el registro de recursos

[DMS.1] Las instancias de replicación de Database Migration Service no deben ser públicas

[EC2.1] Las instantáneas de Amazon EBS no deben configurarse para que se puedan restaurar públicamente

[EC2.2] Los grupos de seguridad predeterminados de VPC no deben permitir el tráfico entrante o saliente

[EC2.6] El registro de flujo de VPC debe estar habilitado en todas las VPC

[EC2.12] Deben eliminarse las EIP de Amazon EC2 no utilizadas

[EC2.13] Los grupos de seguridad no deberían permitir la entrada desde la versión 0.0.0. 0/0 o: :/0 al puerto 22

[ELB.1] El balanceador de carga de aplicaciones debe configurarse para redirigir todas las solicitudes HTTP a HTTPS

[ES.1] Los dominios de Elasticsearch deben tener habilitado el cifrado en reposo

[ES.2] Los dominios de Elasticsearch no deben ser de acceso público

[GuardDuty.1] GuardDuty debería estar activado

[IAM.1] Las políticas de IAM no deberían permitir todos los privilegios administrativos «*»

[IAM.2] Los usuarios de IAM no deberían tener políticas de IAM adjuntas

[IAM.4] La clave de acceso del usuario raíz de IAM no debería existir

[IAM.6] La MFA de hardware debe estar habilitada para el usuario root

[IAM.8] Se deben eliminar las credenciales de usuario de IAM no utilizadas

[IAM.9] La MFA debe estar habilitada para el usuario root

[IAM.10] Las políticas de contraseñas para los usuarios de IAM deben tener configuraciones sólidas

[IAM.19] La MFA debe estar habilitada para todos los usuarios de IAM

[KMS.4]AWS KMSla rotación de claves debe estar habilitada

[Lambda.1] Las políticas de las funciones de Lambda deberían prohibir el acceso público

[Lambda.3] Las funciones de Lambda deben estar en una VPC

[Opensearch.1] OpenSearch los dominios deben tener activado el cifrado en reposo

[Opensearch.2] OpenSearch los dominios no deben ser de acceso público

[RDS.1] La instantánea de RDS debe ser privada

[RDS.2] Las instancias de base de datos de RDS deben prohibir el acceso público, según lo determine la configuración PubliclyAccessible

[Redshift.1] Los clústeres de Amazon Redshift deberían prohibir el acceso público

[S3.1] Los cubos de uso general de S3 deben tener habilitada la configuración de bloqueo del acceso público

[S3.2] Los cubos de uso general de S3 deberían bloquear el acceso de lectura pública

[S3.3] Los cubos S3 de uso general deberían bloquear el acceso público a la escritura

[S3.5] Los cubos de uso general de S3 deberían requerir que las solicitudes usen TLS

[S3.7] Los cubos de uso general de S3 deben utilizar la replicación entre regiones

[SageMaker.1] Las instancias de Amazon SageMaker Notebook no deberían tener acceso directo a Internet

[SSM.1] Las instancias de Amazon EC2 deben administrarse medianteAWS Systems Manager

[SSM.2] Las instancias de Amazon EC2 administradas por Systems Manager deben tener el estado de conformidad con los parches de CONFORMIDAD CON LOS PARCHES tras la instalación de un parche

[SSM.3] Las instancias de Amazon EC2 administradas por Systems Manager deben tener el estado de conformidad de la asociación de COMPLIANT

Controles que se aplican a PCI DSS v4.0.1

La siguiente lista especifica qué controles del CSPM de Security Hub se aplican a PCI DSS v4.0.1. Para revisar los detalles de un control, seleccione el control.

[ACM.1] ACM-issued Los certificados importados y renovados deben renovarse después de un período de tiempo específico

[ACM.2] Los certificados RSA gestionados por ACM deben utilizar una longitud de clave de al menos 2048 bits

[APIGateway.9] El registro de acceso debe configurarse para las etapas V2 de API Gateway

[AppSync.2]AWS AppSyncdebe tener habilitado el registro a nivel de campo

[AutoScaling.3] Las configuraciones de lanzamiento grupal de Auto Scaling deberían configurar las instancias EC2 para que requieran la versión 2 del Servicio de Metadatos de Instancia (IMDSv2)

[Autoscaling.5] Las instancias de Amazon EC2 lanzadas mediante configuraciones de lanzamiento grupal de Auto Scaling no deben tener direcciones IP públicas

[CloudFront.1] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado

[CloudFront.10] CloudFront las distribuciones no deben usar protocolos SSL obsoletos entre ubicaciones de borde y orígenes personalizados

[CloudFront.12] CloudFront las distribuciones no deben apuntar a orígenes de S3 inexistentes

[CloudFront.3] CloudFront las distribuciones deben requerir el cifrado durante el tránsito

[CloudFront.5] CloudFront las distribuciones deben tener habilitado el registro

[CloudFront.6] CloudFront las distribuciones deben tener WAF activado

[CloudFront.9] CloudFront las distribuciones deben cifrar el tráfico para convertirlo en orígenes personalizados

[CloudTrail.2] CloudTrail debe tener activado el cifrado en reposo

[CloudTrail.3] Debe estar habilitada al menos una CloudTrail ruta

[CloudTrail.4] La validación del archivo de CloudTrail registro debe estar habilitada

[CloudTrail.6] Asegúrese de que el depósito de S3 que se utiliza para almacenar CloudTrail los registros no sea de acceso público

[CloudTrail.7] Asegúrese de que el registro de acceso al bucket de S3 esté habilitado en el CloudTrail bucket de S3

[CodeBuild.1] Las URL del repositorio fuente de CodeBuild Bitbucket no deben contener credenciales confidenciales

[CodeBuild.2] las variables de entorno CodeBuild del proyecto no deben contener credenciales de texto claro

[CodeBuild.3] Los registros de CodeBuild S3 deben estar cifrados

[DMS.1] Las instancias de replicación de Database Migration Service no deben ser públicas

[DMS.10] Los puntos finales de DMS para las bases de datos de Neptune deben tener habilitada la autorización de IAM

[DMS.11] Los puntos finales de DMS para MongoDB deben tener un mecanismo de autenticación habilitado

[DMS.12] Los puntos finales de DMS para Redis OSS deben tener el TLS habilitado

[DMS.6] Las instancias de replicación de DMS deben tener habilitada la actualización automática de las versiones secundarias

[DMS.7] Las tareas de replicación del DMS para la base de datos de destino deben tener el registro habilitado

[DMS.8] Las tareas de replicación del DMS para la base de datos de origen deben tener el registro activado

[DMS.9] Los puntos finales del DMS deben usar SSL

[DocumentDB.2] Los clústeres de Amazon DocumentDB deben tener un período de retención de copias de seguridad adecuado

[DocumentDB.3] Las instantáneas de clústeres manuales de Amazon DocumentDB no deben ser públicas

[DocumentDB.4] Los clústeres de Amazon DocumentDB deben publicar los registros de auditoría en Logs CloudWatch

[DynamoDB.7] Los clústeres de DynamoDB Accelerator deben cifrarse en tránsito

[EC2.13] Los grupos de seguridad no deberían permitir la entrada desde la versión 0.0.0. 0/0 o: :/0 al puerto 22

[EC2.14] Los grupos de seguridad no deberían permitir la entrada desde la versión 0.0.0. 0/0 o: :/0 al puerto 3389

[EC2.15] Las subredes de Amazon EC2 no deben asignar automáticamente direcciones IP públicas

[EC2.16] Se deben eliminar las listas de control de acceso a la red no utilizadas

[EC2.170] Las plantillas de lanzamiento de EC2 deben utilizar la versión 2 del servicio de metadatos de instancias (IMDSv2)

[EC2.171] Las conexiones VPN de EC2 deberían tener el registro habilitado

[EC2.21] Las ACL de red no deberían permitir la entrada desde la versión 0.0.0. 0/0 al puerto 22 o al puerto 3389

[EC2.25] Las plantillas de lanzamiento de Amazon EC2 no deben asignar direcciones IP públicas a las interfaces de red

[EC2.51] Los puntos finales EC2 Client VPN deben tener habilitado el registro de conexiones de clientes

[EC2.53] Los grupos de seguridad de EC2 no deberían permitir la entrada desde la versión 0.0.0. 0/0 a los puertos de administración remota del servidor

[EC2.54] Los grupos de seguridad de EC2 no deberían permitir la entrada desde: :/0 a los puertos de administración remota del servidor

[EC2.8] Las instancias EC2 deben utilizar la versión 2 del servicio de metadatos de instancia (IMDSv2)

[ECR.1] Los repositorios privados de ECR deben tener configurado el escaneo de imágenes

[ECS.10] Los servicios Fargate de ECS deberían ejecutarse en la última versión de la plataforma Fargate

[ECS.16] Los conjuntos de tareas de ECS no deben asignar automáticamente direcciones IP públicas

[ECS.2] Los servicios de ECS no deberían tener direcciones IP públicas asignadas automáticamente

[ECS.8] Los secretos no deben transmitirse como variables de entorno de contenedores

[EFS.4] Los puntos de acceso EFS deben exigir la identidad del usuario

[EKS.1] Los puntos finales del clúster EKS no deben ser de acceso público

[EKS.2] Los clústeres de EKS deben ejecutarse en una versión de Kubernetes compatible

[EKS.3] Los clústeres de EKS deben usar secretos de Kubernetes cifrados

[EKS.8] Los clústeres de EKS deben tener habilitado el registro de auditoría

[ElastiCache.2] ElastiCache los clústeres deberían tener habilitadas las actualizaciones automáticas de las versiones secundarias

[ElastiCache.5] los grupos de ElastiCache replicación deben cifrarse en tránsito

[ElastiCache.6] ElastiCache (Redis OSS) Los grupos de replicación de versiones anteriores deberían tener habilitada la autenticación de Redis OSS

[ElasticBeanstalk.2] Las actualizaciones de la plataforma gestionada de Elastic Beanstalk deben estar habilitadas

[ElasticBeanstalk.3] Elastic Beanstalk debería transmitir los registros a CloudWatch

[ELB.12] El balanceador de carga de aplicaciones debe configurarse con el modo defensivo o de mitigación de desincronización más estricto

[ELB.14] El balanceador de carga clásico debe configurarse con el modo defensivo o de mitigación de desincronización más estricto

[ELB.3] Los oyentes de Classic Load Balancer deben configurarse con terminación HTTPS o TLS

[ELB.4] El balanceador de carga de aplicaciones debe configurarse para eliminar los encabezados http no válidos

[ELB.8] Los balanceadores de carga clásicos con receptores SSL deben usar una política de seguridad predefinida que sea sólida AWS Config Duración

[EMR.1] Los nodos principales del clúster de Amazon EMR no deben tener direcciones IP públicas

[EMR.2] La configuración de acceso público del bloque Amazon EMR debe estar habilitada

[ES.2] Los dominios de Elasticsearch no deben ser de acceso público

[ES.3] Los dominios de Elasticsearch deben cifrar los datos enviados entre nodos

[ES.5] Los dominios de Elasticsearch deben tener habilitado el registro de auditoría

[ES.8] Las conexiones a los dominios de Elasticsearch deben cifrarse con la política de seguridad TLS más reciente

[EventBridge.3] los autobuses de eventos EventBridge personalizados deben tener adjunta una política basada en los recursos

[GuardDuty.1] GuardDuty debería estar activado

[GuardDuty.10] La protección GuardDuty S3 debe estar habilitada

[GuardDuty.6] GuardDuty La protección Lambda debe estar habilitada

[GuardDuty.7] La monitorización del tiempo de ejecución de GuardDuty EKS debe estar habilitada

[GuardDuty.9] La protección GuardDuty RDS debe estar habilitada

[IAM.3] Las claves de acceso de los usuarios de IAM deben rotarse cada 90 días o menos

[IAM.5] La MFA debe estar habilitada para todos los usuarios de IAM que tengan una contraseña de consola

[IAM.6] La MFA de hardware debe estar habilitada para el usuario root

[IAM.7] Las políticas de contraseñas para los usuarios de IAM deben tener configuraciones sólidas

[IAM.8] Se deben eliminar las credenciales de usuario de IAM no utilizadas

[IAM.9] La MFA debe estar habilitada para el usuario root

[IAM.11] Asegúrese de que la política de contraseñas de IAM requiera al menos una letra mayúscula

[IAM.12] Asegúrese de que la política de contraseñas de IAM requiera al menos una letra minúscula

[IAM.14] Asegúrese de que la política de contraseñas de IAM requiera al menos un número

[IAM.16] Asegúrese de que la política de contraseñas de IAM impida la reutilización de contraseñas

[IAM.17] Asegúrese de que la política de contraseñas de IAM haga caducar las contraseñas en un plazo de 90 días o menos

[IAM.18] Asegúrese de que se haya creado una función de soporte para gestionar los incidentes conAWS Support

[IAM.19] La MFA debe estar habilitada para todos los usuarios de IAM

[Inspector.1] El escaneo EC2 de Amazon Inspector debe estar activado

[Inspector.2] El escaneo ECR de Amazon Inspector debe estar activado

[Inspector.3] El escaneo de código Lambda de Amazon Inspector Lambda debe estar activado

[Inspector.4] El escaneo estándar de Amazon Inspector Lambda debe estar activado

[KMS.4]AWS KMSla rotación de claves debe estar habilitada

[Lambda.1] Las políticas de las funciones de Lambda deberían prohibir el acceso público

[Lambda.2] Las funciones de Lambda deben usar los tiempos de ejecución compatibles

[MQ.2] Los corredores de ActiveMQ deben transmitir los registros de auditoría a CloudWatch

[MSK.1] Los clústeres de MSK deben cifrarse en tránsito entre los nodos de intermediación

[MSK.3] Los conectores MSK Connect deben estar cifrados en tránsito

[Neptune.2] Los clústeres de bases de datos de Neptune deberían publicar registros de auditoría en Logs CloudWatch

[Neptune.3] Las instantáneas del clúster de base de datos de Neptune no deben ser públicas

[Opensearch.10] OpenSearch los dominios deben tener instalada la última actualización de software

[Opensearch.5] OpenSearch los dominios deben tener activado el registro de auditoría

[RDS.13] Las actualizaciones automáticas de las versiones secundarias de RDS deben estar habilitadas

[RDS.2] Las instancias de base de datos de RDS deben prohibir el acceso público, según lo determine la configuración PubliclyAccessible

[RDS.20] Las suscripciones de notificación de eventos de RDS existentes deben configurarse para los eventos críticos de las instancias de bases de datos

[RDS.21] Se debe configurar una suscripción a las notificaciones de eventos de RDS para los eventos de grupos de parámetros de base de datos críticos

[RDS.22] Se debe configurar una suscripción a las notificaciones de eventos de RDS para los eventos críticos de grupos de seguridad de bases de datos

[RDS.24] Los clústeres de bases de datos de RDS deben usar un nombre de usuario de administrador personalizado

[RDS.25] Las instancias de bases de datos de RDS deben usar un nombre de usuario de administrador personalizado

[RDS.34] Los clústeres de bases de datos Aurora MySQL deben publicar los registros de auditoría en Logs CloudWatch

[RDS.35] Los clústeres de bases de datos de RDS deben tener habilitada la actualización automática de versiones secundarias

[RDS.36] Las instancias de base de datos de RDS para PostgreSQL deben publicar los registros en Logs CloudWatch

[RDS.37] Los clústeres de bases de datos de Aurora PostgreSQL deben publicar los registros en Logs CloudWatch

[RDS.9] Las instancias de base de datos de RDS deben publicar los registros en Logs CloudWatch

[Redshift.1] Los clústeres de Amazon Redshift deberían prohibir el acceso público

[Redshift.15] Los grupos de seguridad de Redshift deberían permitir la entrada en el puerto del clúster solo desde orígenes restringidos

[Redshift.2] Las conexiones a los clústeres de Amazon Redshift deben cifrarse en tránsito

[Redshift.4] Los clústeres de Amazon Redshift deben tener habilitado el registro de auditoría

[Route53.2] Las zonas alojadas públicas de Route 53 deberían registrar las consultas de DNS

[S3.1] Los cubos de uso general de S3 deben tener habilitada la configuración de bloqueo del acceso público

[S3.15] Los cubos de uso general de S3 deben tener activado el bloqueo de objetos

[S3.17] Los cubos de uso general de S3 deben cifrarse en reposo con AWS KMS keys

[S3.19] Los puntos de acceso S3 deben tener habilitada la configuración de bloqueo de acceso público

[S3.22] Los cubos de uso general de S3 deben registrar los eventos de escritura a nivel de objeto

[S3.23] Los cubos de uso general de S3 deben registrar los eventos de lectura a nivel de objeto

[S3.24] Los puntos de Multi-Region acceso S3 deben tener habilitada la configuración de bloqueo del acceso público

[S3.5] Los cubos de uso general de S3 deberían requerir que las solicitudes usen TLS

[S3.8] Los cubos de uso general de S3 deben bloquear el acceso público

[S3.9] Los cubos de uso general de S3 deben tener habilitado el registro de acceso al servidor

[SageMaker.1] Las instancias de Amazon SageMaker Notebook no deberían tener acceso directo a Internet

[SecretsManager.1] Los secretos de Secrets Manager deberían tener habilitada la rotación automática

[SecretsManager.2] Los secretos de Secrets Manager configurados con rotación automática deberían girar correctamente

[SecretsManager.4] Los secretos de Secrets Manager deben rotarse en un número específico de días

[SSM.2] Las instancias de Amazon EC2 administradas por Systems Manager deben tener el estado de conformidad con los parches de CONFORMIDAD CON LOS PARCHES tras la instalación de un parche

[SSM.3] Las instancias de Amazon EC2 administradas por Systems Manager deben tener el estado de conformidad de la asociación de COMPLIANT

[StepFunctions.1] Step Functions indica que las máquinas deben tener el registro activado

[Transfer.2] Los servidores Transfer Family no deben usar el protocolo FTP para la conexión de puntos finales

[WAF.1]AWS WAFEl registro de ACL web global clásico debe estar habilitado

[WAF.11]AWS WAFEl registro de ACL web debe estar habilitado

Service-managed estándares en Security Hub CSPM

Un estándar administrado por servicios es un estándar de seguridad que Servicio de AWS administra otro, pero que puede ver en Security Hub CSPM. Por ejemplo, Service-Managed Standard: AWS Control Tower es un estándar administrado por servicios que administra. AWS Control Tower Un estándar administrado por el servicio se diferencia de un estándar de seguridad que el CSPM de AWS Security Hub administra de las siguientes maneras:

- Creación y eliminación de estándares: puede crear y eliminar un estándar de administración de servicios con la consola o la API del servicio de administración, o con AWS CLI. Hasta que cree el estándar en el servicio que lo administra mediante alguno de esos métodos, el estándar no aparece en la consola del CSPM de Security Hub y no está disponible a través de la API del CSPM de Security Hub ni de la AWS CLI.
- No hay habilitación automática de controles: cuando crea un estándar administrado por el servicio, ni el CSPM de Security Hub ni el servicio que lo administra habilitan automáticamente los controles que corresponden al estándar. Además, cuando el CSPM de Security Hub lanza controles nuevos para el estándar, estos controles tampoco se habilitan de manera automática. Esto se aparta del funcionamiento habitual de los estándares que administra directamente el CSPM de Security Hub. Para obtener más información sobre la forma habitual de configurar controles en el CSPM de Security Hub, consulte Comprensión de los controles de seguridad en el CSPM de Security Hub.
- Habilitar y deshabilitar los controles: se recomienda habilitar y deshabilitar los controles en el servicio de administración para evitar desviaciones.
- Disponibilidad de los controles: el servicio de administración elige qué controles están disponibles como parte del estándar de administración del servicio. Los controles disponibles pueden incluir todos o solo un subconjunto de los controles existentes del CSPM de Security Hub.

Después de que el servicio administrador crea el estándar administrado por el servicio y pone a disposición los controles que lo conforman, puede acceder a sus resultados, estados de control y puntaje de seguridad desde la consola del CSPM de Security Hub, la API del CSPM de Security Hub

o la AWS CLI. Es posible que parte o toda esta información también esté disponible en el servicio de administración.

Seleccione un estándar gestionado por el servicio de la siguiente lista para ver más detalles al respecto.

Service-managed estándares

- Service-Managed Estándar: AWS Control Tower

Service-Managed Estándar: AWS Control Tower

Esta sección proporciona información sobre Service-Managed Standard:. AWS Control Tower

Qué es Service-Managed Standard: AWS Control Tower?

Service-Managed Estándar: AWS Control Tower es un estándar administrado por servicios que AWS Control Tower administra y admite un subconjunto de controles de Security Hub. Este estándar está diseñado para los usuarios de AWS Security Hub CSPM y. AWS Control Tower Le permite configurar los controles de detección de Security Hub CSPM desde el servicio. AWS Control Tower

Los controles de Detective detectan el incumplimiento de los recursos (por ejemplo, errores de configuración) dentro de su Cuentas de AWS.

> **Tip**
>
> Service-managed los estándares difieren de los estándares que administra AWS Security Hub CSPM. Por ejemplo, debe crear y eliminar un estándar administrado por un servicio en el servicio de administración. Para obtener más información, consulte Service-managed estándares en Security Hub CSPM.

Cuando habilita un control de CSPM de Security Hub AWS Control Tower, Control Tower también habilita el CSPM de Security Hub para usted en esas cuentas y regiones específicas, si aún no está habilitado. En la consola y la API del CSPM de Security Hub, puede ver el Service-Managed estándar: AWS Control Tower junto con otros estándares del CSPM de Security Hub, una vez que el estándar esté habilitado desde. AWS Control Tower

Para obtener más información sobre este estándar, consulte Controles del CSPM de Security Hub en la Guía del usuario de AWS Control Tower .

Creación del estándar

Este estándar solo está disponible en el CSPM de Security Hub si habilita los controles del CSPM de Security Hub desde. AWS Control Tower AWS Control Tower crea el estándar cuando se habilita por primera vez un control aplicable mediante uno de los métodos siguientes:

- AWS Control Tower consola
- AWS Control Tower API (llame a la `EnableControl` API)
- AWS CLI (ejecuta el `enable-control` comando)

Cuando habilita un control de CSPM de Security Hub AWS Control Tower, si aún no ha habilitado el CSPM de Security Hub, AWS Control Tower también habilita el CSPM de Security Hub para usted en esas cuentas y regiones específicas.

Para identificar un control CSPM de Security Hub por su identificador de control en el Catálogo de controles, puede utilizar el campo de. `Implementation.Identifier` AWS Control Tower Este campo se asigna al ID de control CSPM de Security Hub y se puede usar para filtrar por un ID de control específico. Para recuperar los metadatos de un control CSPM de Security Hub específico (por ejemplo, "CodeBuild.1«) en AWS Control Tower, puede usar la API: `ListControls`

```
aws controlcatalog list-controls --filter '{"Implementations":
{"Identifiers":["CodeBuild.1"],"Types":
["AWS::SecurityHub::SecurityControl"]}}'
```

No puede ver ni acceder a este estándar en la consola CSPM de Security Hub ni en la API de CSPM de Security Hub ni AWS CLI sin antes configurar AWS Control Tower y habilitar los controles de CSPM de Security Hub mediante uno de los métodos anteriores. AWS Control Tower

Este estándar solo está disponible donde está disponible. Regiones de AWSAWS Control Tower

Habilitación y deshabilitación de de los controles en el estándar

Una vez que haya habilitado los controles CSPM de Security Hub AWS Control Tower y haya creado el Service-Managed AWS Control Tower estándar: estándar, podrá ver el estándar y los controles disponibles en Security Hub CSPM.

Cuando el CSPM de Security Hub agrega nuevos controles al Service-Managed estándar: AWS Control Tower estándar, no se habilitan automáticamente para los clientes que tienen el estándar

habilitado. Debe habilitar y deshabilitar los controles del estándar AWS Control Tower mediante uno de los siguientes métodos:

- AWS Control Tower consola
- AWS Control Tower API (llame a las `DisableControl` API `EnableControl` y)
- AWS CLI (ejecuta los `disable-control` comandos `enable-control` y)

Al cambiar el estado de activación de un control en AWS Control Tower, el cambio también se refleja en Security Hub CSPM.

Sin embargo, si se deshabilita un control en Security Hub CSPM que está habilitado, se produce un cambio de control. AWS Control Tower El estado del control en AWS Control Tower se muestra como. `Drifted` Puede resolver este desfase utilizando la ResetEnabledControl API para restablecer el control que está en suspenso, seleccionando la Re-register unidad organizativa en la AWS Control Tower consola o deshabilitando y volviendo a habilitar el control AWS Control Tower mediante uno de los métodos anteriores.

Completar las acciones de activación y desactivación te ayuda a evitar que el control se desvíe. AWS Control Tower

Al activar o desactivar los controles AWS Control Tower, la acción se aplica a todas las cuentas y regiones que rigen. AWS Control Tower Si habilitas y deshabilitas los controles en el CSPM de Security Hub (no se recomienda para este estándar), la acción solo se aplica a la cuenta y la región actuales.

> **Note**
>
> La configuración central no se puede usar para administrar Service-Managed Standard:. AWS Control TowerSolo puede usar el AWS Control Tower servicio para habilitar y deshabilitar los controles de este estándar.

Visualización del estado de activación y el estado de control

Puede ver el estado de habilitación de un control mediante uno de los métodos siguientes:

- La consola CSPM de Security Hub, la API CSPM de Security Hub o AWS CLI
- AWS Control Tower consola

- AWS Control Tower API para ver una lista de los controles habilitados (llama a la `ListEnabledControls` API)
- AWS CLI para ver una lista de los controles habilitados (ejecuta el `list-enabled-controls` comando)

Un control en el que esté AWS Control Tower deshabilitado tendrá un estado de activación de `Disabled` en Security Hub CSPM, a menos que habilite explícitamente ese control en Security Hub CSPM.

El CSPM de Security Hub calcula el estado del control según el estado del flujo de trabajo y el estado de cumplimiento de los resultados del control. Para obtener más información sobre el estado de activación y el estado de control, consulte Cómo revisar los detalles de los controles en el CSPM de Security Hub.

Según los estados de control, el CSPM de Security Hub calcula una puntuación de seguridad para Standard:. ??? Service-Managed AWS Control Tower Este puntaje solo está disponible en el CSPM de Security Hub. Además, solo puede ver los resultados de control en el CSPM de Security Hub. La puntuación de seguridad estándar y las conclusiones de control no están disponibles en. AWS Control Tower

> **Note**
>
> Al habilitar los controles en Service-Managed Standard: AWS Control Tower, Security Hub CSPM puede tardar hasta 18 horas en generar los resultados de los controles que utilizan una regla vinculada a un AWS Config servicio existente. Si ha habilitado otros estándares y controles en el CSPM de Security Hub, es posible que ya cuente con reglas vinculadas al servicio. Para obtener más información, consulte Programación para ejecutar comprobaciones de seguridad.

Eliminación de la norma

Puede eliminar este estándar gestionado por servicios en AWS Control Tower deshabilitando todos los controles aplicables mediante uno de los siguientes métodos:

- AWS Control Tower consola
- AWS Control Tower API (llame a la `DisableControl` API)
- AWS CLI (ejecuta el `disable-control` comando)

Al deshabilitar todos los controles, se elimina el estándar en todas las cuentas administradas y regiones gobernadas de AWS Control Tower. Al eliminar el estándar en, se AWS Control Tower elimina de la página de estándares de la consola CSPM de Security Hub y ya no podrá acceder a él mediante la API CSPM de Security Hub o. AWS CLI

> **Note**
>
> La desactivación de todos los controles del estándar en el CSPM de Security Hub no desactiva ni elimina el estándar.

Al deshabilitar el servicio CSPM de Security Hub, se elimina Service-Managed Standard AWS Control Tower y cualquier otro estándar que haya habilitado.

Buscando el formato de campo para Standard: Service-Managed AWS Control Tower

Cuando crees Service-Managed Standard: AWS Control Tower y habilites sus controles, empezarás a recibir los resultados de los controles en Security Hub CSPM. El CSPM de Security Hub informa de los resultados de control en el AWS Formato de búsqueda de seguridad (ASFF). Estos son los valores ASFF del nombre de recurso de Amazon (ARN) de este estándar y `GeneratorId`:

- ARN estándar — `arn:aws:us-east-1:securityhub:::standards/service-managed-aws-control-tower/v/1.0.0`
- GeneratorId – `service-managed-aws-control-tower/v/1.0.0/CodeBuild.1`

Para ver un ejemplo de los resultados de Service-Managed Standard: consulte AWS Control Tower. Ejemplos de resultados de controles

Controles que se aplican a Service-Managed Standard: AWS Control Tower

Service-Managed Estándar: AWS Control Tower admite un subconjunto de controles que forman parte del estándar AWS Fundational Security Best Practices (FSBP). Elija un control para ver información al respecto, incluidos los pasos para remediar los resultados fallidos.

Para ver qué controles de CSPM de Security Hub son compatibles AWS Control Tower, puede usar uno de los métodos siguientes:

- AWS Consola de Control Catalog, donde puede filtrar por “`Control owner = AWS Security Hub`”

- AWS La API de Control Catalog (llamada `ListControls` API) con un filtro `Implementations` para comprobar si `Types` es `AWS::SecurityHub::SecurityControl`
- AWS CLI (ejecuta el `list-controls` comando) con un filtro para`Implementations`. Ejemplo de comando de la CLI:

```
aws controlcatalog list-controls --filter '{"Implementations":{"Types":
["AWS::SecurityHub::SecurityControl"]}}'
```

Los límites regionales de los controles CSPM de Security Hub, cuando están habilitados mediante el estándar de la Torre de Control, pueden no coincidir con los límites regionales de los controles subyacentes.

En el CSPM de Security Hub, si las comprobaciones de control consolidadas están desactivadas en su cuenta, el `ProductFields.ControlId` campo de las conclusiones generadas utiliza el identificador de control basado en el estándar. El ID de control estándar tiene el formato CT. ***ControlId***(por ejemplo,). CT.CodeBuild.1

Para obtener más información sobre este estándar, consulte Controles del CSPM de Security Hub en la Guía del usuario de AWS Control Tower .

Habilitación de un estándar de seguridad

Al habilitar un estándar de seguridad en AWS Security Hub CSPM, Security Hub CSPM crea y habilita automáticamente todos los controles que se aplican al estándar. El CSPM de Security Hub también inicia las comprobaciones de seguridad y empieza a generar resultados para esos controles.

Para optimizar la cobertura y la precisión de los hallazgos, habilite y configure el registro de recursos AWS Config antes de habilitar un estándar. Cuando configure el registro de recursos, asegúrese también de habilitarlo para todos los tipos de recursos que los controles del estándar verifican. De lo contrario, es posible que el CSPM de Security Hub no pueda evaluar los recursos adecuados ni generar los resultados precisos para los controles aplicables al estándar. Para obtener más información, consulte Activación y configuración AWS Config para Security Hub CSPM.

Los estándares de seguridad multinube, como CIS Azure Foundations Benchmark v4.0.0, tienen requisitos diferentes a los de los estándares. AWS Los estándares multinube requieren un conector CSPM de Security Hub para el proveedor de nube externo y no requieren que configure AWS Config o cree manualmente un grabador de configuración. El conector multinube CSPM de Security Hub configura automáticamente un grabador vinculado a un servicio para evaluar los recursos del entorno de nube externo.

Después de habilitar un estándar, puede desactivar o volver a habilitar posteriormente controles individuales que se aplican al estándar. Si desactiva un control para un estándar, el CSPM de Security Hub deja de generar resultados para dicho control. Además, el CSPM de Security Hub ignora ese control al calcular la puntuación de seguridad del estándar. La puntuación de seguridad es el porcentaje de controles que superaron la evaluación, en relación con el número total de controles que se aplican al estándar, están habilitados y disponen de datos de evaluación.

Cuando habilita un estándar, el CSPM de Security Hub genera una puntuación de seguridad preliminar para el estándar, normalmente dentro de los primeros 30 minutos tras su primera visita a la página Resumen o a la página Estándares de seguridad, dentro de la consola del CSPM de Security Hub. Las puntuaciones de seguridad solo se generan para los estándares que están habilitados cuando visita esas páginas en la consola. Además, se debe configurar la grabación de recursos AWS Config para que aparezcan las partituras. En las regiones de China y AWS GovCloud (US) Regions, Security Hub CSPM puede tardar hasta 24 horas en generar una puntuación de seguridad preliminar para una norma. Después de que el CSPM de Security Hub genera una puntuación preliminar, este actualiza la puntuación cada 24 horas. Para determinar cuándo se actualizó por última vez una puntuación de seguridad, puede consultar una marca de tiempo que el CSPM de Security Hub proporciona para la puntuación. Para obtener más información, consulte Calcular las puntuaciones de seguridad.

La forma en que habilita un estándar depende de si utiliza la configuración centralizada para administrar el CSPM de Security Hub para varias cuentas y Regiones de AWS. Recomendamos utilizar la configuración centralizada si desea habilitar los estándares en entornos con varias cuentas y regiones. Puede usar la configuración central si integra Security Hub con CSPM. AWS Organizations Si no utiliza la configuración centralizada, debe habilitar cada estándar por separado en cada cuenta y en cada región.

Temas

- Habilitar un estándar en varias cuentas y Regiones de AWS
- Habilitar un estándar en una sola cuenta y Región de AWS
- Verificación del estado de un estándar

Habilitar un estándar en varias cuentas y Regiones de AWS

Para habilitar y configurar un estándar de seguridad en varias cuentas y Regiones de AWS usar la configuración central. Con la configuración centralizada, el administrador delegado del CSPM de Security Hub puede crear políticas de configuración del CSPM de Security Hub que habilitan uno o

varios estándares. El administrador puede asociar posteriormente una política de configuración con cuentas individuales, unidades organizativas (UO) o con la raíz. Una política de configuración afecta a la región de origen, también denominada región de agregación, y a todas las regiones vinculadas.

Las políticas de configuración ofrecen opciones de personalización. Por ejemplo, puede optar por habilitar solo el estándar AWS Fundational Security Best Practices (FSBP) para una OU. Para otra OU, puede optar por habilitar tanto el estándar FSBP como el estándar Foundations Benchmark v1.4.0 del Center for Internet Security (CIS) AWS . Para obtener información sobre cómo crear una política de configuración que habilite los estándares que especifique, consulte Creación y asociación de políticas de configuración.

Si utiliza la configuración centralizada, el CSPM de Security Hub no habilita automáticamente ningún estándar en las cuentas nuevas o existentes. En su lugar, el administrador del CSPM de Security Hub especifica qué estándares habilitar en las distintas cuentas cuando crea políticas de configuración del CSPM de Security Hub para la organización. El CSPM de Security Hub ofrece una política de configuración recomendada en la cual solo se habilita el estándar FSBP. Para obtener más información, consulte Tipos de políticas de configuración.

> **Note**
>
> El administrador del CSPM de Security Hub puede utilizar políticas de configuración para habilitar cualquier estándar, excepto el estándar administrado por el servicio:AWS Control Tower. Para habilitar este estándar, el administrador debe usarlo directamente. AWS Control Tower También deben utilizarla AWS Control Tower para habilitar o deshabilitar los controles individuales de esta norma para una cuenta gestionada de forma centralizada.

Si desea que algunas cuentas habiliten y configuren los estándares para sus propias cuentas, el administrador de CSPM de Security Hub puede designar esas cuentas como cuentas autoadministradas. Self-managed las cuentas deben habilitar y configurar los estándares por separado en cada región.

Habilitar un estándar en una sola cuenta y Región de AWS

Si no utiliza la configuración centralizada o si tiene una cuenta autoadministrada, no puede utilizar políticas de configuración para habilitar estándares de seguridad de manera centralizada en varias cuentas o Regiones de AWS. Sin embargo, puede habilitar un estándar en una sola cuenta y región. Puede hacerlo mediante la consola del CSPM de Security Hub o mediante la API del CSPM de Security Hub.

Security Hub CSPM console

Siga estos pasos para habilitar un estándar en una cuenta y región a través de la consola del CSPM de Security Hub.

Habilitación de un estándar en una cuenta y región

1. Abra la consola CSPM de AWS Security Hub en. https://console.aws.amazon.com/securityhub/
2. Con el Región de AWS selector de la esquina superior derecha de la página, elija la región en la que desea habilitar el estándar.
3. En el panel de navegación, elija Estándares de seguridad. La página Estándares de seguridad muestra todos los estándares que el CSPM de Security Hub admite actualmente. Si ya habilitó un estándar, la sección correspondiente incluye la puntuación de seguridad actual y detalles adicionales sobre el estándar.
4. En la sección del estándar que desea habilitar, elija Habilitar estándar.

Para habilitar el estándar en otras regiones, repita los pasos anteriores en cada región adicional.

Security Hub CSPM API

Para habilitar un estándar mediante programación en una sola cuenta y región, utilice la operación BatchEnableStandards. O bien, si utilizas el AWS Command Line Interface (AWS CLI), ejecuta el batch-enable-standards comando.

En la solicitud, utilice el parámetro `StandardsArn` para especificar el nombre de recurso de Amazon (ARN) del estándar que desea habilitar. Especifique también la región a la que se aplica la solicitud. Por ejemplo, el siguiente comando habilita el estándar AWS Foundational Security Best Practices (FSBP):

```
$ aws securityhub batch-enable-standards \
--standards-subscription-requests '{"StandardsArn":"arn:aws:securityhub:us-east-1::standards/aws-foundational-security-best-practices/v/1.0.0"}' \
--region us-east-1
```

¿Dónde *`arn:aws:securityhub:us-east-1::standards/aws-foundational-security-best-practices/v/1.0.0`* está el ARN del estándar FSBP en la región EE.UU. Este (Norte de Virginia) y la región en la que *`us-east-1`* se habilita?

Para obtener el ARN de un estándar, utilice la DescribeStandards operación o, si utiliza el AWS CLI, ejecute el comando. describe-standards

Para revisar primero la lista de estándares que están habilitados actualmente en la cuenta, puede utilizar la operación GetEnabledStandards. Si utilizas el AWS CLI, puedes ejecutar el comando get-enabled-standards para recuperar esta lista.

Después de habilitar un estándar, el CSPM de Security Hub inicia las tareas necesarias para habilitar el estándar en la cuenta y en la región especificada. Esto incluye crear todos los controles que se aplican al estándar. Para supervisar el estado de estas tareas, puede consultar el estado del estándar en la cuenta y la región.

Verificación del estado de un estándar

Cuando habilita un estándar de seguridad para una cuenta, el CSPM de Security Hub empieza a crear todos los controles que corresponden a ese estándar en la cuenta. El CSPM de Security Hub también realiza otras tareas necesarias para habilitarlo, como generar una puntuación de seguridad preliminar del estándar. Mientras el CSPM de Security Hub completa estas tareas, el estado del estándar aparece como Pending para esa cuenta. Después, el estado cambia a otros valores que puede consultar y supervisar.

> **Note**
>
> Los cambios que haga en controles individuales no modifican el estado general del estándar. Por ejemplo, si vuelve a habilitar un control que antes había desactivado, el estado del estándar no cambia. Lo mismo ocurre si modifica un parámetro de un control que ya está habilitado: el estado del estándar permanece igual.

Para revisar el estado de un estándar desde la consola del CSPM de Security Hub, seleccione Estándares de seguridad en el panel de navegación. La página Estándares de seguridad muestra todos los estándares que el CSPM de Security Hub admite actualmente. Si el CSPM de Security Hub aún está en proceso de habilitar un estándar, la sección correspondiente indicará que continúa en el proceso de generar la puntuación de seguridad correspondiente al estándar. Si un estándar está habilitado, la sección correspondiente muestra la puntuación actual. Seleccione Ver resultados para revisar más detalles, incluido el estado de los controles individuales que se aplican al estándar. Para obtener más información, consulte Programación para ejecutar comprobaciones de seguridad.

Para verificar el estado de un estándar mediante programación con la API del CSPM de Security Hub, utilice la operación GetEnabledStandards. En la solicitud, puede usar de forma opcional el parámetro `StandardsSubscriptionArns` para especificar el nombre de recurso de Amazon (ARN) del estándar cuyo estado desea consultar. Si usa el AWS Command Line Interface (AWS CLI), puede ejecutar el comando get-enabled-standards para comprobar el estado de un estándar. Para indicar el ARN del estándar que desea consultar, utilice el parámetro `standards-subscription-arns`. Para determinar qué ARN especificar, puedes usar la DescribeStandards operación o, para ello, ejecutar el comando. AWS CLIdescribe-standards

Si la solicitud se completa correctamente, el CSPM de Security Hub responde con una matriz de objetos `StandardsSubscription`. Una suscripción estándar es un AWS recurso que Security Hub CSPM crea en una cuenta cuando se habilita un estándar para la cuenta. Cada objeto `StandardsSubscription` proporciona información sobre un estándar que está habilitado actualmente o que está en proceso de habilitarse o desactivarse para la cuenta. Dentro de cada objeto, el campo `StandardsStatus` indica el estado actual del estándar para la cuenta.

El estado de un estándar (`StandardsStatus`) puede ser uno de los siguientes:

PENDING

El CSPM de Security Hub realiza tareas para habilitar el estándar en la cuenta. Esto incluye crear los controles que se aplican al estándar y generar una puntuación de seguridad preliminar. El CSPM de Security Hub puede tardar varios minutos en completar todas estas tareas. Un estándar también puede tener este estado si ya está habilitado para la cuenta y el CSPM de Security Hub se encuentra en proceso de agregar controles nuevos al estándar.

Si un estándar tiene este estado, es posible que no pueda obtener los detalles de los controles individuales que se aplican al estándar. Además, es posible que no pueda configurar o desactivar controles individuales del estándar. Por ejemplo, si intenta desactivar un control mediante la operación UpdateStandardsControl, se producirá un error.

Para saber si puede configurar o administrar controles individuales del estándar, consulte el valor del campo `StandardsControlsUpdatable`. Si el valor de este campo es `READY_FOR_UPDATES`, puede comenzar a administrar los controles individuales del estándar. De lo contrario, espere a que el CSPM de Security Hub complete las tareas adicionales necesarias para habilitar el estándar.

READY

El estándar está habilitado actualmente para la cuenta. El CSPM de Security Hub puede ejecutar comprobaciones de seguridad y generar resultados para todos los controles que se aplican al estándar y que están habilitados. El CSPM de Security Hub también puede calcular una puntuación de seguridad para el estándar.

Si un estándar tiene este estado, puede consultar los detalles de los controles individuales que se aplican al estándar. Además, puede configurar, desactivar o volver a habilitar los controles. También puede desactivar el estándar.

INCOMPLETE

El CSPM de Security Hub no pudo habilitar por completo el estándar para la cuenta. El CSPM de Security Hub no puede ejecutar comprobaciones de seguridad ni generar resultados para los controles que se aplican al estándar y que están habilitados actualmente. Además, el CSPM de Security Hub no puede calcular una puntuación de seguridad para el estándar.

En el caso de los estándares multinube, la suscripción se introduce `INCOMPLETE` con el siguiente estado: `NO_AVAILABLE_MULTICLOUD_CONNECTOR` si se habilita el estándar sin un conector CSPM. La suscripción pasa automáticamente al `READY` momento en que hay un conector disponible.

Para determinar por qué el estándar no se pudo habilitar por completo, consulte la información de la `StandardsStatusReason` matriz. Esta matriz especifica los problemas que impidieron que el CSPM de Security Hub habilitara el estándar. Si ocurrió un error interno, intente habilitar nuevamente el estándar para la cuenta. Para otros tipos de problemas, comprueba tu AWS Config configuración. También puede desactivar controles individuales que no desee evaluar, o desactivar por completo el estándar.

DELETING

El CSPM de Security Hub está en proceso de completar una solicitud para desactivar el estándar de la cuenta. Esto incluye desactivar los controles que se aplican al estándar y eliminar la puntuación de seguridad asociada. El CSPM de Security Hub puede tardar varios minutos en completar esta solicitud.

Si un estándar tiene este estado, no puede volver a habilitarlo ni intentar desactivarlo otra vez para la cuenta. El CSPM de Security Hub debe concluir primero la solicitud actual. Además, no puede consultar los detalles de los controles individuales que se aplican al estándar ni administrarlos mientras el estándar está en este estado.

FAILED

El CSPM de Security Hub no pudo desactivar el estándar para la cuenta. Ocurrieron uno o más errores cuando el CSPM de Security Hub intentó desactivar el estándar. Además, el CSPM de Security Hub no puede calcular una puntuación de seguridad para el estándar.

Para determinar por qué el estándar no se desactivó por completo, consulte la información en la matriz `StandardsStatusReason`. Esta matriz especifica los problemas que impidieron que el CSPM de Security Hub desactivara el estándar.

Si un estándar tiene este estado, no puede consultar los detalles de los controles individuales que se aplican al estándar ni administrarlos. Sin embargo, puede volver a habilitar el estándar para la cuenta. Si resuelve los problemas que impidieron que el CSPM de Security Hub desactivara el estándar, también puede intentar desactivar el estándar nuevamente.

Si el estado de un estándar es `READY`, el CSPM de Security Hub ejecuta comprobaciones de seguridad y genera resultados para todos los controles que se aplican al estándar y que están habilitados. Para otros estados, el CSPM de Security Hub puede ejecutar comprobaciones y generar resultados solo para algunos controles habilitados, pero no para todos. La generación o actualización de resultados de controles puede tardar hasta 24 horas. Para obtener más información, consulte Programación para ejecutar comprobaciones de seguridad.

Revisión de los detalles de un estándar de seguridad

Después de habilitar un estándar de AWS seguridad en Security Hub CSPM, puede usar la consola para revisar los detalles del estándar. En la consola de , la página de detalles de un estándar incluye la siguiente información:

- El puntaje de seguridad actual del estándar.
- Una tabla con los controles que se aplican al estándar.
- Las estadísticas agregadas de los controles que se aplican al estándar.
- Un resumen visual del estado de los controles que se aplican al estándar.
- Un resumen visual de las comprobaciones de seguridad para los controles habilitados que se aplican al estándar. Si lo integras AWS Organizations, los controles que están habilitados en al menos una cuenta de la organización se consideran habilitados.

Para revisar estos detalles, seleccione Estándares de seguridad en el panel de navegación de la consola. Luego, en la sección del estándar, seleccione Ver salidas. Para un análisis más detallado, puede filtrar y ordenar los datos y profundizar en los detalles de los controles individuales que se aplican al estándar.

Temas

- Descripción de la puntuación de seguridad del estándar
- Revisión de los controles de un estándar

Descripción de la puntuación de seguridad del estándar

En la consola CSPM de AWS Security Hub, la página de detalles de un estándar muestra la puntuación de seguridad del estándar. La puntuación es el porcentaje de controles que superaron la evaluación, en relación con el número total de controles que se aplican al estándar, están habilitados y cuentan con datos de evaluación. Debajo de la puntuación se muestra un gráfico que resume las comprobaciones de seguridad de los controles habilitados que se aplican al estándar. Este resumen incluye la cantidad de comprobaciones de seguridad aprobadas y fallidas. En el caso de las cuentas de administrador, la puntuación y el gráfico estándar se agregan en la cuenta de administrador y en todas las cuentas de los miembros. Para revisar las comprobaciones de seguridad fallidas de los controles con una gravedad específica, seleccione la gravedad correspondiente.

Cuando habilita un estándar, el CSPM de Security Hub genera una puntuación de seguridad preliminar para el estándar, normalmente dentro de los primeros 30 minutos desde su primera visita a la página Resumen o a la página Estándares de seguridad en la consola del CSPM de Security Hub. Las puntuaciones solo se generan para los estándares que están habilitados cuando visita esas páginas. Además, se debe configurar el registro de AWS Config recursos para que aparezcan las puntuaciones. En las regiones de China y AWS GovCloud (US) Regions, Security Hub CSPM puede tardar hasta 24 horas en generar una puntuación preliminar. Después de que el CSPM de Security Hub genera una puntuación preliminar para un estándar, actualiza la puntuación cada 24 horas. Para obtener más información, consulte Calcular las puntuaciones de seguridad.

Todos los datos de las páginas de detalles de las normas de seguridad son específicos de cada región actual, a Región de AWS menos que se establezca una región de agregación. Si configura una región de agregación, las puntuaciones de seguridad se aplican en todas las regiones vinculadas e incluyen los resultados de todas esas regiones. Además, el estado de cumplimiento de los controles refleja los resultados de las regiones vinculadas, y la cantidad de comprobaciones de seguridad incluye los resultados provenientes de esas regiones.

Revisión de los controles de un estándar

Cuando utilice la consola CSPM de AWS Security Hub para revisar los detalles de una norma que haya habilitado, puede consultar una tabla de controles de seguridad que se aplican a la norma. Para cada control, la tabla incluye la siguiente información:

- El identificador y el título del control.
- El estado del control. Para obtener más información, consulte Evaluación del estado de cumplimiento y del estado del control.
- La gravedad asignada al control.
- La cantidad de comprobaciones fallidas y la cantidad total de comprobaciones. Si corresponde, el campo Comprobaciones fallidas también especifica la cantidad de resultados con un estado de Desconocido.
- Si el control admite parámetros personalizados. Para obtener más información, consulte Comprensión de los parámetros de control en el CSPM de Security Hub.

El CSPM de Security Hub actualiza los estados de los controles y la cantidad de comprobaciones de seguridad cada 24 horas. En la parte superior de la página, una marca de tiempo indica cuándo el CSPM de Security Hub actualizó estos datos por última vez.

Para las cuentas de administrador, los estados de los controles y la cantidad de comprobaciones de seguridad se agregan entre la cuenta de administrador y todas las cuentas de miembro. La cantidad de controles habilitados incluye aquellos que están habilitados para el estándar en la cuenta de administrador o en al menos una cuenta de miembro. La cantidad de controles desactivados incluye aquellos que están desactivados para el estándar en la cuenta de administrador y en todas las cuentas de miembro.

Puede filtrar la tabla de controles que se aplican al estándar. Si utiliza las opciones Filtrar por junto a la tabla, puede elegir ver únicamente los controles habilitados o únicamente los controles desactivados del estándar. Si muestra solo los controles habilitados, puede filtrar aún más la tabla por estado del control. Luego se puede centrar en los controles que tienen un estado específico. Además de las opciones Filtrar por, puede escribir criterios de filtrado en el cuadro Filtrar controles. Por ejemplo, puede filtrar por ID o título de control.

Elija el método de acceso que prefiera. Luego siga los pasos para revisar los controles que se aplican a un estándar que haya habilitado.

Security Hub CSPM console

Para revisar los controles de un estándar habilitado

1. Abra la consola AWS CSPM de Security Hub en. https://console.aws.amazon.com/securityhub/
2. Elija Estándares de seguridad en el panel de navegación.
3. En la sección del estándar, seleccione Ver resultados.

La tabla al final de la página muestra todos los controles que se aplican al estándar. Puede filtrar y ordenar la tabla. También puede descargar la página actual de la tabla como un archivo CSV. Para hacerlo, seleccione Descargar encima de la tabla. Si aplicó un filtro a la tabla, el archivo descargado solo incluirá los controles que coinciden con la configuración del filtro.

Security Hub CSPM API

Para revisar los controles de un estándar habilitado

1. Use la operación ListSecurityControlDefinitions de la API del CSPM de Security Hub. Si utiliza el comando AWS CLIhttps://docs.aws.amazon.com/cli/latest/reference/securityhub/list-security-control-definitions.html list-security-control-definitions, ejecute el comando.

   Especifique el nombre de recurso de Amazon (ARN) del estándar cuyos controles desea revisar. Para obtener los ARN de los estándares, utilice la operación o ejecute el DescribeStandards comando describe-standards. https://docs.aws.amazon.com/cli/latest/reference/securityhub/describe-standards.html Si no especifica el ARN de un estándar, el CSPM de Security Hub devuelve todos los ID de controles de seguridad.
2. Utilice la operación ListStandardsControlAssociations de la API del CSPM de Security Hub, o ejecute el comando list-standards-control-associations. Esta operación indica en qué estándares está activado un control.

   Identifique el control proporcionando el ARN o ID del control de seguridad. Los parámetros de paginación son opcionales.

El siguiente ejemplo indica en qué estándares está habilitado el Config.1 control.

```
$ aws securityhub list-standards-control-associations --region us-east-1 --security-control-id Config.1
```

Desactivación de estándares de seguridad habilitados automáticamente

Si la organización no utiliza la configuración centralizada, emplea un tipo de configuración denominada configuración local. Con la configuración local, el CSPM de AWS Security Hub puede habilitar automáticamente los estándares de seguridad predeterminados para las nuevas cuentas de miembro cuando esas cuentas se integran a la organización. Todos los controles que se aplican a estos estándares predeterminados también se habilitan automáticamente.

Actualmente, los estándares de seguridad predeterminados son el estándar AWS Foundational Security Best Practices y el estándar Foundation Benchmark v1.2.0 del Center for Internet Security (CIS) AWS . Para obtener información sobre estos estándares, consulte Referencia de estándares para el CSPM de Security Hub.

Si prefiere habilitar manualmente los estándares de seguridad para las nuevas cuentas de miembro, puede desactivar la habilitación automática de los estándares predeterminados. Solo puede hacerlo si se integra con la configuración local AWS Organizations y la usa. Si utiliza la configuración centralizada, en su lugar puede crear una política de configuración que habilite los estándares predeterminados y asociar esa política con la raíz. Todas las cuentas y UO de la organización heredan esta política de configuración, a menos que estén asociadas a una política diferente o sean autoadministradas. Si no lo integra AWS Organizations, puede deshabilitar un estándar predeterminado cuando habilite por primera vez Security Hub CSPM o una versión posterior. Para aprender a hacerlo, consulte Desactivación de un estándar.

Para desactivar la habilitación automática de los estándares predeterminados para las nuevas cuentas de miembro, puede usar la consola del CSPM de Security Hub o la API del CSPM de Security Hub.

Security Hub CSPM console

Siga estos pasos para desactivar la habilitación automática de los estándares predeterminados a través de la consola del CSPM de Security Hub.

Desactivación de la habilitación automática de estándares predeterminados

1. Abra la consola AWS CSPM de Security Hub en. https://console.aws.amazon.com/securityhub/

   Inicie sesión en las credenciales de una cuenta del administrador.

2. En el panel de navegación, en Configuración, elija Configuración.

3. En la sección Información general, seleccione Editar.
4. En Configuración de nuevas cuentas, desmarque la casilla Habilitar los estándares de seguridad predeterminados.
5. Elija Confirmar.

Security Hub CSPM API

Para desactivar la habilitación automática de los estándares predeterminados mediante programación, desde la cuenta de administrador del CSPM de Security Hub utilice la operación UpdateOrganizationConfiguration de la API del CSPM de Security Hub. En la solicitud, especifique `NONE` para el parámetro `AutoEnableStandards`.

Si está utilizando el AWS CLI, ejecute el update-organization-configuration comando para desactivar la activación automática de los estándares predeterminados. En el parámetro `auto-enable-standards`, especifique `NONE`. Por ejemplo, el siguiente comando habilita automáticamente el CSPM de Security Hub para las nuevas cuentas de miembro y desactiva la habilitación automática de los estándares predeterminados para esas cuentas.

```
$ aws securityhub update-organization-configuration --auto-enable --auto-enable-
standards NONE
```

Deshabilitación de un estándar de seguridad

Al deshabilitar un estándar de seguridad en AWS Security Hub CSPM, ocurre lo siguiente:

- Todos los controles que se aplican al estándar se desactivan, a menos que estén asociados a otro estándar que permanezca habilitado.
- Ya no se ejecutan comprobaciones de seguridad para los controles desactivados y no se generan resultados adicionales para esos controles.
- Los resultados existentes de los controles desactivados se archivan automáticamente después de aproximadamente 3 a 5 días.
- AWS Config se eliminan las reglas que el CSPM de Security Hub creó para los controles deshabilitados.

La eliminación de las AWS Config reglas apropiadas se produce normalmente a los pocos minutos de la desactivación de una norma. aunque en algunos casos puede tardar más. Si la primera

solicitud para eliminar las reglas falla, el CSPM de Security Hub vuelve a intentarlo cada 12 horas. Sin embargo, si desactivó el CSPM de Security Hub o no tiene otros estándares habilitados, el CSPM de Security Hub no puede volver a intentarlo, lo que significa que no podrá eliminar las reglas. Si esto ocurre y necesita eliminar las reglas, póngase en contacto con AWS Support.

Temas

- Deshabilitar un estándar en varias cuentas y Regiones de AWS
- deshabilitar un estándar en una sola cuenta y Región de AWS

Deshabilitar un estándar en varias cuentas y Regiones de AWS

Para deshabilitar un estándar de seguridad en varias cuentas Regiones de AWS, utilice la configuración ??? central. Con la configuración centralizada, el administrador delegado del CSPM de Security Hub puede crear políticas de configuración del CSPM de Security Hub que desactivan uno o varios estándares. El administrador puede asociar posteriormente una política de configuración con cuentas individuales, unidades organizativas (UO) o con la raíz. Una política de configuración afecta a la región de origen, también denominada región de agregación, y a todas las regiones vinculadas.

Las políticas de configuración ofrecen opciones de personalización. Por ejemplo, puede optar por desactivar el estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI-DSS) en una unidad organizativa. Para otra unidad organizativa, podría desactivar tanto el estándar PCI-DSS como el estándar NIST SP 800-53 Rev. 5. Para obtener información sobre cómo crear una política de configuración que habilite o desactive los estándares que especifique, consulte Creación y asociación de políticas de configuración.

> **Note**
>
> El administrador del CSPM de Security Hub puede usar políticas de configuración para desactivar cualquier estándar, excepto el estándar administrado por el servicio:AWS Control Tower. Para deshabilitar este estándar, el administrador debe usarlo AWS Control Tower directamente. También deben utilizarla AWS Control Tower para deshabilitar o habilitar los controles individuales de esta norma para una cuenta gestionada de forma centralizada.

Si desea que algunas cuentas configuren o deshabiliten los estándares para sus propias cuentas, el administrador de CSPM de Security Hub puede designar esas cuentas como cuentas

autoadministradas. Self-managed las cuentas deben inhabilitar los estándares por separado en cada región.

deshabilitar un estándar en una sola cuenta y Región de AWS

Si no utiliza la configuración centralizada o si tiene una cuenta autoadministrada, no puede usar políticas de configuración para desactivar estándares de seguridad de forma centralizada en varias cuentas o Regiones de AWS. Sin embargo, puede desactivar un estándar en una sola cuenta y región. Puede hacerlo mediante la consola del CSPM de Security Hub o mediante la API del CSPM de Security Hub.

Security Hub CSPM console

Siga estos pasos para desactivar un estándar en una cuenta y región con la consola del CSPM de Security Hub.

Deshabilitación de un estándar en una cuenta y región

1. Abra la consola CSPM de AWS Security Hub en. https://console.aws.amazon.com/securityhub/
2. Con el Región de AWS selector de la esquina superior derecha de la página, elija la región en la que desea deshabilitar la norma.
3. En el panel de navegación, elija Estándares de seguridad.
4. En la sección del estándar que desea desactivar, seleccione Desactivar estándar.

Para desactivar el estándar en regiones adicionales, repita los pasos anteriores en cada región adicional.

Security Hub CSPM API

Para desactivar un estándar mediante programación en una sola cuenta y región, utilice la operación BatchDisableStandards. O bien, si utilizas el AWS Command Line Interface (AWS CLI), ejecuta el batch-disable-standards comando.

En la solicitud, utilice el parámetro `StandardsSubscriptionArns` para especificar el nombre de recurso de Amazon (ARN) del estándar que desea desactivar. Si está utilizando el AWS CLI, utilice el `standards-subscription-arns` parámetro para especificar el ARN. Especifique también la región a la que se aplica la solicitud. Por ejemplo, el siguiente comando desactiva el estándar AWS Fundational Security Best Practices (FSBP) para una cuenta (): *123456789012*

```
$ aws securityhub batch-disable-standards \
--standards-subscription-arns "arn:aws:securityhub:us-
east-1:123456789012:subscription/aws-foundational-security-best-practices/v/1.0.0" \
--region us-east-1
```

¿Dónde `arn:aws:securityhub:us-east-1:123456789012:subscription/aws-foundational-security-best-practices/v/1.0.0` está el ARN del estándar FSBP para la cuenta en la región EE.UU. Este (Norte de Virginia) y la región en la que `us-east-1` se va a deshabilitar?

Para obtener el ARN de un estándar, puede usar la operación GetEnabledStandards. Esta operación recupera información sobre los estándares que están habilitados actualmente en la cuenta. Si utilizas el AWS CLI, puedes ejecutar el comando https://docs.aws.amazon.com/cli/latest/reference/securityhub/get-enabled-standards.html get-enabled-standards para recuperar esta información.

Después de desactivar un estándar, el CSPM de Security Hub comienza a ejecutar tareas para desactivar el estándar en la cuenta y en la región especificada. Esto incluye desactivar todos los controles que se aplican al estándar. Para supervisar el estado de estas tareas, puede consultar el estado del estándar en la cuenta y la región.

Comprensión de los controles de seguridad en el CSPM de Security Hub

En AWS Security Hub CSPM, un control de seguridad, también denominado control, es una salvaguarda dentro de un estándar de seguridad que ayuda a una organización a proteger la confidencialidad, integridad y disponibilidad de su información. En Security Hub CSPM, un control está relacionado con un recurso específico. AWS

Cuando habilita un control en uno o más estándares, el CSPM de Security Hub comienza a ejecutar comprobaciones de seguridad en este. Las comprobaciones de seguridad generan los resultados del CSPM de Security Hub. Cuando desactiva un control, el CSPM de Security Hub deja de ejecutar las comprobaciones de seguridad sobre este y deja de generar los resultados correspondientes.

Puede habilitar o deshabilitar los controles de forma individual para una sola cuenta y. Región de AWS Para ahorrar tiempo y reducir los errores de configuración en los entornos multicuenta, recomendamos utilizar la configuración centralizada para activar o desactivar los controles. Con

la configuración centralizada, el administrador delegado del CSPM de Security Hub puede crear políticas que especifiquen cómo se debe configurar un control en varias cuentas y regiones. Para obtener más información sobre cómo habilitar y deshabilitar controles, consulte Habilitación de controles en el CSPM de Security Hub.

Vista de controles consolidados

La página de controles de la consola CSPM de Security Hub muestra todos los controles disponibles en ese momento Región de AWS (para ver los controles en el contexto de una norma, visite la página de normas de seguridad y seleccione una norma habilitada). El CSPM de Security Hub asigna a los controles un identificador, un título y una descripción coherentes en todos los estándares. Los ID de los controles incluyen el número correspondiente Servicio de AWS y un número único (por ejemplo, CodeBuild.3).

La siguiente información está disponible en la página Controles de la consola del CSPM de Security Hub:

- Una puntuación general de seguridad basada en la proporción de controles aprobados en comparación con el número total de controles habilitados con datos
- Desglose de los estados de control en todos los controles compatibles con el CSPM de Security Hub
- El número total de controles de seguridad aprobados y con fallos.
- El número de controles de seguridad con fallos para controles de diferente gravedad y los enlaces para ver más detalles sobre esos controles de seguridad con fallos.
- Una lista de controles del CSPM de Security Hub, con filtros para ver subconjuntos específicos de controles.

En la página Controles, puede elegir un control para ver sus detalles y tomar medidas en función de los resultados generados por el control. Desde esta página, también puedes activar o desactivar un control de seguridad en tu Cuenta de AWS y actual Región de AWS. Las acciones de activación y desactivación de la página Controles se aplican a todos los estándares. Para obtener más información, consulte Habilitación de controles en el CSPM de Security Hub.

En el caso de las cuentas de administrador, la página Controles refleja el estado de los controles en las cuentas de los miembros. Si se produce un error en una comprobación de control en al menos una cuenta miembro, el estado de control es Con error. Si ha establecido una región de agregación, la página Controles refleja el estado de los controles en todas las regiones vinculadas. Si se produce

un error en una comprobación de control en al menos una región vinculada, el estado del control es Con error.

La vista de controles consolidados provoca cambios en los campos de búsqueda de controles del formato de búsqueda de AWS seguridad (ASFF) que pueden afectar a los flujos de trabajo. Para obtener más información, consulte Vista de controles consolidada: cambios en ASFF.

Puntuación general de seguridad de los controles

La página Controles muestra una puntuación de seguridad general que va del 0 al 100 por ciento. La puntuación de seguridad general se calcula en función de la proporción de controles aprobados en comparación con el número total de controles habilitados con datos en todos los estándares.

> **Note**
>
> Para ver la puntuación de seguridad general de los controles, debe agregar al rol de IAM que utiliza para acceder al CSPM de Security Hub.un permiso para llamar a **`BatchGetControlEvaluations`**. Este permiso no es necesario para ver las puntuaciones de seguridad según estándares específicos.

Al habilitar el CSPM de Security Hub, la solución calcula la puntuación de seguridad inicial en un plazo de 30 minutos después de su primera visita a la página Resumen o a la página Estándares de seguridad de la consola del CSPM de Security Hub. Las puntuaciones de seguridad por primera vez pueden tardar hasta 24 horas en generarse en las regiones de China y de AWS GovCloud (US) Regions.

Además de la puntuación de seguridad general, el CSPM de Security Hub calcula una puntuación de seguridad para cada estándar habilitado en un plazo de 30 minutos después de su primera visita a la página Resumen o a la página Estándares de seguridad. Para ver una lista de los estándares que están habilitados actualmente, utilice la operación de API `GetEnabledStandards`.

AWS Config debe estar habilitado con el registro de recursos para que aparezcan las partituras. Para obtener más información sobre cómo el CSPM de Security Hub calcula las puntuaciones de seguridad, consulte Calcular las puntuaciones de seguridad.

Tras la primera generación de puntuaciones, el CSPM de Security Hub actualiza las puntuaciones de seguridad cada 24 horas. El CSPM de Security Hub muestra una marca de tiempo que indica cuándo se actualizó por última vez la puntuación de seguridad.

Si ha establecido una región de agregación, la puntuación de seguridad general refleja los resultados de control en las regiones vinculadas.

Referencia de controles para el CSPM de Security Hub

Esta referencia de controles proporciona una tabla de los controles CSPM de AWS Security Hub disponibles con enlaces a más información sobre cada control. En la tabla, los controles están organizados en orden alfabético según su ID de control. Aquí solo se incluyen los controles que el CSPM de Security Hub tiene en uso activo. Los controles retirados quedan excluidos de la tabla.

La tabla proporciona la siguiente información para cada control:

- ID de control de seguridad: este ID se aplica a todos los estándares e indica el Servicio de AWS recurso al que se refiere el control. La consola del CSPM de Security Hub muestra los ID de los controles de seguridad, sin importar si la funcionalidad de resultados consolidados de controles está habilitada o desactivada en la cuenta. Sin embargo, los resultados del CSPM de Security Hub solo hacen referencia a los ID de los controles de seguridad si la funcionalidad de resultados consolidados de controles está habilitada en la cuenta. Si los resultados de control consolidados están desactivados en su cuenta, algunos identificadores de control varían según el estándar en los resultados de control. Para ver un mapeo de los identificadores de control específicos del estándar con los identificadores de control de seguridad, consulte Cómo afecta la consolidación a las identificaciones y títulos de control.

  Si desea configurar las automatizaciones de los controles de seguridad, le recomendamos que filtre en función del identificador del control y no del título o la descripción. Aunque el CSPM de Security Hub actualiza ocasionalmente los títulos o las descripciones de los controles, los ID de los controles permanecen iguales.

  Los identificadores de control pueden omitir números. Estos son marcadores de posición para futuros controles.

- Título de control de seguridad: este título se aplica a todos los estándares. La consola del CSPM de Security Hub muestra los títulos de los controles de seguridad sin importar si la funcionalidad de resultados consolidados de controles está habilitada o desactivada en la cuenta. Sin embargo, los resultados del CSPM de Security Hub solo hacen referencia a los títulos de los controles de seguridad si la funcionalidad de resultados consolidados de controles está habilitada en la cuenta. Si los resultados de control consolidados están desactivados en su cuenta, algunos títulos de control varían según el estándar en los resultados de control. Para ver un mapeo de los

identificadores de control específicos del estándar con los identificadores de control de seguridad, consulte Cómo afecta la consolidación a las identificaciones y títulos de control.

- Normas aplicables: indica a qué normas se aplica un control. Seleccione un control para revisar los requisitos específicos de los marcos de cumplimiento de terceros.
- Gravedad: la gravedad de un control identifica su importancia desde el punto de vista de la seguridad. Para obtener información sobre cómo el CSPM de Security Hub determina la gravedad del control, consulte Niveles de gravedad correspondientes a los resultados de control.
- Admite parámetros personalizados: indica si el control admite valores personalizados para uno o varios parámetros. Seleccione un control para revisar los detalles de los parámetros. Para obtener más información, consulte Comprensión de los parámetros de control en el CSPM de Security Hub.
- Tipo de programa: indica cuándo se evalúa el control. Para obtener más información, consulte Programación para ejecutar comprobaciones de seguridad.

Seleccione un control para revisar información adicional. Los controles están organizados en orden alfabético según el ID del control de seguridad.

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
Account.1	Se debe proporcionar la información de contacto de seguridad para un Cuenta de AWS	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, AWS Foundational Security Best Practices v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	Periódico
Account.2	Cuenta de AWS debe AWS Organizations	NIST SP 800-53 Rev. 5	ALTO	⊗ No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
	ser parte de una organización				
ACM.1	ACM-issued Los certificados importados y renovados deben renovarse después de un período de tiempo específico	AWS Fundational Security Best Practices v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1	MEDIO	Sí	El cambio se desencadena y es periódico
ACM.2	Los certificados RSA administrados por ACM deben usar una longitud de clave de al menos 2048 bits	AWS Mejores prácticas fundamentales de seguridad v1.0.0, PCI DSS v4.0.1	ALTO	No	El cambio se ha activado
ACM.3	Los certificados ACM deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
Amplify.1	Las aplicaciones de Amplify deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
Amplify.2	Las ramificaciones de Amplify deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
APIGateway.1	El registro de ejecución de WebSocket API y REST de API Gateway deben estar habilitados	AWS Mejores prácticas básicas de seguridad v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	Sí	El cambio se ha activado
APIGateway.2	Las etapas de la API de REST de API Gateway deben configurarse para usar certificados SSL para la autenticación de backend	AWS Mejores prácticas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	MEDIO	No	El cambio se ha activado
APIGateway.3	Las etapas de la API AWS X-Ray REST de API Gateway deben tener habilitado el rastreo	AWS Mejores prácticas básicas de seguridad v1.0.0, NIST SP 800-53 Rev. 5	BAJA	No	El cambio se ha activado
APIGateway.4	La API de Gateway debe estar asociada a una ACL web de WAF	AWS Mejores prácticas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
APIGateway.5	Los datos de la caché de la API de REST de API Gateway deben cifrarse en reposo	AWS Mejores prácticas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	El cambio se ha activado
APIGateway.8	Las rutas de API Gateway deben especificar un tipo de autorización	AWS Mejores prácticas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	⊙ Sí	Periódico
APIGateway.9	El registro de acceso debe configurarse para las etapas V2 de API Gateway	AWS Mejores prácticas de seguridad básicas v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	⊗ No	El cambio se ha activado
APIGateway.10	Las integraciones de API Gateway V2 deben usar HTTPS para las conexiones privadas	AWS Mejores prácticas fundamentales de seguridad v1.0.0	MEDIO	⊗ No	El cambio se ha activado
APIGateway.11	Los nombres de dominio de API Gateway deben usar las políticas de seguridad recomendadas	AWS Mejores prácticas fundamentales de seguridad	MEDIO	⊗ No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
AppConfig.1	AWS AppConfig las aplicaciones deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
AppConfig.2	AWS AppConfig Los perfiles de configuración deben etiquetarse	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
AppConfig.3	AWS AppConfig los entornos deben etiquetarse	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
AppConfig.4	AWS AppConfig las asociaciones de extensiones deben etiquetarse	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
AppFlow.1	AppFlow Los flujos de Amazon deben etiquetarse	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
AppRunner.1	Los servicios de App Runner deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
AppRunner.2	Los conectores de VPC de App Runner deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
AppSync.2	AWS AppSync debe tener habilitado el registro a nivel de campo	AWS Mejores prácticas de seguridad básicas v1.0.0, PCI DSS v4.0.1	MEDIO	Sí	El cambio se ha activado
AppSync.4	AWS AppSync Las API de GraphQL deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
AppSync.5	AWS AppSync Las API de GraphQL no deben autenticarse con claves de API	AWS Mejores prácticas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5	ALTO	No	El cambio se ha activado
Athena.2	Los catálogos de datos de Athena deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
Athena.3	Los grupos de trabajo de Athena deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
Athena.4	Los grupos de trabajo de Athena deben tener el registro habilitado	AWS Mejores prácticas fundamentales de seguridad	MEDIO	⊗ No	El cambio se ha activado
AutoScaling.1	Los grupos de escalado automático asociados con un equilibrador de carga deben usar comprobaciones de estado de ELB	AWS Mejores prácticas fundamentales de seguridad, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5	BAJA	⊗ No	El cambio se ha activado
AutoScaling.2	El grupo de Amazon EC2 Auto Scaling debe cubrir varias zonas de disponibilidad	AWS Mejores prácticas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	⊙ Sí	El cambio se ha activado
AutoScaling.3	Las configuraciones de lanzamiento de grupo de escalado automático deben configurar las instancias de EC2 para que requieran el servicio de metadatos de instancias versión 2 (IMDSv2)	AWS Mejores prácticas de seguridad básicas v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	ALTO	⊗ No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
Autoscaling.5	Las instancias de Amazon EC2 lanzadas mediante configuraciones de lanzamiento de grupo de escalado automático no deben tener direcciones IP públicas	AWS Mejores prácticas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	ALTO	⊗ No	El cambio se ha activado
AutoScaling.6	Los grupos de escalado automático deben usar varios tipos de instancias en varias zonas de disponibilidad	AWS Mejores prácticas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	El cambio se ha activado
AutoScaling.9	Los grupos de escalado automático de EC2 deberían usar plantillas de lanzamiento de EC2	AWS Mejores prácticas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	El cambio se ha activado
AutoScaling.10	Los grupos de escalado automático de EC2 deberían estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	⊙ Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
Backup.1	AWS Backup los puntos de recuperación deben estar cifrados en reposo	AWS Mejores prácticas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	No	El cambio se ha activado
Backup.2	AWS Backup los puntos de recuperación deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
Backup.3	AWS Backup Las bóvedas deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
Backup.4	AWS Backup Los planes de informes deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
Backup.5	AWS Backup los planes de respaldo deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
Batch.1	Las colas de trabajos de Batch deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
Batch.2	Las políticas de programación de Batch deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
Batch.3	Los entornos de computación de Batch deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
Batch.4	Las propiedades de los recursos de computación en los entornos de computación administrados de Batch deben estar etiquetadas.	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
Bedrock.1	Las fuentes de datos de Amazon Bedrock deben cifrarse con claves administradas por el cliente AWS KMS	AWS Mejores prácticas de seguridad fundamentales	MEDIO	No	El cambio se ha activado
BedrockAgentCore.1	Los AgentCore tiempos de ejecución de Bedrock deben configurarse con el modo de red VPC	AWS Mejores prácticas de seguridad fundamentales	ALTO	No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
BedrockAgentCore.2	Bedrock AgentCore Gateways debería requerir autorización para las solicitudes entrantes	AWS Mejores prácticas de seguridad fundamentales	ALTO	⊗ No	El cambio se ha activado
BedrockAgentCore.3	Bedrock AgentCore Memory debe cifrarse con claves administradas por el cliente AWS KMS	NIST SP 800-53 Rev. 5	MEDIO	⊗ No	El cambio se ha activado
BedrockAgentCore.4	Bedrock AgentCore Gateway debe cifrarse con claves administradas por el cliente AWS KMS	NIST SP 800-53 Rev. 5	MEDIO	⊗ No	El cambio se ha activado
BedrockAgentCore.5	Los navegadores AgentCore personalizados de Bedrock no deben usar el modo de red pública	AWS Mejores prácticas de seguridad fundamentales	ALTO	⊗ No	El cambio se ha activado
BedrockAgentCore.6	Los navegadores AgentCore personalizados de Bedrock deben tener habilitada la grabación de sesiones	AWS Mejores prácticas de seguridad fundamentales	MEDIO	⊗ No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
BedrockAgentCore.7	Los intérpretes de código AgentCore personalizados de Bedrock deben usar una configuración de red privada	AWS Mejores prácticas de seguridad fundamentales	ALTO	⊗ No	El cambio se ha activado
CloudFormation.2	CloudFormation las pilas deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	⊙ Sí	El cambio se ha activado
CloudFormation.3	CloudFormation las pilas deben tener habilitada la protección de terminación	AWS Mejores prácticas fundamentales de seguridad	MEDIO	⊗ No	El cambio se ha activado
CloudFormation.4	CloudFormation las pilas deben tener funciones de servicio asociadas	AWS Mejores prácticas de seguridad fundamentales	MEDIO	⊗ No	El cambio se ha activado
CloudFront.1	CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado	AWS Mejores prácticas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	ALTO	⊗ No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
CloudFront.3	CloudFront las distribuciones deben requerir el cifrado en tránsito	AWS Mejores prácticas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	⊗ No	El cambio se ha activado
CloudFront.4	CloudFront las distribuciones deben tener configurada la conmutación por error de origen	AWS Mejores prácticas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5	BAJA	⊗ No	El cambio se ha activado
CloudFront.5	CloudFront las distribuciones deben tener habilitado el registro	AWS Mejores prácticas de seguridad básicas v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	⊗ No	El cambio se ha activado
CloudFront.6	CloudFront las distribuciones deben tener WAF activado	AWS Mejores prácticas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	⊗ No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
CloudFront.7	CloudFront las SSL/TLS distribuciones deben usar certificados personalizados	AWS Fundational Security Best Practices v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	BAJA	⊗ No	El cambio se ha activado
CloudFront.8	CloudFront las distribuciones deben usar SNI para atender las solicitudes HTTPS	AWS Mejores prácticas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5	BAJA	⊗ No	El cambio se ha activado
CloudFront.9	CloudFront las distribuciones deben cifrar el tráfico para convertirlo en orígenes personalizados	AWS Mejores prácticas de seguridad básicas v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	⊗ No	El cambio se ha activado
CloudFront.10	CloudFront las distribuciones no deben usar protocolos SSL obsoletos entre las ubicaciones de borde y los orígenes personalizados	AWS Fundational Security Best Practices v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1	MEDIO	⊗ No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
CloudFront.12	CloudFront las distribuciones no deben apuntar a orígenes inexistentes de S3	AWS Mejores prácticas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	ALTO	⊗ No	Periódico
CloudFront.13	CloudFront las distribuciones deben usar el control de acceso de origen	AWS Mejores prácticas fundamentales de seguridad v1.0.0	MEDIO	⊗ No	El cambio se ha activado
CloudFront.14	CloudFront las distribuciones deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	⊙ Sí	El cambio se ha activado
CloudFront.15	CloudFront las distribuciones deben usar la política de seguridad TLS recomendada	AWS Mejores prácticas fundamentales de seguridad v1.0.0	MEDIO	⊗ No	El cambio se ha activado
CloudFront.16	CloudFront las distribuciones deben usar el control de acceso de origen para los orígenes de las URL de las funciones de Lambda	AWS Mejores prácticas de seguridad fundamentales v1.0.0	MEDIO	⊗ No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
CloudFront.17	CloudFront las distribuciones deben usar grupos de claves confiables para las URL y cookies firmadas	AWS Mejores prácticas fundamentales de seguridad v1.0.0	MEDIO	⊗ No	El cambio se ha activado
CloudTrail.1	CloudTrail debe habilitarse y configurarse con al menos un registro multirregional que incluya eventos de administración de lectura y escritura	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CIS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, AWS Foundational Security Best Practices, NIST SP 800-53 Rev AWS . 5	ALTO	⊗ No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
CloudTrail.2	CloudTrail debe tener habilitado el cifrado en reposo	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CIS Foundations Benchmark v1.2.0, CIS AWS Foundations Benchmark v1.4.0 AWS AWS Foundational Security Best Practices v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v3.2.1, PCI DSS v4.0.1	MEDIO	⊗ No	Periódico
CloudTrail.3	CloudTrail Debe estar habilitada al menos una ruta	NIST SP 800-171 Rev. 2; PCI DSS v4.0.1; PCI DSS v3.2.1	ALTO	⊗ No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
CloudTrail.4	CloudTrail La validación del archivo de registro debe estar habilitada	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CIS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, AWS AWS Foundational Security Best Practices v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1, PCI DSS v3.2.1	BAJA	⊗ No	Periódico
CloudTrail.5	CloudTrail CloudWatch las rutas deben estar integradas con Amazon Logs	CIS AWS Foundations Benchmark v1.2.0, CIS AWS Foundations Benchmark v1.4.0, AWS Foundational Security Best Practices v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1	MEDIO	⊗ No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
CloudTrail.6	Asegúrese de que CloudTrail el bucket S3 utilizado para almacenar los registros no sea de acceso público	CIS AWS Foundations Benchmark v1.2.0, CIS AWS Foundations Benchmark v1.4.0, PCI DSS v4.0.1	CRÍTICO	⊗ No	El cambio se desencadena y es periódico
CloudTrail.7	Asegúrese de que el registro de acceso al bucket S3 esté habilitado en el bucket S3 CloudTrail	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CIS Foundations Benchmark v1.2.0, CIS AWS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v3.0.0, PCI DSS v4.0.1 AWS	BAJA	⊗ No	Periódico
CloudTrail.9	CloudTrail los senderos deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	⊙ Sí	El cambio se ha activado
CloudTrail.10	CloudTrail Los almacenes de datos de eventos de Lake deben estar cifrados y gestionados por el cliente AWS KMS keys	NIST SP 800-53 Rev. 5	MEDIO	⊙ Sí	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
CloudWatch.1	Debe existir un filtro de métrica de registro y una alarma para el uso del usuario raíz	CIS AWS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 Rev. 2, PCI DSS v3.2.1	BAJA	⊗ No	Periódico
CloudWatch.2	Asegurar que haya un filtro de métricas de registro y alarma para las llamadas a la API no autorizadas	CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 Rev. 2	BAJA	⊗ No	Periódico
CloudWatch.3	Garantizar que haya un filtro de métricas de registro y una alarma de registro para el inicio de sesión en la sin MFA en la consola de administración	CIS AWS Foundations Benchmark v1.2.0	BAJA	⊗ No	Periódico
CloudWatch.4	Garantizar que haya un filtro de métricas de registro y una alarma para los cambios de política de IAM	CIS AWS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 Rev. 2	BAJA	⊗ No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
CloudWatch.5	Asegúrese de que haya un registro, un filtro métrico y una alarma para los cambios de configuración CloudTrail	CIS AWS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 Rev. 2	BAJA	⊗ No	Periódico
CloudWatch.6	Asegúrese de que haya un filtro métrico de registro y una alarma para los errores de autenticación Consola de administración de AWS	CIS AWS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 Rev. 2	BAJA	⊗ No	Periódico
CloudWatch.7	Garantizar que haya un filtro de métricas de registro y una alarma para la deshabilitación o eliminación programada de las CMK creadas por el cliente	CIS AWS Foundations Benchmark v1.4.0, CIS Foundations Benchmark v1.2.0, NIST SP 800-171 Rev. 2 AWS	BAJA	⊗ No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
CloudWatch.8	Garantizar que haya un filtro de métricas de registro y una alarma para los cambios de política de bucket de S3	CIS AWS Foundations Benchmark v1.4.0, CIS Foundations Benchmark v1.2.0, NIST SP 800-171 Rev. 2 AWS	BAJA	⊗ No	Periódico
CloudWatch.9	Asegúrese de que haya un registro, un filtro métrico y una alarma para los cambios de configuración AWS Config	CIS AWS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 Rev. 2	BAJA	⊗ No	Periódico
CloudWatch.10	Garantizar que haya un filtro de métricas de registro y una alarma para los cambios de grupos de seguridad	CIS AWS Foundations Benchmark v1.4.0, CIS Foundations Benchmark v1.2.0, NIST SP 800-171 Rev. 2 AWS	BAJA	⊗ No	Periódico
CloudWatch.11	Garantizar que haya un filtro de métricas de registro y una alarma para los cambios en las listas de control de acceso a la red (NACL)	CIS AWS Foundations Benchmark v1.4.0, CIS Foundations Benchmark v1.2.0, NIST SP 800-171 Rev. 2 AWS	BAJA	⊗ No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
CloudWatch.12	Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios a las puertas de enlace de la red	CIS AWS Foundations Benchmark v1.4.0, CIS Foundations Benchmark v1.2.0, NIST SP 800-171 Rev. 2 AWS	BAJA	⊗ No	Periódico
CloudWatch.13	Garantizar que haya un filtro de métricas de registro y una alarma para los cambios en la tabla de enrutamiento	CIS AWS Foundations Benchmark v1.4.0, CIS Foundations Benchmark v1.2.0, NIST SP 800-171 Rev. 2 AWS	BAJA	⊗ No	Periódico
CloudWatch.14	Garantizar que haya un filtro de métricas de registro y una alarma para los cambios en la VPC	CIS AWS Foundations Benchmark v1.4.0, CIS Foundations Benchmark v1.2.0, NIST SP 800-171 Rev. 2 AWS	BAJA	⊗ No	Periódico
CloudWatch.15	CloudWatch las alarmas deben tener configuradas acciones específicas	NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	ALTO	⊙ Sí	El cambio se ha activado
CloudWatch.16	CloudWatch los grupos de registros deben conservarse durante un período de tiempo específico	NIST SP 800-53 Rev. 5	MEDIO	⊙ Sí	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
CloudWatch.17	CloudWatch las acciones de alarma deben estar habilitadas	NIST SP 800-53 Rev. 5	ALTO	⊗ No	El cambio se ha activado
CodeArtifact.1	CodeArtifact los repositorios deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	⊙ Sí	El cambio se ha activado
CodeBuild.1	CodeBuild Las URL del repositorio de origen de Bitbucket no deben contener credenciales confidenciales	AWS Mejores prácticas básicas de seguridad, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1	CRÍTICO	⊗ No	El cambio se ha activado
CodeBuild.2	CodeBuild Las variables de entorno del proyecto no deben contener credenciales en texto sin cifrar	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1	CRÍTICO	⊗ No	El cambio se ha activado
CodeBuild.3	CodeBuild Los registros de S3 deben estar cifrados	AWS Mejores prácticas básicas de seguridad, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1,	BAJA	⊗ No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
CodeBuild.4	CodeBuild los entornos de proyecto deben tener una configuración de registro	AWS Mejores prácticas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	El cambio se ha activado
CodeBuild.7	CodeBuild las exportaciones de grupos de informes deben cifrarse en reposo	AWS Mejores prácticas fundamentales de seguridad	MEDIO	⊗ No	El cambio se ha activado
CodeGuruProfiler.1	CodeGuru Los grupos de creación de perfiles de Profiler deben etiquetarse	AWS Estándar de etiquetado de recursos	BAJA	⊙ Sí	El cambio se ha activado
CodeGuruReviewer.1	CodeGuru Las asociaciones de repositorios de Reviewer deben etiquetarse	AWS Estándar de etiquetado de recursos	BAJA	⊙ Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
Cognito.1	Los grupos de usuarios de Cognito deben tener la protección contra amenazas activada con el modo de aplicación de funciones completo para la autenticación estándar	AWS Mejores prácticas fundamentales de seguridad	MEDIO	Sí	El cambio se ha activado
Cognito.2	Los grupos de identidades de Cognito no deben permitir identidades sin autenticar	AWS Mejores prácticas fundamentales de seguridad	MEDIO	No	El cambio se ha activado
Cognito.3	Las políticas de contraseñas para grupos de usuarios de Cognito deben tener configuraciones seguras	AWS Mejores prácticas fundamentales de seguridad	MEDIO	Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
Cognito.4	Los grupos de usuarios de Cognito deben tener activada la protección contra amenazas y el modo de aplicación con todas las funciones para la autenticación personalizada	AWS Mejores prácticas fundamentales de seguridad	MEDIO	⊗ No	El cambio se ha activado
Cognito.5	La MFA debe estar habilitada para los grupos de usuarios de Cognito	AWS Mejores prácticas fundamentales de seguridad	MEDIO	⊗ No	El cambio se ha activado
Cognito.6	Los grupos de usuarios de Cognito deben tener habilitada la protección contra la eliminación	AWS Mejores prácticas fundamentales de seguridad	MEDIO	⊗ No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
Config.1	AWS Config debe estar habilitada y usar la función vinculada al servicio para el registro de recursos	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CIS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, AWS AWS Foundational Security Best Practices, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1	CRÍTICO	Sí	Periódico
Connect.1	Los tipos de objetos de Connect Customer Profiles deben etiquetarse	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
Connect.2	Las instancias de Connect Customer deben tener habilitado el CloudWatch registro	AWS Mejores prácticas fundamentales de seguridad	MEDIO	No	El cambio se ha activado
DataFirehose.1	Los flujos de entrega de Firehose deben estar cifrados en reposo	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5	MEDIO	No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
DataSync.1	DataSync las tareas deben tener el registro habilitado	AWS Mejores prácticas fundamentales de seguridad	MEDIO	⊗ No	El cambio se ha activado
DataSync.2	DataSync las tareas deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	⊙ Sí	El cambio se ha activado
Detective.1	Los gráficos de comportamiento de Detective deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	⊙ Sí	El cambio se ha activado
DMS.1	Las instancias de replicación de Servicio de migración de bases de datos no deben ser públicas	AWS Mejores prácticas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1	CRÍTICO	⊗ No	Periódico
DMS.2	Los certificados DMS deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	⊙ Sí	El cambio se ha activado
DMS.3	Las suscripciones a eventos de DMS deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	⊙ Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
DMS.4	Las instancias de replicación de DMS deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	⊙ Sí	El cambio se ha activado
DMS.5	Los grupos de subredes de replicación del DMS deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	⊙ Sí	El cambio se ha activado
DMS.6	Las instancias de replicación de DMS deben tener habilitada la actualización automática de las versiones secundarias	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	⊗ No	El cambio se ha activado
DMS.7	Las tareas de replicación del DMS para la base de datos de destino deben tener el registro habilitado	AWS Mejores prácticas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	⊗ No	El cambio se ha activado
DMS.8	Las tareas de replicación del DMS para la base de datos de origen deben tener el registro habilitado	AWS Mejores prácticas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	⊗ No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
DMS.9	Los puntos finales del DMS deben usar SSL	AWS Mejores prácticas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	⊗ No	El cambio se ha activado
DMS.10	Los puntos de conexión de DMS para las bases de datos de Neptune deben tener habilitada la autorización de IAM	AWS Mejores prácticas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	⊗ No	El cambio se ha activado
DMS.11	Los puntos de conexión de DMS para MongoDB deben tener un mecanismo de autenticación habilitado	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	⊗ No	El cambio se ha activado
DMS.12	Los puntos de conexión de DMS para Redis OSS deben tener el TLS habilitado	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	⊗ No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
DMS.13	Las instancias de replicación de DMS se deben configurar para utilizar varias zonas de disponibilidad	AWS Mejores prácticas fundamentales de seguridad	MEDIO	⊗ No	El cambio se ha activado
DocumentDB.1	Los clústeres de Amazon DocumentDB deben estar cifrados en reposo	AWS Mejores prácticas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	El cambio se ha activado
DocumentDB.2	Los clústeres de Amazon DocumentDB deben tener un período de retención de copias de seguridad adecuado	AWS Mejores prácticas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	⊙ Sí	El cambio se ha activado
DocumentDB.3	Las instantáneas de clústeres manuales de Amazon DocumentDB no deben ser públicas	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	CRÍTICO	⊗ No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
DocumentDB.4	Los clústeres de Amazon DocumentDB deben publicar los registros de auditoría en Logs CloudWatch	AWS Mejores prácticas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	⊗ No	El cambio se ha activado
DocumentDB.5	Los clústeres de Amazon DocumentDB deben tener habilitada la protección contra eliminaciones	AWS Mejores prácticas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	El cambio se ha activado
DocumentDB.6	Los clústeres de Amazon DocumentDB deben estar cifrados en tránsito	AWS Mejores prácticas fundamentales de seguridad	MEDIO	⊗ No	Periódico
DynamoDB.1	Las tablas de DynamoDB deberían escalar automáticamente la capacidad en función de la demanda	AWS Mejores prácticas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	⊙ Sí	Periódico
DynamoDB.2	Las tablas de DynamoDB tienen que tener habilitada la recuperación a un momento dado	AWS Mejores prácticas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
DynamoDB 3	Los clústeres de DynamoDB Accelerator (DAX) deben cifrarse en reposo	AWS Mejores prácticas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	Periódico
DynamoDB 4	Las tablas de DynamoDB deben estar presentes en un plan de copia de seguridad	NIST SP 800-53 Rev. 5	MEDIO	⊙ Sí	Periódico
DynamoDB 5	Las tablas de DynamoDB deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	⊙ Sí	El cambio se ha activado
DynamoDB 6	Las tablas de DynamoDB deben tener la protección contra eliminación habilitada	AWS Mejores prácticas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	El cambio se ha activado
DynamoDB 7	Los clústeres del Acelerador de DynamoDB deben estar cifrados en tránsito	AWS Mejores prácticas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	⊗ No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
EC2.1	Las instantáneas de EBS no se deben poder restaurar públicamente	AWS Mejores prácticas fundamentales de seguridad v1.0.0, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5	CRÍTICO	⊗ No	Periódico
EC2.2	Los grupos de seguridad predeterminados de VPC no deben permitir el tráfico entrante ni saliente	CIS AWS Foundations Benchmark v5.0.0, CIS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.2.0, AWS Foundational Security Best Practices v1.0.0, PCI AWS DSS v3.2.1, CIS Foundations Benchmark v1.4.0, NIST SP 800-53 Rev. 5 AWS	ALTO	⊗ No	El cambio se ha activado
EC2.3	Los volúmenes de EBS asociados deben cifrarse en reposo	AWS Mejores prácticas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
EC2.4	Las instancias EC2 detenidas deben eliminarse después de un período de tiempo específico	AWS Mejores prácticas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	Sí	Periódico
EC2.6	El registro de flujos de VPC debe estar habilitado en todos los VPC	CIS AWS Foundations Benchmark v5.0.0, CIS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.2.0, AWS AWS Foundational Security Best Practices v1.0.0, PCI DSS v3.2.1, CIS Foundations Benchmark v1.4.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2 AWS	MEDIO	No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
EC2.7	El cifrado predeterminado EBS debe estar habilitado	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, AWS Foundational Security Best Practices v1.0.0, CIS AWS Foundations Benchmark v1.4.0, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	Periódico
EC2.8	Las instancias EC2 deben usar el servicio de metadatos de instancias (IMDS) versión 2 (IMDSv2)	CIS AWS Foundations Benchmark v5.0.0, CIS Foundations Benchmark v3.0.0, AWS Foundational Security Best Practices, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1 AWS	ALTO	⊗ No	El cambio se ha activado
EC2.9	Las instancias EC2 no deben tener una dirección IPv4 pública	AWS Mejores prácticas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5	ALTO	⊗ No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
EC2.10	Amazon EC2 debe configurarse para utilizar los puntos de enlace de VPC que se crean para el servicio Amazon EC2	AWS Mejores prácticas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	MEDIO	⊗ No	Periódico
EC2.12	Los EIP EC2 sin utilizar deben eliminarse	PCI DSS v3.2.1, NIST SP 800-53 rev. 5	BAJA	⊗ No	El cambio se ha activado
EC2.13	Los grupos de seguridad no deben permitir la entrada desde la versión 0.0.0. 0/0 o: :/0 al puerto 22	CIS AWS Foundations Benchmark v1.2.0, PCI DSS v3.2.1, PCI DSS v4.0.1, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	ALTO	⊗ No	El cambio se desencadena y es periódico
EC2.14	Los grupos de seguridad no deben permitir la entrada desde la versión 0.0.0. 0/0 o: :/0 al puerto 3389	CIS AWS Foundations Benchmark v1.2.0, PCI DSS v4.0.1	ALTO	⊗ No	El cambio se desencadena y es periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
EC2.15	Las subredes de EC2 no deberían asignar automáticamente direcciones IP públicas	AWS Mejores prácticas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1,	MEDIO	⊗ No	El cambio se ha activado
EC2.16	Deben eliminarse las listas de control de acceso a la red no utilizadas	AWS Mejores prácticas de seguridad fundamentales, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1,	BAJA	⊗ No	El cambio se ha activado
EC2.17	Las instancias de EC2 no tienen que ser compatibles con varios ENI	AWS Mejores prácticas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5	BAJA	⊗ No	El cambio se ha activado
EC2.18	Los grupos de seguridad solo deben permitir el tráfico entrante sin restricciones en los puertos autorizados	AWS Mejores prácticas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	ALTO	⊙ Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
EC2.19	Los grupos de seguridad no deben permitir el acceso irrestricto a los puertos de alto riesgo	AWS Mejores prácticas de seguridad fundamentales, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	CRÍTICO	⊗ No	El cambio se desencadena y es periódico
EC2.20	Los dos túneles VPN para una conexión VPN deben estar activos AWS Site-to-Site	AWS Mejores prácticas de seguridad básicas v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	MEDIO	⊗ No	El cambio se ha activado
EC2.21	Las ACL de red no deben permitir la entrada desde la versión 0.0.0. 0/0 al puerto 22 o al puerto 3389	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CIS Foundations Benchmark v1.4.0, AWS AWS Foundational Security Best Practices, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1	MEDIO	⊗ No	El cambio se ha activado
EC2.22	Los grupos de seguridad de EC2 que no se utilicen deben eliminarse		MEDIO	⊗ No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
EC2.23	Las pasarelas de tránsito de EC2 no deberían aceptar automáticamente las solicitudes de adjuntos de VPC	AWS Mejores prácticas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5	ALTO	⊗ No	El cambio se ha activado
EC2.24	No se deben utilizar los tipos de instancias paravirtuales EC2	AWS Mejores prácticas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	El cambio se ha activado
EC2.25	Las plantillas de lanzamiento de EC2 no deben asignar direcciones IP públicas a las interfaces de red	AWS Mejores prácticas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	ALTO	⊗ No	El cambio se ha activado
EC2.28	Los volúmenes de EBS tienen que ser parte de un plan de copia de seguridad	NIST SP 800-53 Rev. 5	BAJA	⊙ Sí	Periódico
EC2.33	La conexión de puerta de enlace de tránsito de EC2 debe estar etiquetada	AWS Estándar de etiquetado de recursos	BAJA	⊙ Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
EC2.34	Las tablas de enrutamiento de las puertas de enlace de tránsito de EC2 deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
EC2.35	Las interfaces de red de EC2 deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
EC2.36	Las puertas de enlace de cliente de EC2 deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
EC2.37	Las direcciones IP elásticas de EC2 deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
EC2.38	Las instancias de EC2 deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
EC2.39	Las puertas de enlace de Internet de EC2 deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
EC2.40	Las puertas de enlace de NAT de EC2 deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
EC2.41	Las ACL de red de EC2 deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
EC2.42	Las tablas de enrutamiento de EC2 deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
EC2.43	Los grupos de seguridad de EC2 deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
EC2.44	Las subredes de EC2 deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
EC2.45	Los volúmenes de EC2 deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
EC2.46	Las VPC de Amazon deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
EC2.47	Los servicios de puntos de conexión de Amazon VPC deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
EC2.48	Los registros de flujo de Amazon VPC deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
EC2.49	Las conexiones de emparejamiento de Amazon VPC deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
EC2.50	Las puertas de enlace de VPN de EC2 deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
EC2.51	Los puntos de conexión de Client VPN de EC2 deben tener habilitado el registro de conexiones de clientes	AWS Mejores prácticas de seguridad fundamentales, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1	BAJA	⊗ No	El cambio se ha activado
EC2.52	Las puertas de enlace de tránsito de EC2 deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	⊙ Sí	El cambio se ha activado
EC2.53	Los grupos de seguridad de EC2 no deben permitir la entrada desde la versión 0.0.0. 0/0 a los puertos de administración de servidores remotos	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, PCI DSS v4.0.1	ALTO	⊗ No	Periódico
EC2.54	Los grupos de seguridad de EC2 no deberían permitir la entrada desde ::/0 a los puertos de administración de servidores remotos	CIS AWS Foundations Benchmark v5.0.0, CIS Foundations Benchmark v3.0.0, PCI DSS v4.0.1 AWS	ALTO	⊗ No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
EC2.55	Las VPC deben estar configuradas con un punto de conexión de interfaz para la API de ECR	AWS Mejores prácticas de seguridad fundamentales, NIST SP 800-53 Rev. 5	MEDIO	Sí	Periódico
EC2.56	Las VPC deben estar configuradas con un punto de conexión de interfaz para el registro de Docker	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5	MEDIO	Sí	Periódico
EC2.57	Las VPC deben estar configuradas con un punto de conexión de interfaz para Systems Manager	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5	MEDIO	Sí	Periódico
EC2.58	Las VPC deben estar configuradas con un punto de conexión de interfaz para los Contactos del Administrador de incidentes de Systems Manager	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5	MEDIO	Sí	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
EC2.60	Las VPC deben estar configuradas con un punto de conexión de interfaz para el Administrador de incidentes de Systems Manager	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5	MEDIO	Sí	Periódico
EC2.170	Las plantillas de lanzamiento de EC2 deben usar el servicio de metadatos de instancias (IMDS) versión 2 (IMDSv2)	AWS Mejores prácticas fundamentales de seguridad, PCI DSS v4.0.1	BAJA	No	El cambio se ha activado
EC2.171	Las conexiones VPN de EC2 deben tener el registro habilitado	AWS Mejores prácticas fundamentales de seguridad, PCI DSS v4.0.1	MEDIO	No	El cambio se ha activado
EC2.172	La configuración de bloqueo de acceso público de VPC para EC2 debe bloquear el tráfico de puerta de enlace de Internet	AWS Mejores prácticas fundamentales de seguridad	MEDIO	Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
EC2.173	Las solicitudes de flota de spot de EC2 con parámetros de lanzamiento deben habilitar el cifrado para los volúmenes de EBS asociados	AWS Mejores prácticas fundamentales de seguridad	MEDIO	No	El cambio se ha activado
EC2.174	Los conjuntos de opciones DHCP de EC2 deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
EC2.175	Las plantillas de lanzamiento de EC2 deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
EC2.176	Las listas de prefijos de EC2 deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
EC2.177	Las sesiones de duplicación de tráfico de EC2 deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
EC2.178	Las sesiones de duplicación de tráfico de EC2 deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
EC2.179	Los destinos de duplicación de tráfico de EC2 deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
EC2.180	Las interfaces de red EC2 deben tener source/destination habilitada la verificación	AWS Mejores prácticas fundamentales de seguridad v1.0.0	MEDIO	No	El cambio se ha activado
EC2.181	Las plantillas de lanzamiento de EC2 deben permitir el cifrado para los volúmenes de EBS asociados	AWS Mejores prácticas fundamentales de seguridad v1.0.0	MEDIO	No	El cambio se ha activado
EC2.182	Las instantáneas de EBS no deben ser de acceso público	AWS Mejores prácticas fundamentales de seguridad	ALTO	No	El cambio se ha activado
EC2.183	Las conexiones VPN de EC2 deben utilizar el protocolo IKEv2	AWS Mejores prácticas de seguridad fundamentales	MEDIO	No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
ECR.1	Los repositorios privados de ECR deben tener configurado el escaneo de imágenes	AWS Mejores prácticas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	ALTO	⊗ No	Periódico
ECR.2	Los repositorios privados de ECR deben tener configurada la inmutabilidad de las etiquetas	AWS Mejores prácticas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	El cambio se ha activado
ECR.3	Los repositorios de ECR deben tener configurada al menos una política de ciclo de vida	AWS Mejores prácticas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	El cambio se ha activado
ECR.4	Los repositorios públicos de ECR deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	⊙ Sí	El cambio se ha activado
ECR.5	Los repositorios de ECR se deben cifrar con AWS KMS keys administradas por el cliente	NIST SP 800-53 Rev. 5	MEDIO	⊙ Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
ECS.2	Los servicios de ECS no deberían tener direcciones IP públicas asignadas automáticamente	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	ALTO	⊗ No	El cambio se ha activado
ECS.3	Las definiciones de tareas de ECS no deben compartir el espacio de nombres del proceso del host	AWS Mejores prácticas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5	ALTO	⊗ No	El cambio se ha activado
ECS.4	Los contenedores ECS deben ejecutarse sin privilegios	AWS Mejores prácticas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5	ALTO	⊗ No	El cambio se ha activado
ECS.5	Los contenedores ECS deben estar limitados a un acceso de solo lectura a los sistemas de archivos raíz	AWS Mejores prácticas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5	ALTO	⊗ No	El cambio se ha activado
ECS.8	Los secretos no deben pasarse como variables de entorno del contenedor	AWS Mejores prácticas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	ALTO	⊗ No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
ECS.9	Las definiciones de tareas de ECS deben tener una configuración de registro	AWS Mejores prácticas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5	ALTO	⊗ No	El cambio se ha activado
ECS.10	Los servicios Fargate de ECS deberían ejecutarse en la última versión de la plataforma Fargate	AWS Mejores prácticas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	⊗ No	El cambio se ha activado
ECS.12	Los clústeres de ECS deben usar Container Insights	AWS Mejores prácticas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	El cambio se ha activado
ECS.13	Los servicios de ECS deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	⊙ Sí	El cambio se ha activado
ECS.14	Los clústeres de ECS deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	⊙ Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
ECS.15	Las definiciones de tareas de ECS deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
ECS.16	Los conjuntos de tareas de ECS no deben asignar automáticamente direcciones IP públicas	AWS Mejores prácticas fundamentales de seguridad, PCI DSS v4.0.1	ALTO	No	El cambio se ha activado
ECS.17	Las definiciones de tareas de ECS no deben utilizar el modo de red de host	NIST SP 800-53 Rev. 5	MEDIO	No	El cambio se ha activado
ECS.18	Las definiciones de tareas de ECS deben utilizar el cifrado en tránsito para los volúmenes de EFS	AWS Mejores prácticas fundamentales de seguridad	MEDIO	No	El cambio se ha activado
ECS.19	Los proveedores de capacidad de ECS deberían tener habilitada la protección de terminación gestionada	AWS Mejores prácticas fundamentales de seguridad	MEDIO	No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
ECS.20	Las definiciones de tareas de ECS deben configurar a los usuarios no root en las definiciones de contenedores de Linux	AWS Mejores prácticas fundamentales de seguridad	MEDIO	⊗ No	El cambio se ha activado
ECS.21	Las definiciones de tareas de ECS deben configurar a los usuarios que no sean administradores en las definiciones de contenedores de Windows	AWS Mejores prácticas fundamentales de seguridad	MEDIO	⊗ No	El cambio se ha activado
EFS.1	Elastic File System debe configurarse para cifrar los datos de los archivos en reposo mediante AWS KMS	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, AWS Foundational Security Best Practices v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
EFS.2	Los volúmenes de Amazon EFS deben estar en los planes de copia de seguridad	AWS Mejores prácticas de seguridad de Foundational v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	Periódico
EFS.3	Los puntos de acceso EFS deben aplicar un directorio raíz	AWS Mejores prácticas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	El cambio se ha activado
EFS.4	Los puntos de acceso EFS deben imponer una identidad de usuario	AWS Mejores prácticas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	⊗ No	El cambio se ha activado
EFS.5	Los puntos de acceso de EFS deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	⊙ Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
EFS.6	Los destinos de montaje de EFS no deben estar asociados a subredes que asignen direcciones IP públicas en el momento del lanzamiento	NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1	MEDIO	⊗ No	Periódico
EFS.7	Los sistemas de archivos de EFS deben tener habilitadas las copias de seguridad automáticas	AWS Mejores prácticas fundamentales de seguridad	MEDIO	⊗ No	El cambio se ha activado
EFS.8	Los sistemas de archivos de EFS deben cifrarse en reposo	CIS AWS Foundations Benchmark v5.0.0, mejores prácticas de seguridad AWS fundamentales	MEDIO	⊙ Sí	El cambio se ha activado
EKS.1	Los puntos de conexión del clúster EKS no deben ser de acceso público	AWS Mejores prácticas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	ALTO	⊗ No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
EKS.2	Los clústeres de EKS deben ejecutarse en una versión compatible de Kubernetes	AWS Mejores prácticas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	ALTO	⊗ No	El cambio se ha activado
EKS.3	Los clústeres de EKS deben usar secretos de Kubernetes cifrados	AWS Mejores prácticas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	⊗ No	Periódico
EKS.6	Los clústeres de EKS deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	⊙ Sí	El cambio se ha activado
EKS.7	Las configuraciones de los proveedores de identidad de EKS deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	⊙ Sí	El cambio se ha activado
EKS.8	Los clústeres de EKS deben tener habilitado el registro de auditoría	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	⊗ No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
EKS.9	Los grupos de nodos de EKS deben ejecutarse en una versión de Kubernetes compatible	AWS Mejores prácticas fundamentales de seguridad	ALTO	⊗ No	El cambio se ha activado
ElastiCache.1	ElastiCache Los clústeres (Redis OSS) deben tener habilitadas las copias de seguridad automáticas	AWS Fundational Security Best Practices v1.0.0, NIST SP 800-53 Rev. 5	ALTO	⊙ Sí	Periódico
ElastiCache.2	ElastiCache los clústeres deben tener habilitadas las actualizaciones automáticas de versiones secundarias	AWS Mejores prácticas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	ALTO	⊗ No	Periódico
ElastiCache.3	ElastiCache los grupos de replicación deben tener habilitada la conmutación por error automática	AWS Mejores prácticas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	Periódico
ElastiCache.4	ElastiCache los grupos de replicación deben estar cifrados en reposo	AWS Mejores prácticas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
ElastiCache.5	ElastiCache los grupos de replicación deben estar cifrados en tránsito	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	⊗ No	Periódico
ElastiCache.6	ElastiCache Los grupos de replicación (Redis OSS) de versiones anteriores deben tener habilitada la autenticación de Redis OSS	AWS Mejores prácticas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	⊗ No	Periódico
ElastiCache.7	ElastiCache los clústeres no deben usar el grupo de subredes predeterminado	AWS Mejores prácticas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5	ALTO	⊗ No	Periódico
ElasticBeanstalk.1	Los entornos de Elastic Beanstalk deberían tener habilitados los informes de estado mejorados	AWS Mejores prácticas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5	BAJA	⊗ No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
ElasticBeanstalk.2	Las actualizaciones de la plataforma gestionada de Elastic Beanstalk deben estar habilitadas	AWS Mejores prácticas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	ALTO	Sí	El cambio se ha activado
ElasticBeanstalk.3	Elastic Beanstalk debe transmitir los registros a CloudWatch	AWS Mejores prácticas de seguridad fundamentales, PCI DSS v4.0.1	ALTO	Sí	El cambio se ha activado
ELB.1	El Equilibrador de carga de aplicación debe configurarse para redirigir todas las solicitudes HTTP a HTTPS	AWS Mejores prácticas fundamentales de seguridad v1.0.0, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5	MEDIO	No	Periódico
ELB.2	Los balanceadores de carga clásicos con oyentes deben usar un certificado proporcionado por SSL/HTTPS AWS Gestor de certificados	AWS Fundational Security Best Practices v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	MEDIO	No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
ELB.3	Los oyentes de Equilibrador de carga clásico deben configurarse con una terminación HTTPS o TLS	AWS Mejores prácticas de seguridad fundamentales, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1	MEDIO	⊗ No	El cambio se ha activado
ELB.4	Equilibrador de carga de aplicación debe configurarse para eliminar los encabezados http	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	⊗ No	El cambio se ha activado
ELB.5	El registro de aplicaciones y de los equilibradores de carga clásicos debe estar habilitado	AWS Mejores prácticas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	El cambio se ha activado
ELB.6	La protección contra la eliminación de un equilibrador de carga de aplicación, de puerta de enlace y de red debe estar habilitada	AWS Mejores prácticas de seguridad fundamentales, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
ELB.7	Los equilibradores de carga clásicos deberían tener habilitado el drenaje de conexiones	AWS Mejores prácticas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5	BAJA	⊗ No	El cambio se ha activado
ELB.8	Los equilibradores de carga clásicos con detectores SSL deben usar una política de seguridad predefinida que tenga una configuración sólida	AWS Mejores prácticas de seguridad fundamentales, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1	MEDIO	⊗ No	El cambio se ha activado
ELB.9	Los equilibradores de carga clásicos deben tener habilitado el equilibrador de carga entre zonas	AWS Mejores prácticas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	El cambio se ha activado
ELB.10	Equilibrador de carga clásico debe abarcar varias zonas de disponibilidad	AWS Mejores prácticas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	⊙ Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
ELB.12	Equilibrador de carga de aplicación debe configurarse con el modo defensivo o de mitigación de desincronización más estricto.	AWS Mejores prácticas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	⊗ No	El cambio se ha activado
ELB.13	Los equilibradores de carga de aplicaciones, redes y puertas de enlace deben abarcar varias zonas de disponibilidad	AWS Mejores prácticas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	⊙ Sí	El cambio se ha activado
ELB.14	Equilibrador de carga clásico debe configurarse con el modo defensivo o con el modo de mitigación de desincronización más estricto.	AWS Mejores prácticas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	⊗ No	El cambio se ha activado
ELB.16	Los balanceadores de carga de aplicaciones deben asociarse a una ACL web de WAF AWS	NIST SP 800-53 Rev. 5	MEDIO	⊗ No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
ELB.17	Los equilibradores de carga de red y de aplicaciones con oyentes deben usar las políticas de seguridad recomendadas	AWS Mejores prácticas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	El cambio se ha activado
ELB.18	Los oyentes de equilibradores de carga de aplicación y de red deben utilizar protocolos seguros para cifrar los datos en tránsito	AWS Mejores prácticas fundamentales de seguridad v1.0.0	MEDIO	⊗ No	El cambio se ha activado
ELB.21	Los grupos objetivo del balanceador de carga de aplicaciones y redes deben usar protocolos de verificación de estado cifrados	AWS Mejores prácticas fundamentales de seguridad v1.0.0	MEDIO	⊗ No	El cambio se ha activado
ELB.22	Los grupos objetivo del ELB deben utilizar protocolos de transporte cifrados	AWS Mejores prácticas fundamentales de seguridad v1.0.0	MEDIO	⊗ No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
EMR.1	Los nodos maestros del clúster de Amazon EMR no deben tener direcciones IP públicas	AWS Mejores prácticas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	ALTO	⊗ No	Periódico
EMR.2	La configuración de bloqueo del acceso público de Amazon EMR debe estar habilitada	AWS Mejores prácticas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	CRÍTICO	⊗ No	Periódico
EMR.3	Las configuraciones de seguridad de Amazon EMR deben estar cifradas en reposo	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	El cambio se ha activado
EMR.4	Las configuraciones de seguridad de Amazon EMR deben estar cifradas en tránsito	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
ES.1	Los dominios de Elasticsearch deben tener habilitado el cifrado en reposo	AWS Mejores prácticas fundamentales de seguridad v1.0.0, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	Periódico
ES.2	Los dominios de Elasticsearch no deben ser de acceso público	AWS Mejores prácticas de seguridad fundamentales, PCI DSS v3.2.1, PCI DSS v4.0.1, NIST SP 800-53 Rev. 5	CRÍTICO	⊗ No	Periódico
ES.3	Los dominios de Elasticsearch deben cifrar los datos enviados entre nodos	AWS Mejores prácticas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1,	MEDIO	⊗ No	El cambio se ha activado
ES.4	El registro de errores de dominio de Elasticsearch en Logs debe estar habilitado CloudWatch	AWS Mejores prácticas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
ES.5	Los dominios de Elasticsearch deben tener habilitado el registro de auditoría	AWS Mejores prácticas de seguridad fundamentales, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	El cambio se ha activado
ES.6	Los dominios de Elasticsearch deben tener al menos tres nodos de datos	AWS Mejores prácticas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	El cambio se ha activado
ES.7	Los dominios de Elasticsearch deben configurarse con al menos tres nodos maestros dedicados	AWS Mejores prácticas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	El cambio se ha activado
ES.8	Las conexiones a dominios de Elasticsearch deben estar cifradas conforme a la política de seguridad TLS más reciente	AWS Mejores prácticas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	⊗ No	El cambio se ha activado
ES.9	Los dominios de Elasticsearch deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	⊙ Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
EventBridge.2	EventBridge Los autobuses de eventos deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
EventBridge.3	EventBridge Los buses de eventos personalizados deben tener adjunta una política basada en los recursos	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	BAJA	No	El cambio se ha activado
EventBridge.4	EventBridge Los terminales globales deben tener habilitada la replicación de eventos	NIST SP 800-53 Rev. 5	MEDIO	No	El cambio se ha activado
FraudDetector.1	Los tipos de entidad de Amazon Fraud Detector deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
FraudDetector.2	Las etiquetas de Amazon Fraud Detector deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
FraudDetector.3	Las salidas de Amazon Fraud Detector deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
FraudDetector.4	Las variables de Amazon Fraud Detector deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
FSx.1	Los sistemas de archivos de FSx para OpenZFS deben configurarse para copiar etiquetas en copias de seguridad y volúmenes	AWS Mejores prácticas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5	BAJA	No	Periódico
FSx.2	Los sistemas de archivos de FSx para Lustre deben configurarse para copiar etiquetas en copias de seguridad	AWS Mejores prácticas de seguridad fundamentales, NIST SP 800-53 Rev. 5	BAJA	No	Periódico
FSx.3	Los sistemas de archivos FSx para OpenZFS deben configurarse para su implementación Multi-AZ	AWS Mejores prácticas fundamentales de seguridad	MEDIO	No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
FSx.4	Los sistemas de archivos FSx para NetApp ONTAP deben configurarse para su implementación Multi-AZ	AWS Mejores prácticas fundamentales de seguridad	MEDIO	Sí	Periódico
FSx.5	Los sistemas de archivos FSx para Windows File Server deben configurarse para su implementación Multi-AZ	AWS Mejores prácticas fundamentales de seguridad	MEDIO	No	Periódico
Glue.1	AWS Glue los trabajos deben etiquetarse	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
Glue.3	AWS Glue las transformaciones del aprendizaje automático deben cifrarse en reposo	AWS Mejores prácticas fundamentales de seguridad	MEDIO	No	El cambio se ha activado
Glue.4	AWS Glue Los trabajos de Spark deben ejecutarse en versiones compatibles de AWS Glue	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5	MEDIO	No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
GlobalAccelerator.1	Los aceleradores de Global Accelerator deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
GuardDuty.1	GuardDuty debe estar habilitado	AWS Mejores prácticas de seguridad fundamentales, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v3.2.1, PCI DSS v4.0.1	ALTO	No	Periódico
GuardDuty.2	GuardDuty los filtros deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
GuardDuty.3	GuardDuty Los IPSets deben etiquetarse	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
GuardDuty.4	GuardDuty los detectores deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
GuardDuty.5	GuardDuty La supervisión del registro de auditoría de EKS debe estar habilitada	AWS Mejores prácticas fundamentales de seguridad	ALTO	⊗ No	Periódico
GuardDuty.6	GuardDuty La protección Lambda debe estar habilitada	AWS Mejores prácticas de seguridad fundamentales, PCI DSS v4.0.1	ALTO	⊗ No	Periódico
GuardDuty.7	GuardDuty La supervisión del tiempo de ejecución de EKS debe estar habilitada	AWS Mejores prácticas básicas de seguridad, PCI DSS v4.0.1	ALTO	⊗ No	Periódico
GuardDuty.8	GuardDuty La protección contra malware para EC2 debe estar habilitada	AWS Mejores prácticas fundamentales de seguridad	ALTO	⊗ No	Periódico
GuardDuty.9	GuardDuty La protección RDS debe estar habilitada	AWS Mejores prácticas fundamentales de seguridad, PCI DSS v4.0.1	ALTO	⊗ No	Periódico
GuardDuty.10	GuardDuty La protección S3 debe estar habilitada	AWS Mejores prácticas fundamentales de seguridad, PCI DSS v4.0.1	ALTO	⊗ No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
GuardDuty.11	GuardDuty La supervisión del tiempo de ejecución debe estar habilitada	AWS Mejores prácticas fundamentales de seguridad	ALTO	⊗ No	Periódico
GuardDuty.12	GuardDuty La supervisión del tiempo de ejecución de ECS debe estar habilitada	AWS Mejores prácticas fundamentales de seguridad	MEDIO	⊗ No	Periódico
GuardDuty.13	GuardDuty La supervisión del tiempo de ejecución de EC2 debe estar habilitada	AWS Mejores prácticas fundamentales de seguridad	MEDIO	⊗ No	Periódico
IAM.1	Las políticas de IAM no deben permitir privilegios administrativos completos “*”	CIS AWS Foundations Benchmark v1.2.0, AWS Foundational Security Best Practices v1.0.0, PCI DSS v3.2.1, CIS AWS Foundations Benchmark v1.4.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	ALTO	⊗ No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
IAM.2	Los usuarios de IAM no deben tener políticas de IAM asociadas	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.2.0, AWS Foundational Security Best Practices v1.0.0, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	BAJA	⊗ No	El cambio se ha activado
IAM.3	Las claves de acceso de los usuarios de IAM deben rotarse cada 90 días o menos	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, CIS AWS AWS Foundations Benchmark v1.2.0, Fundational Security Best Practices, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	⊗ No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
IAM.4	La clave de acceso del usuario raíz de IAM no debería existir	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, AWS Foundational Security Best Practices v1.0.0, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5	CRÍTICO	⊗ No	Periódico
IAM.5	MFA debe estar habilitado para todos los usuarios de IAM que tengan una contraseña de consola	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, CIS AWS AWS Foundations Benchmark v1.2.0, Fundational Security Best Practices, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	⊗ No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
IAM.6	La MFA de hardware debe estar habilitada para el usuario raíz	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, CIS AWS AWS Foundations Benchmark v1.2.0, prácticas recomendadas de seguridad fundamental, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1	CRÍTICO	⊗ No	Periódico
IAM.7	Las políticas de contraseñas para usuarios de IAM deben tener configuraciones seguras	AWS Mejores prácticas de seguridad fundamentales, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1	MEDIO	⊙ Sí	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
IAM.8	Deben eliminarse las credenciales de usuario de IAM que no se utilicen	CIS AWS Foundations Benchmark v1.2.0, prácticas recomendadas de seguridad AWS fundamentales, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v3.2.1, PCI DSS v4.0.1	MEDIO	⊗ No	Periódico
IAM.9	La MFA debe estar habilitada para el usuario raíz	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1	CRÍTICO	⊗ No	Periódico
IAM.10	Las políticas de contraseñas para usuarios de IAM deben tener configuraciones seguras	NIST SP 800-171 Rev. 2, PCI DSS v3.2.1	MEDIO	⊗ No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
IAM.11	Asegurar que la política de contraseñas de IAM requiere al menos una letra mayúscula	CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1	MEDIO	⊗ No	Periódico
IAM.12	Asegurar que la política de contraseñas de IAM requiere al menos una letra minúscula	CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1	MEDIO	⊗ No	Periódico
IAM.13	Asegurar que la política de contraseñas de IAM requiere al menos un símbolo	CIS Foundations Benchmark v1.2.0, NIST SP 800-171 Rev. 2 AWS	MEDIO	⊗ No	Periódico
IAM.14	Asegurar que la política de contraseñas de IAM requiere al menos un número	CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1	MEDIO	⊗ No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
IAM.15	Asegurar que la política de contraseñas de IAM requiere una longitud mínima de 14 o más	CIS AWS Foundations Benchmark v5.0.0, CIS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, CIS Foundations Benchmark v1.2.0, NIST SP 800-171 Rev. 2 AWS AWS	MEDIO	⊗ No	Periódico
IAM.16	Garantizar que la política de contraseñas de IAM impida la reutilización de contraseñas	CIS AWS Foundations Benchmark v5.0.0, CIS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, CIS Foundations Benchmark v1.2.0, NIST SP 800-171 Rev. 2, PCI AWS DSS v4.0.1 AWS	BAJA	⊗ No	Periódico
IAM.17	Asegurar que la política de contraseñas de IAM haga caducar las contraseñas al cabo de 90 días o menos	CIS AWS Foundations Benchmark v1.2.0, PCI DSS v4.0.1	BAJA	⊗ No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
IAM.18	Asegurar que se ha creado un rol de soporte para administrar incidentes con AWS Support	CIS AWS Foundations Benchmark v5.0.0, CIS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 Rev. 2, PCI DSS AWS v4.0.1	BAJA	⊗ No	Periódico
IAM.19	MFA se debe habilitar para todos los usuarios de IAM	NIST SP 800-53 Rev. 5; NIST SP 800-171 Rev. 2; PCI DSS v3.2.1; PCI DSS v4.0.1	MEDIO	⊗ No	Periódico
IAM.21	Las políticas de IAM administrada por los clientes que usted cree no deberían permitir acciones comodín para los servicios	AWS Mejores prácticas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	BAJA	⊗ No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
IAM.22	Deben eliminarse las credenciales de usuario de IAM que no se hayan utilizado durante 45 días	CIS AWS Foundations Benchmark v5.0.0, CIS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, NIST SP 800-171 Rev. 2 AWS	MEDIO	⊗ No	Periódico
IAM.23	Los analizadores del Analizador de acceso de IAM deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	⊙ Sí	El cambio se ha activado
IAM.24	Los roles de IAM deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	⊙ Sí	El cambio se ha activado
IAM.25	Los usuarios de IAM deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	⊙ Sí	El cambio se ha activado
IAM.26	Se deben SSL/TLS eliminar los certificados caducados gestionados en IAM	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0	MEDIO	⊗ No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
IAM.27	Las identidades de IAM no deben tener la política adjunta AWSCloudShellFullAccess	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0	MEDIO	⊗ No	El cambio se ha activado
IAM.28	El analizador de acceso externo del Analizador de acceso de IAM debe estar habilitado	CIS AWS Foundations Benchmark v5.0.0, CIS Foundations Benchmark v3.0.0 AWS	ALTO	⊗ No	Periódico
Inspector.1	El análisis de EC2 en Amazon Inspector debe estar habilitado	AWS Mejores prácticas de seguridad fundamentales, PCI DSS v4.0.1	ALTO	⊗ No	Periódico
Inspector.2	El análisis de ECR en Amazon Inspector debe estar habilitado	AWS Mejores prácticas fundamentales de seguridad, PCI DSS v4.0.1	ALTO	⊗ No	Periódico
Inspector.3	El análisis de código de Lambda en Amazon Inspector debe estar habilitado	AWS Mejores prácticas fundamentales de seguridad, PCI DSS v4.0.1	ALTO	⊗ No	Periódico
Inspector.4	El análisis de estándar de Lambda en Amazon Inspector debe estar habilitado	AWS Mejores prácticas fundamentales de seguridad, PCI DSS v4.0.1	ALTO	⊗ No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
IoT.1	AWS IoT Device Defender los perfiles de seguridad deben etiquetarse	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
IoT.2	AWS IoT Core las acciones de mitigación deben etiquetarse	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
IoT.3	AWS IoT Core las dimensiones deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
IoT.4	AWS IoT Core los autorizadores deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
IoT.5	AWS IoT Core los alias de los roles deben etiquetarse	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
IoT.6	AWS IoT Core las políticas deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
IoTSiteWise.1	AWS IoT SiteWise Los modelos de activos deben etiquetarse	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
IoTSiteWise.2	AWS IoT SiteWise los paneles deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
IoTSiteWise.3	AWS IoT SiteWise Las pasarelas deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
IoTSiteWise.4	AWS IoT SiteWise los portales deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
IoTSiteWise.5	AWS IoT SiteWise los proyectos deben etiquetarse	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
IoTTwinMaker.1	AWS Los trabajos de TwinMaker sincronización de IoT deben etiquetarse	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
IoTTwinMaker.2	AWS Los TwinMaker espacios de trabajo de IoT deben etiquetarse	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
IoTTwinMaker.3	AWS TwinMaker Las escenas de IoT deben etiquetarse	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
IoTTwinMaker.4	AWS TwinMaker Las entidades de IoT deben etiquetarse	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
IoTWireless.1	AWS Los grupos de multidifusión inalámbricos de IoT deben etiquetarse	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
IoTWireless.2	AWS Los perfiles de servicio inalámbrico de IoT deben etiquetarse	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
IoTWireless.3	AWS Las tareas de IoT Wireless (FUOTA) deben etiquetarse	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
IVS.1	Los pares de claves de reproducción de IVS deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
IVS.2	Las configuraciones de grabación de IVS deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
IVS.3	Los canales de IVS deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
Keyspaces.1	Los espacios clave de Amazon Keyspaces deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
Kinesis.1	Las transmisiones de Kinesis deben cifrarse en reposo	AWS Mejores prácticas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	No	El cambio se ha activado
Kinesis.2	Las transmisiones de Kinesis deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
Kinesis.3	Las transmisiones de Kinesis deben tener un periodo adecuado de retención de datos	AWS Mejores prácticas fundamentales de seguridad	MEDIO	Sí	El cambio se ha activado
KMS.1	Las políticas administradas por los clientes de IAM no deberían permitir acciones de descifrado en todas las claves de KMS	AWS Mejores prácticas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	No	El cambio se ha activado
KMS.2	Las entidades principales de IAM no deberían tener políticas integradas de IAM que permitan realizar acciones de descifrado en todas las claves de KMS	AWS Mejores prácticas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	No	El cambio se ha activado
KMS.3	AWS KMS keys no debe borrarse de forma involuntaria	AWS Mejores prácticas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5	CRÍTICO	No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
KMS.4	AWS KMS key la rotación debe estar habilitada	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, CIS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-53 AWS Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1	MEDIO	⊗ No	Periódico
KMS.5	Las claves KMS no deben ser de acceso público	AWS Mejores prácticas de seguridad fundamentales	CRÍTICO	⊗ No	El cambio se ha activado
Lambda.1	Las funciones de Lambda deberían prohibir el acceso público	AWS Mejores prácticas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1	CRÍTICO	⊗ No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
Lambda.2	Las funciones de Lambda deben usar los últimos tiempos de ejecución	AWS Mejores prácticas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	⊗ No	El cambio se ha activado
Lambda.3	Las funciones de Lambda deben estar en una VPC	PCI DSS v3.2.1, NIST SP 800-53 rev. 5	BAJA	⊗ No	El cambio se ha activado
Lambda.5	Las funciones de Lambda de la VPC deben funcionar en varias zonas de disponibilidad	AWS Mejores prácticas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	⊙ Sí	El cambio se ha activado
Lambda.6	Las funciones de Lambda deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	⊙ Sí	El cambio se ha activado
Lambda.7	Las funciones de Lambda deben tener habilitado el rastreo AWS X-Ray activo	NIST SP 800-53 Rev. 5	BAJA	⊗ No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
Macie.1	Amazon Macie debe estar habilitado	AWS Mejores prácticas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	Periódico
Macie.2	La detección automática de datos confidenciales de Macie debe estar habilitada	AWS Mejores prácticas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5	ALTO	⊗ No	Periódico
MSK.1	Los clústeres de MSK deben cifrarse en tránsito entre los nodos de los corredores	AWS Mejores prácticas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	⊗ No	El cambio se ha activado
MSK.2	Los clústeres de MSK deberían tener configurada una supervisión mejorada	NIST SP 800-53 Rev. 5	BAJA	⊗ No	El cambio se ha activado
MSK.3	Los conectores de MSK Connect deben cifrarse en tránsito	AWS Mejores prácticas fundamentales de seguridad, PCI DSS v4.0.1	MEDIO	⊗ No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
MSK.4	Los clústeres de MSK deben tener el acceso público desactivado	AWS Mejores prácticas fundamentales de seguridad	CRÍTICO	⊗ No	El cambio se ha activado
MSK.5	Los conectores de MSK deben tener el registro habilitado	AWS Mejores prácticas fundamentales de seguridad	MEDIO	⊗ No	El cambio se ha activado
MSK.6	Los clústeres de MSK deben desactivar el acceso no autenticado	AWS Mejores prácticas fundamentales de seguridad	MEDIO	⊗ No	El cambio se ha activado
MQ.2	Los corredores de ActiveMQ deben transmitir los registros de auditoría a CloudWatch	AWS Mejores prácticas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	⊗ No	El cambio se ha activado
MQ.4	Los agentes de Amazon MQ deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	⊙ Sí	El cambio se ha activado
MQ.5	Los corredores de ActiveMQ deben usar el modo de implementación active/standby	NIST SP 800-53 Rev. 5	BAJA	⊗ No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
MQ.6	Los corredores de RabbitMQ deberían usar el modo de implementación de clústeres	NIST SP 800-53 Rev. 5	BAJA	⊗ No	El cambio se ha activado
Neptune.1	Los clústeres de bases de datos de Neptune deberían estar cifrados en reposo	AWS Mejores prácticas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	El cambio se ha activado
Neptune.2	Los clústeres de bases de datos de Neptune deben publicar los registros de auditoría en Logs CloudWatch	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	⊗ No	El cambio se ha activado
Neptune.3	Las instantáneas del clúster de base de datos de Neptune no deben ser públicas	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	CRÍTICO	⊗ No	El cambio se ha activado
Neptune.4	Los clústers de Neptune DB deben tener habilitada la protección contra eliminación.	AWS Mejores prácticas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5	BAJA	⊗ No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
Neptune.5	Los clústeres de bases de datos de Neptune deberían tener habilitadas las copias de seguridad automatizadas	AWS Mejores prácticas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	Sí	El cambio se ha activado
Neptune.6	Las instantáneas del clúster de base de datos de Neptune deben cifrarse en reposo	AWS Mejores prácticas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	No	El cambio se ha activado
Neptune.7	Los clústeres de base de datos de Neptune deben tener habilitada la autenticación de bases de datos de IAM	AWS Mejores prácticas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	No	El cambio se ha activado
Neptune.8	Los clústeres de base de datos de Neptune deben configurarse para copiar etiquetas a las instantáneas	AWS Mejores prácticas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5	BAJA	No	El cambio se ha activado
Neptune.9	Los clústeres de base de datos de Neptune se deben implementar en varias zonas de disponibilidad	NIST SP 800-53 Rev. 5	MEDIO	No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
NetworkFirewall.1	Los firewalls de Network Firewall se deben implementar en varias zonas de disponibilidad	NIST SP 800-53 Rev. 5	MEDIO	⊗ No	El cambio se ha activado
NetworkFirewall.2	El registro de Network Firewall debe estar habilitado	AWS Mejores prácticas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	MEDIO	⊗ No	Periódico
NetworkFirewall.3	Las políticas de Network Firewall deben tener asociado al menos un grupo de reglas	AWS Mejores prácticas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	MEDIO	⊗ No	El cambio se ha activado
NetworkFirewall.4	La acción sin estado predeterminada para las políticas de Network Firewall debe ser eliminar o reenviar paquetes completos.	AWS Mejores prácticas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
NetworkFirewall.5	La acción sin estado predeterminada para las políticas de Network Firewall debe ser eliminar o reenviar paquetes fragmentados.	AWS Mejores prácticas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	MEDIO	⊗ No	El cambio se ha activado
NetworkFirewall.6	El grupo de reglas de firewall de redes sin estado no debe estar vacío	AWS Mejores prácticas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	MEDIO	⊗ No	El cambio se ha activado
NetworkFirewall.7	Los firewall de Network Firewall deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	⊙ Sí	El cambio se ha activado
NetworkFirewall.8	Las políticas de firewall de Network Firewall deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	⊙ Sí	El cambio se ha activado
NetworkFirewall.9	Los firewalls de Network Firewall deben tener habilitada la protección de eliminación	AWS Mejores prácticas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
NetworkFirewall.10	Los firewalls de Network Firewall deben tener habilitada la protección contra cambios de subred	AWS Mejores prácticas de seguridad fundamentales, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	El cambio se ha activado
Opensearch.1	OpenSearch los dominios deben tener habilitado el cifrado en reposo	AWS Mejores prácticas básicas de seguridad v1.0.0, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	El cambio se ha activado
Opensearch.2	OpenSearch los dominios no deben ser de acceso público	AWS Mejores prácticas fundamentales de seguridad v1.0.0, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5	CRÍTICO	⊗ No	El cambio se ha activado
Opensearch.3	OpenSearch los dominios deben cifrar los datos enviados entre nodos	AWS Mejores prácticas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	El cambio se ha activado
Opensearch.4	OpenSearch El registro de errores de dominio en Logs debe estar habilitado CloudWatch	AWS Mejores prácticas básicas de seguridad v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
Opensearch.5	OpenSearch los dominios deben tener habilitado el registro de auditoría	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	⊗ No	El cambio se ha activado
Opensearch.6	OpenSearch los dominios deben tener al menos tres nodos de datos	AWS Mejores prácticas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	El cambio se ha activado
Opensearch.7	OpenSearch los dominios deben tener habilitado un control de acceso detallado	AWS Mejores prácticas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5	ALTO	⊗ No	El cambio se ha activado
Opensearch.8	Las conexiones a los OpenSearch dominios deben cifrarse con la política de seguridad TLS más reciente	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	El cambio se ha activado
Opensearch.9	OpenSearch los dominios deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	⊙ Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
Opensearch.10	OpenSearch los dominios deben tener instalada la última actualización de software	AWS Mejores prácticas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	⊗ No	El cambio se ha activado
Opensearch.11	OpenSearch los dominios deben tener al menos tres nodos principales dedicados	NIST SP 800-53 Rev. 5	BAJA	⊗ No	Periódico
PCA.1	AWS Privada CA la autoridad de certificación raíz debe estar deshabilitada	AWS Mejores prácticas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5	BAJA	⊗ No	Periódico
PCA.2	AWS Las autoridades certificadoras privadas de CA deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	⊙ Sí	El cambio se ha activado
RDS.1	Las instantáneas de RDS deben ser privadas	AWS Mejores prácticas de seguridad básicas v1.0.0, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5	CRÍTICO	⊗ No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
RDS.2	Las instancias de base de datos de RDS deben prohibir el acceso público, según lo determine la configuración PubliclyAccessible	CIS AWS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, AWS Foundational Security Best Practices, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1	CRÍTICO	⊗ No	El cambio se ha activado
RDS.3	Las instancias de base de datos de RDS deben tener habilitado el cifrado en reposo	CIS AWS Foundations Benchmark v5.0.0, CIS Foundations Benchmark v3.0.0, CIS Foundations Benchmark v1.4.0, AWS Foundational Security Best Practices v1.0.0, NIST SP 800-53 Rev. 5 AWS AWS	MEDIO	⊗ No	El cambio se ha activado
RDS.4	Las instantáneas del clúster de RDS y las instantáneas de las bases de datos deben cifrarse en reposo	AWS Mejores prácticas de seguridad de Foundational v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
RDS.5	Las instancias de base de datos de RDS deben configurarse con varias zonas de disponibilidad	CIS AWS Foundations Benchmark v5.0.0, AWS Foundational Security Best Practices v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	El cambio se ha activado
RDS.6	Se debe configurar una supervisión mejorada para las instancias de base de datos de RDS	AWS Mejores prácticas de seguridad de Foundational v1.0.0, NIST SP 800-53 Rev. 5	BAJA	⊙ Sí	El cambio se ha activado
RDS.7	Los clústeres RDS deben tener habilitada la protección contra la eliminación	AWS Mejores prácticas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	El cambio se ha activado
RDS.8	Indica si las instancias de base de datos de RDS debe tener la protección contra eliminación habilitada.	AWS Mejores prácticas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5	BAJA	⊗ No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
RDS.9	Las instancias de base de datos de RDS deben publicar los registros en Logs CloudWatch	AWS Mejores prácticas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	⊗ No	El cambio se ha activado
RDS.10	La autenticación de IAM debe configurarse para las instancias de RDS	AWS Mejores prácticas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	El cambio se ha activado
RDS.11	Las instancias RDS deben tener habilitadas las copias de seguridad automáticas	AWS Mejores prácticas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	⊙ Sí	El cambio se ha activado
RDS.12	La autenticación de IAM debe configurarse para los clústeres de RDS	AWS Mejores prácticas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
RDS.13	Deben habilitarse las actualizaciones automáticas entre versiones secundarias de RDS	CIS AWS Foundations Benchmark v5.0.0, CIS Foundations Benchmark v3.0.0, AWS AWS Foundational Security Best Practices, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	ALTO	⊗ No	El cambio se ha activado
RDS.14	Los clústeres de Amazon Aurora deben tener habilitada la característica de búsqueda de datos anteriores	AWS Mejores prácticas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	⊙ Sí	El cambio se ha activado
RDS.15	Los clústeres de bases de datos de RDS deben configurarse para varias zonas de disponibilidad	CIS AWS Foundations Benchmark v5.0.0, AWS Foundational Security Best Practices v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	El cambio se ha activado
RDS.16	Los clústeres de bases de datos de Aurora se deben configurar para copiar etiquetas en instantáneas de bases de datos	AWS Mejores prácticas de seguridad de Foundational v1.0.0, NIST SP 800-53 Rev. 5	BAJA	⊗ No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
RDS.17	Las instancias de base de datos de RDS deben configurarse para copiar etiquetas en las instantáneas	AWS Mejores prácticas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5	BAJA	⊗ No	El cambio se ha activado
RDS.19	Las suscripciones de notificación de eventos de RDS existentes deben configurarse para los eventos críticos del clúster	AWS Mejores prácticas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5	BAJA	⊗ No	El cambio se ha activado
RDS.20	Las suscripciones de notificación de eventos de RDS existentes deben configurarse para los eventos críticos de las instancias de bases de datos	AWS Mejores prácticas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	BAJA	⊗ No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
RDS.21	Se debe configurar una suscripción a las notificaciones de eventos de RDS para los eventos críticos de los grupos de parámetros de bases de datos	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	BAJA	⊗ No	El cambio se ha activado
RDS.22	Se debe configurar una suscripción a las notificaciones de eventos de RDS para los eventos críticos de los grupos de seguridad de bases de datos	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	BAJA	⊗ No	El cambio se ha activado
RDS.23	Las instancias RDS no deben usar el puerto predeterminado de un motor de base de datos	AWS Mejores prácticas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5	BAJA	⊗ No	El cambio se ha activado
RDS.24	Los clústeres de bases de datos de RDS deben usar un nombre de usuario de administrador personalizado	AWS Mejores prácticas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	⊗ No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
RDS.25	Las instancias de bases de datos de RDS deben usar un nombre de usuario de administrador personalizado	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	No	El cambio se ha activado
RDS.26	Las instancias de base de datos de RDS tienen que ser protegidas por planes de copia de seguridad	NIST SP 800-53 Rev. 5	MEDIO	Sí	Periódico
RDS.27	Los clústeres de bases de datos de RDS deben cifrarse en reposo	AWS Mejores prácticas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	No	El cambio se ha activado
RDS.28	Los clústeres de base de datos de RDS deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
RDS.29	Las instantáneas del clúster de base de datos de RDS deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
RDS.30	Las instancias de bases de datos de RDS deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
RDS.31	Los grupos de seguridad de bases de datos de RDS deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
RDS.32	Las instantáneas de bases de datos de RDS deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
RDS.33	Los grupos de subredes de bases de datos de RDS deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
RDS.34	Los clústeres de bases de datos de Aurora MySQL deben publicar los registros de auditoría en Logs CloudWatch	AWS Mejores prácticas básicas de seguridad, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
RDS.35	Los clústeres de bases de datos de RDS deberían tener habilitada la actualización automática de las versiones secundarias	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	⊗ No	El cambio se ha activado
RDS.36	Las instancias de base de datos de RDS para PostgreSQL deben publicar los registros en Logs CloudWatch	AWS Mejores prácticas fundamentales de seguridad, PCI DSS v4.0.1	MEDIO	⊙ Sí	El cambio se ha activado
RDS.37	Los clústeres de bases de datos de Aurora PostgreSQL deben publicar los registros en Logs CloudWatch	AWS Mejores prácticas fundamentales de seguridad, PCI DSS v4.0.1	MEDIO	⊗ No	El cambio se ha activado
RDS.38	Las instancias de base de datos de RDS para PostgreSQL se deben cifrar en tránsito	AWS Mejores prácticas fundamentales de seguridad	MEDIO	⊗ No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
RDS.39	Las instancias de base de datos de RDS para MySQL se deben cifrar en tránsito	AWS Mejores prácticas fundamentales de seguridad	MEDIO	⊗ No	Periódico
RDS.40	Las instancias de base de datos de RDS para SQL Server deben publicar los registros en Logs CloudWatch	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5	MEDIO	⊙ Sí	El cambio se ha activado
RDS.41	Las instancias de base de datos de RDS para SQL Server se deben cifrar en tránsito	AWS Mejores prácticas fundamentales de seguridad	MEDIO	⊗ No	Periódico
RDS.42	Las instancias de base de datos de RDS para MariaDB deben publicar los registros en Logs CloudWatch	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5	MEDIO	⊙ Sí	Periódico
RDS.43	Los proxies de base de datos de RDS deben exigir el cifrado TLS para las conexiones	AWS Mejores prácticas fundamentales de seguridad	MEDIO	⊗ No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
RDS.44	Las instancias de base de datos de RDS para MariaDB se deben cifrar en tránsito	AWS Mejores prácticas fundamentales de seguridad	MEDIO	⊗ No	Periódico
RDS.45	Los clústeres de base de datos de Aurora MySQL deben tener habilitado el registro de auditoría	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	Periódico
RDS.46	Las instancias de bases de datos de RDS no se deben implementar en subredes públicas con rutas hacia puertas de enlace de Internet.	AWS Mejores prácticas fundamentales de seguridad	ALTO	⊗ No	Periódico
RDS.47	Los clústeres de bases de datos de RDS para PostgreSQL se deben configurar para copiar etiquetas en las instantáneas de bases de datos	AWS Mejores prácticas fundamentales de seguridad	BAJA	⊗ No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
RDS.48	Los clústeres de bases de datos de RDS para MySQL se deben configurar para copiar etiquetas en las instantáneas de bases de datos	AWS Mejores prácticas fundamentales de seguridad	BAJA	⊗ No	El cambio se ha activado
RDS.50	Los clústeres de bases de datos de RDS deben tener un período de retención de respaldo suficiente	AWS Mejores prácticas fundamentales de seguridad v1.0.0	MEDIO	⊗ Sí	El cambio se ha activado
RDS.51	Los clústeres globales de RDS deben ejecutarse en una versión compatible de Aurora MySQL	AWS Mejores prácticas fundamentales de seguridad	ALTO	⊗ No	El cambio se ha activado
Redshift.1	Los clústeres de Amazon Redshift deberían prohibir el acceso público	AWS Mejores prácticas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1	CRÍTICO	⊗ No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
Redshift.2	Las conexiones a los clústeres de Amazon Redshift deben cifrarse en tránsito	AWS Mejores prácticas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	⊗ No	El cambio se ha activado
Redshift.3	Los clústeres de Amazon Redshift deben tener habilitadas las instantáneas automáticas	AWS Mejores prácticas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	⊙ Sí	El cambio se ha activado
Redshift.4	Los clústeres de Amazon Redshift deben tener habilitado el registro de auditoría	AWS Mejores prácticas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	⊗ No	El cambio se ha activado
Redshift.6	Amazon Redshift debería tener habilitadas las actualizaciones automáticas a las versiones principales	AWS Mejores prácticas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	El cambio se ha activado
Redshift.7	Los clústeres de Redshift deberían utilizar un enrutamiento de VPC mejorado	AWS Mejores prácticas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
Redshift.8	Los clústeres de Amazon Redshift no deben usar el nombre de usuario de administrador predeterminado	AWS Mejores prácticas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	El cambio se ha activado
Redshift.10	Los clústeres de Redshift deben estar cifrados en reposo	AWS Mejores prácticas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	El cambio se ha activado
Redshift.11	Los clústeres de Redshift deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	⊙ Sí	El cambio se ha activado
Redshift.12	Las suscripciones a notificaciones de eventos de Redshift deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	⊙ Sí	El cambio se ha activado
Redshift.13	Las instantáneas del clúster de Redshift deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	⊙ Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
Redshift.14	Los grupos de subredes del clúster de Redshift deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
Redshift.15	Los grupos de seguridad de Redshift deberían permitir la entrada en el puerto del clúster solo desde orígenes restringidos	AWS Mejores prácticas fundamentales de seguridad, PCI DSS v4.0.1	ALTO	No	Periódico
Redshift.16	Los grupos de subredes del clúster de Redshift deben tener subredes de varias zonas de disponibilidad	NIST SP 800-53 Rev. 5	MEDIO	No	El cambio se ha activado
Redshift.17	Los grupos de parámetros del clúster de Redshift deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
Redshift.18	Los clústeres de Redshift deben tener habilitadas las implementaciones Multi-AZ	AWS Mejores prácticas fundamentales de seguridad	MEDIO	No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
RedshiftServerless.1	Los grupos de trabajo de Amazon Redshift sin servidor deben utilizar enrutamiento de VPC mejorado	AWS Mejores prácticas fundamentales de seguridad	ALTO	⊗ No	Periódico
RedshiftServerless.2	Se debe requerir que las conexiones a los grupos de trabajo de Redshift Serverless utilicen SSL	AWS Mejores prácticas fundamentales de seguridad	MEDIO	⊗ No	Periódico
RedshiftServerless.3	Los grupos de trabajo de Redshift sin servidor deben prohibir el acceso público	AWS Mejores prácticas fundamentales de seguridad	ALTO	⊗ No	Periódico
RedshiftServerless.4	Los espacios de nombres sin servidor de Redshift deben cifrarse y administrarse por el cliente AWS KMS keys	NIST SP 800-53 Rev. 5	MEDIO	⊙ Sí	Periódico
RedshiftServerless.5	Los espacios de nombres de Amazon Redshift no deben usar el nombre de usuario de administrador predeterminado	AWS Mejores prácticas fundamentales de seguridad	MEDIO	⊗ No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
RedshiftServerless.6	Los espacios de nombres sin servidor de Redshift deben exportar los registros a los registros CloudWatch	AWS Mejores prácticas fundamentales de seguridad	MEDIO	⊗ No	Periódico
Route53.1	Las comprobaciones de estado de Route 53 deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	⊙ Sí	El cambio se ha activado
Route53.2	Las zonas alojadas públicas de Route 53 deben registrar las consultas de DNS	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	⊗ No	El cambio se ha activado
S3.1	Los buckets de uso general de S3 deben tener habilitado el bloqueo de acceso público	CIS AWS Foundations Benchmark v5.0.0, CIS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, AWS Foundational Security Best Practices, AWS NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1	MEDIO	⊗ No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
S3.2	Los buckets de uso general de S3 deben bloquear el acceso público de lectura	AWS Mejores prácticas de seguridad fundamentales, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5	CRÍTICO	⊗ No	El cambio se desencadena y es periódico
S3.3	Los buckets de uso general de S3 deben bloquear el acceso público de escritura	AWS Mejores prácticas fundamentales de seguridad, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5	CRÍTICO	⊗ No	El cambio se desencadena y es periódico
S3.5	En las solicitudes de los buckets de uso general de S3, se debe pedir el uso de SSL	CIS AWS Foundations Benchmark v5.0.0, CIS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, AWS AWS Foundational Security Best Practices, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v3.2.1, PCI DSS v4.0.1	MEDIO	⊗ No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
S3.6	Las políticas de bucket de uso general de S3 deberían restringir el acceso a otros Cuentas de AWS	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	ALTO	⊗ No	El cambio se ha activado
S3.7	Los buckets de uso general de S3 deben usar la replicación entre regiones	PCI DSS v3.2.1, NIST SP 800-53 rev. 5	BAJA	⊗ No	El cambio se ha activado
S3.8	Los buckets de uso general de S3 deben bloquear el acceso público	CIS AWS Foundations Benchmark v5.0.0, CIS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, Foundational Security Best Practices, NIST AWS SP 800-53 Rev. 5, AWS PCI DSS v4.0.1	ALTO	⊗ No	El cambio se ha activado
S3.9	Los buckets de uso general de S3 deben tener habilitado el registro de acceso al servidor	AWS Mejores prácticas de seguridad fundamentales, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1	MEDIO	⊗ No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
S3.10	Los buckets de uso general de S3 con el control de versiones habilitado deben tener configuraciones de ciclo de vida	NIST SP 800-53 Rev. 5	MEDIO	⊗ No	El cambio se ha activado
S3.11	Los buckets de uso general de S3 deben tener habilitadas las notificaciones de eventos	NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	MEDIO	⊙ Sí	El cambio se ha activado
S3.12	Las ACL no deben utilizarse para administrar el acceso de los usuarios a los buckets de uso general de S3	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	El cambio se ha activado
S3.13	Los buckets de uso general de S3 deben tener configuraciones de ciclo de vida	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5	BAJA	⊙ Sí	El cambio se ha activado
S3.14	Los buckets de uso general de S3 deben tener habilitado el control de versiones	NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	BAJA	⊗ No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
S3.15	Los buckets de uso general de S3 deben tener habilitado el bloqueo de objetos	NIST SP 800-53 Rev. 5; PCI DSS v4.0.1	MEDIO	Sí	El cambio se ha activado
S3.17	Los cubos de uso general de S3 deben cifrarse cuando están en reposo con AWS KMS keys	NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1	MEDIO	No	El cambio se ha activado
S3.19	Los puntos de acceso de S3 deben tener habilitada la configuración de Bloqueo de acceso público	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	CRÍTICO	No	El cambio se ha activado
S3.20	Los buckets de uso general de S3 deben tener habilitada la eliminación de MFA	CIS AWS Foundations Benchmark v5.0.0, CIS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, NIST SP 800-53 Rev. 5 AWS	BAJA	No	El cambio se ha activado
S3.22	Los buckets de uso general de S3 deben registrar eventos de escritura a nivel de objeto	CIS Foundations Benchmark v5.0.0, CIS AWS Foundations Benchmark v3.0.0, PCI DSS v4.0.1 AWS	MEDIO	No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
S3.23	Los buckets de uso general de S3 deben registrar eventos de lectura a nivel de objeto	CIS AWS Foundations Benchmark v5.0.0, CIS Foundations Benchmark v3.0.0, PCI DSS v4.0.1 AWS	MEDIO	⊗ No	Periódico
S3.24	Los puntos de Multi-Region acceso S3 deben tener habilitada la configuración de bloqueo de acceso público	AWS Mejores prácticas básicas de seguridad, PCI DSS v4.0.1	ALTO	⊗ No	El cambio se ha activado
S3.25	Los buckets de directorio de S3 deben tener configuraciones de ciclo de vida	AWS Mejores prácticas fundamentales de seguridad	BAJA	⊙ Sí	El cambio se ha activado
SageMaker.1	Las instancias de Amazon SageMaker Notebook no deben tener acceso directo a Internet	AWS Mejores prácticas básicas de seguridad, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1	ALTO	⊗ No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
SageMaker.2	SageMaker las instancias de ordenadores portátiles deben lanzarse en una VPC personalizada	AWS Mejores prácticas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5	ALTO	⊗ No	El cambio se ha activado
SageMaker.3	Los usuarios no deben tener acceso root a las instancias de los ordenadores portátiles SageMaker	AWS Mejores prácticas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5	ALTO	⊗ No	El cambio se ha activado
SageMaker.4	SageMaker Las variantes de producción de terminales deben tener un recuento inicial de instancias superior a 1	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	Periódico
SageMaker.5	SageMaker los modelos deben tener habilitado el aislamiento de red	AWS Mejores prácticas fundamentales de seguridad	MEDIO	⊗ No	El cambio se ha activado
SageMaker.6	SageMaker Las configuraciones de imágenes de las aplicaciones deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	⊙ Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
SageMaker.7	SageMaker las imágenes deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
SageMaker.8	SageMaker las instancias de ordenadores portátiles deben ejecutarse en las plataformas compatibles	AWS Mejores prácticas fundamentales de seguridad	MEDIO	No	Periódico
SageMaker.9	SageMaker las definiciones de trabajos de calidad de los datos deben tener habilitado el cifrado del tráfico entre contenedores	AWS Mejores prácticas fundamentales de seguridad v1.0.0	MEDIO	No	El cambio se ha activado
SageMaker.10	SageMaker explicabilidad del modelo: las definiciones de los trabajos deben tener habilitado el cifrado del tráfico entre contenedores	AWS Mejores prácticas fundamentales de seguridad v1.0.0	MEDIO	No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
SageMaker.11	SageMaker las definiciones de trabajos de calidad de los datos deben tener habilitado el aislamiento de red	AWS Mejores prácticas fundamentales de seguridad v1.0.0	MEDIO	⊗ No	El cambio se ha activado
SageMaker.12	SageMaker las definiciones de trabajo basadas en el sesgo de modelo deben tener habilitado el aislamiento de red	AWS Mejores prácticas fundamentales de seguridad v1.0.0	MEDIO	⊗ No	El cambio se ha activado
SageMaker.13	SageMaker las definiciones de trabajos de calidad del modelo deben tener habilitado el cifrado del tráfico entre contenedores	AWS Mejores prácticas fundamentales de seguridad v1.0.0	MEDIO	⊗ No	El cambio se ha activado
SageMaker.14	SageMaker los programas de monitoreo deben tener habilitado el aislamiento de red	AWS Mejores prácticas fundamentales de seguridad v1.0.0	MEDIO	⊗ No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
SageMaker.15	SageMaker las definiciones de trabajos de sesgo de modelo deben tener habilitado el cifrado de tráfico entre contenedores	AWS Mejores prácticas fundamentales de seguridad v1.0.0	MEDIO	⊗ No	El cambio se ha activado
SageMaker.16	SageMaker los modelos deben usar un registro privado en la VPC para los contenedores principales	AWS Mejores prácticas fundamentales de seguridad	MEDIO	⊗ No	El cambio se ha activado
SageMaker.17	SageMaker Las tiendas offline de los grupos de funciones deben cifrarse con claves AWS KMS	AWS Mejores prácticas de seguridad fundamentales	MEDIO	⊗ No	El cambio se ha activado
SageMaker.18	SageMaker Las tiendas en línea de grupos de funciones con almacenamiento estándar deben cifrarse con claves AWS KMS	NIST SP 800-53 Rev. 5	MEDIO	⊗ No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
SageMaker.19	SageMaker los modelos deben usar un registro privado en la VPC para las canalizaciones de inferencia de varios contenedores	AWS Mejores prácticas fundamentales de seguridad	MEDIO	⊗ No	El cambio se ha activado
SageMaker.20	SageMaker explicabilidad del modelo: las definiciones de trabajo deben tener habilitado el aislamiento de red	AWS Mejores prácticas fundamentales de seguridad	ALTO	⊗ No	El cambio se ha activado
SageMaker.21	SageMaker las instancias de ordenadores portátiles deben cifrarse con claves administradas por AWS KMS el cliente	AWS Mejores prácticas fundamentales de seguridad	MEDIO	⊗ No	El cambio se ha activado
SageMaker.22	SageMaker los programas de supervisión deben tener habilitado el cifrado del tráfico entre contenedores	AWS Mejores prácticas fundamentales de seguridad	MEDIO	⊗ No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
SageMaker.23	SageMaker los experimentos de inferencia deben cifrar el volumen de almacenamiento de la instancia con claves administradas por el cliente AWS KMS	AWS Mejores prácticas fundamentales de seguridad	MEDIO	⊗ No	El cambio se ha activado
SageMaker.24	SageMaker los experimentos de inferencia deben tener el almacenamiento de datos cifrado con claves administradas por el cliente AWS KMS	AWS Mejores prácticas fundamentales de seguridad	MEDIO	⊗ No	El cambio se ha activado
SageMaker.25	SageMaker las definiciones de trabajos de calidad del modelo deben tener habilitado el aislamiento de red	AWS Mejores prácticas fundamentales de seguridad	ALTO	⊗ No	El cambio se ha activado
SecretsManager.1	Los secretos de Secrets Manager deberían tener habilitada la rotación automática	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	⊙ Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
SecretsManager.2	Los secretos de Secrets Manager configurados con rotación automática deberían rotar correctamente	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	⊗ No	El cambio se ha activado
SecretsManager.3	Eliminación de secretos no utilizados de Secrets Manager	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5	MEDIO	⊙ Sí	Periódico
SecretsManager.4	Los secretos de Secrets Manager deben rotarse en un número específico de días	AWS Mejores prácticas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	⊙ Sí	Periódico
SecretsManager.5	Los secretos de Secrets Manager deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	⊙ Sí	El cambio se ha activado
ServiceCatalog.1	Las carteras de Service Catalog solo deben compartirse dentro de una organización AWS	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
SES.1	Las listas de contactos de SES deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
SES.2	Los conjuntos de configuración de SES deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
SES.3	Los conjuntos de configuración de SES deben tener TLS habilitado para enviar correos electrónicos	AWS Mejores prácticas fundamentales de seguridad	MEDIO	No	El cambio se ha activado
SNS.1	Los temas de SNS deben cifrarse en reposo mediante AWS KMS	NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	MEDIO	No	El cambio se ha activado
SNS.3	Los temas de SNS deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
SNS.4	Las políticas de acceso a los temas de SNS no deberían permitir el acceso público	AWS Mejores prácticas fundamentales de seguridad	CRÍTICO	No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
SQS.1	Las colas de Amazon SQS deben cifrarse en reposo	AWS Mejores prácticas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	El cambio se ha activado
SQS.2	Las colas de SQS deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	⊙ Sí	El cambio se ha activado
SQS.3	Las políticas de acceso de la cola de SQS no deben permitir el acceso público	AWS Mejores prácticas fundamentales de seguridad	CRÍTICO	⊗ No	El cambio se ha activado
SSM.1	Las instancias EC2 deben gestionarse mediante AWS Systems Manager	AWS Fundational Security Best Practices v1.0.0, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
SSM.2	Las instancias EC2 administradas por Systems Manager deben tener un estado de conformidad de parche de COMPLIANT después de la instalación de un parche	AWS Mejores prácticas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v3.2.1, PCI DSS v4.0.1	ALTO	⊗ No	El cambio se ha activado
SSM.3	Las instancias EC2 administradas por el Administrador de sistemas deben tener un estado de conformidad de asociación de COMPLIANT	AWS Mejores prácticas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1	BAJA	⊗ No	El cambio se ha activado
SSM.4	Los documentos del SSM no deben ser públicos	AWS Mejores prácticas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5	CRÍTICO	⊗ No	Periódico
SSM.5	Los documentos de SSM deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	⊙ Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
SSM.6	La automatización de SSM debe tener CloudWatch habilitado el registro	AWS Mejores prácticas fundamentales de seguridad v1.0.0	MEDIO	⊗ No	Periódico
SSM.7	Los documentos de SSM deben tener habilitada la configuración para bloquear el uso compartido público	AWS Mejores prácticas fundamentales de seguridad v1.0.0	CRÍTICO	⊗ No	Periódico
StepFunctions.1	Step Functions indica que las máquinas deberían tener el registro activado	AWS Mejores prácticas fundamentales de seguridad v1.0.0, PCI DSS v4.0.1	MEDIO	⊙ Sí	El cambio se ha activado
StepFunctions.2	Las actividades de Step Functions deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	⊙ Sí	El cambio se ha activado
Transfer.1	Los flujos de trabajo de Transfer Family deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	⊙ Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
Transfer.2	Los servidores de Transfer Family no deben utilizar el protocolo FTP para la conexión del punto de conexión	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	⊗ No	Periódico
Transfer.3	Los conectores de Transfer Family deben tener el registro habilitado	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	El cambio se ha activado
Transfer.4	Los acuerdos de Transfer Family deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	⊙ Sí	El cambio se ha activado
Transfer.5	Los certificados de Transfer Family deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	⊙ Sí	El cambio se ha activado
Transfer.6	Los conectores de Transfer Family deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	⊙ Sí	El cambio se ha activado
Transfer.7	Los perfiles de Transfer Family deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	⊙ Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
WAF.1	AWS El registro de ACL web global de WAF Classic debe estar habilitado	AWS Mejores prácticas básicas de seguridad, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	⊗ No	Periódico
WAF.2	AWS Las reglas regionales de WAF Classic deben tener al menos una condición	AWS Mejores prácticas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	El cambio se ha activado
WAF.3	AWS Los grupos de reglas regionales de WAF Classic deben tener al menos una regla	AWS Mejores prácticas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	El cambio se ha activado
WAF.4	AWS Las ACL web regionales de WAF Classic deben tener al menos una regla o un grupo de reglas	AWS Mejores prácticas de seguridad básicas v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	El cambio se ha activado
WAF.6	AWS Las reglas globales de WAF Classic deben tener al menos una condición	AWS Mejores prácticas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
WAF.7	AWS Los grupos de reglas globales de WAF Classic deben tener al menos una regla	AWS Mejores prácticas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	El cambio se ha activado
WAF.8	AWS Las ACL web globales de WAF Classic deben tener al menos una regla o un grupo de reglas	AWS Mejores prácticas de seguridad básicas v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	El cambio se ha activado
WAF.10	AWS Las ACL web de WAF deben tener al menos una regla o un grupo de reglas	AWS Mejores prácticas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	⊗ No	El cambio se ha activado
WAF.11	AWS El registro de ACL web de WAF debe estar habilitado	NIST SP 800-53 Rev. 5; PCI DSS v4.0.1	BAJA	⊗ No	Periódico
WAF.12	AWS Las reglas de WAF deben tener CloudWatch habilitadas las métricas	AWS Mejores prácticas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	MEDIO	⊗ No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
WorkSpaces.1	WorkSpaces los volúmenes de usuario deben estar cifrados en reposo	AWS Mejores prácticas fundamentales de seguridad	MEDIO	⊗ No	El cambio se ha activado
WorkSpaces.2	WorkSpaces los volúmenes raíz deben cifrarse en reposo	AWS Mejores prácticas fundamentales de seguridad	MEDIO	⊗ No	El cambio se ha activado

Registro de cambios de los controles del CSPM de Security Hub

El siguiente registro de cambios registra los cambios importantes en los controles CSPM de AWS Security Hub existentes, lo que puede provocar cambios en el estado general de un control y en el estado de cumplimiento de sus hallazgos. Para obtener información sobre cómo el CSPM de Security Hub evalúa el estado de un control, consulte Evaluación del estado de cumplimiento y del estado del control. Los cambios pueden tardar unos días después de su entrada en este registro y afectar a todas las partes Regiones de AWS en las que el control está disponible.

Este registro realiza el seguimiento de los cambios que se han producido desde abril de 2023. Elija un control para revisar información adicional sobre él. Los cambios en el título se mantienen visibles en la descripción detallada del control durante 90 días.

Fecha del cambio	ID y título de control	Descripción del cambio
11 de septiembre de 2026	[RDS.35] Los clústeres de bases de datos de RDS deben tener habilitada la actualización automática de versiones secundarias	Este control comprueba si la actualización automática de versiones secundarias

Fecha del cambio	ID y título de control	Descripción del cambio
		está habilitada para un clúster de base de datos de Amazon RDS. El CSPM de Security Hub amplió el control para evaluar los clústeres de bases de datos de Aurora, que anteriormente no arrojaban ningún resultado.
11 de septiembre de 2026	[S3.5] Los cubos de uso general de S3 deberían requerir que las solicitudes usen TLS	Security Hub CSPM actualizó el título y la descripción de este control para hacer referencia a TLS en lugar de a SSL, ya que SSL está obsoleto.

Fecha del cambio	ID y título de control	Descripción del cambio
27 de agosto de 2026	[RDS.2] Las instancias de base de datos de RDS deben prohibir el acceso público, según lo determine la configuración PubliclyAccessible	Este control comprueba si las instancias de Amazon RDS prohíben el acceso público. Dado que Neptune DB ahora admite puntos de enlace públicos, este control evalúa y genera conclusiones procesables para las instancias de base de datos de Neptune. Security Hub CSPM actualizó la descripción del control para reflejar este cambio.

Fecha del cambio	ID y título de control	Descripción del cambio
12 de agosto de 2026	[EKS.2] Los clústeres de EKS deben ejecutarse en una versión de Kubernetes compatible	Este control comprueba si un clúster de Amazon EKS se ejecuta en una versión de Kubernetes compatible. El CSPM de Security Hub modificó el valor del parámetro de este control de `1.33` a `1.34`. El soporte estándar para la versión 1.33 de Kubernetes en Amazon EKS finalizó el 29 de julio de 2026.

Fecha del cambio	ID y título de control	Descripción del cambio
12 de agosto de 2026	[EKS.9] Los grupos de nodos de EKS deben ejecutarse en una versión de Kubernetes compatible	Este control comprueba si un grupo de nodos de Amazon EKS se ejecuta en una versión de Kubernetes compatible. El CSPM de Security Hub modificó el valor del parámetro de este control de `1.33` a `1.34`. El soporte estándar para la versión 1.33 de Kubernetes en Amazon EKS finalizó el 29 de julio de 2026.

Fecha del cambio	ID y título de control	Descripción del cambio
3 de agosto de 2026	[Lambda.2] Las funciones de Lambda deben usar los tiempos de ejecución compatibles	Lambda.2 comprueba si la configuración de las AWS Lambda funciones para los tiempos de ejecución coincide con los valores esperados establecidos para los tiempos de ejecución compatibles en cada idioma. Security Hub CSPM ahora admite `java17.al2023`, `java11.al2023`, `java8.al2023` como valor de parámetro, y se AWS Lambda ha añadido compatibilidad con este tiempo de ejecución.
3 de agosto de 2026	[EFS.6] Los destinos de montaje de EFS no deben asociarse a subredes que asignan direcciones IP públicas en el momento del lanzamiento	Security Hub CSPM ha eliminado este control del estándar AWS Fundational Security Best Practices (FSBP).

Fecha del cambio	ID y título de control	Descripción del cambio
31 de julio de 2026	[SageMaker.8] las instancias de SageMaker notebooks deben ejecutarse en plataformas compatibles	El CSPM de Security Hub modificó el valor del parámetro de este control de `notebook-al2-v3` a `notebook-al2023-v1` . SageMaker La IA migró las plataform as de instancias de notebooks de Amazon Linux 2 a AL2023.
13 de julio de 2026	[EC2.10] Amazon EC2 debe configurarse para utilizar los puntos de enlace de VPC que se crean para el servicio Amazon EC2	Security Hub CSPM cambió la regla de respaldo de este control, que pasó de estar habilitada para service-vpc-endpoint-enabled a vpc-endpo int-enabled. La regla actualizada reconoce que los nombres de los servicios de FIPS-variant punto final cumplen con los requisitos y genera una búsqueda para las VPC que utilizan puntos de enlace FIPS. `PASSED`

Fecha del cambio	ID y título de control	Descripción del cambio
29 de junio de 2026	[EFS.6] Los destinos de montaje de EFS no deben asociarse a subredes que asignan direcciones IP públicas en el momento del lanzamiento	Security Hub CSPM ha agregado este control a los siguiente s estándares aplicable s: el estándar NIST SP 800-53 Rev. 5, el estándar NIST SP 800-171 Revisión 2 y el estándar PCI DSS v4.0.1. https://docs.aws.amazon.com/securityhub/latest/userguide/pci-standard.html El 30 de julio de 2026, este control se eliminará del estándar Fundation al Security Best Practices (FSBP). AWS

Fecha del cambio	ID y título de control	Descripción del cambio
5 de junio de 2026	[EKS.3] Los clústeres de EKS deben usar secretos de Kubernetes cifrados	Security Hub CSPM notificó que este control se retirará y eliminará de todos los estándares CSPM de Security Hub aplicables a partir del 10 de agosto de 2026. A partir de la versión 1.28 de Kubernetes, los clústeres de Amazon EKS protegen los secretos de Kubernetes con cifrado de sobres de forma predeterminada.
5 de junio de 2026	[IoTEvents.1] IoTEvents.1	Security Hub CSPM notificó que este control se retirará y eliminará de todos los estándares CSPM de Security Hub aplicables a partir del 7 de julio de 2026. AWS anunció el fin del soporte para el servicio AWS IoT Events a partir del 20 de mayo de 2026.

Fecha del cambio	ID y título de control	Descripción del cambio
5 de junio de 2026	[IoTEvents.2] IoTEvents.2	Security Hub CSPM notificó que este control se retirará y eliminará de todos los estándares CSPM de Security Hub aplicables a partir del 7 de julio de 2026. AWS anunció el fin del soporte para el servicio AWS IoT Events a partir del 20 de mayo de 2026.
5 de junio de 2026	[IoTEvents.3] IoTEvents.3	Security Hub CSPM notificó que este control se retirará y eliminará de todos los estándares CSPM de Security Hub aplicables a partir del 7 de julio de 2026. AWS anunció el fin del soporte para el servicio AWS IoT Events a partir del 20 de mayo de 2026.

Fecha del cambio	ID y título de control	Descripción del cambio
5 de junio de 2026	[ECS.1] Las definiciones de tareas de Amazon ECS deben tener modos de red y definiciones de usuario seguros	Security Hub CSPM retiró este control y lo eliminó de todos los estándares aplicable s. Anteriormente, el control comprobab a si una definición de tarea de Amazon ECS activa que utilizaba el modo de red de host también tenía `privileged` definiciones de `user` contenedor.

Fecha del cambio	ID y título de control	Descripción del cambio
5 de junio de 2026	[RDS.18] Las instancias de RDS deben implementarse en una VPC	Security Hub CSPM retiró este control y lo eliminó de todos los estándares aplicable s. Desde que se retiró la EC2-Class ic red de Amazon, las instancias de Amazon Relationa l Database Service (Amazon RDS) ya no se pueden implement ar fuera de una VPC. Anteriormente, el control comprobab a si una instancia de Amazon RDS estaba implementada en una. EC2-VPC

Fecha del cambio	ID y título de control	Descripción del cambio
4 de mayo de 2026	[Lambda.2] Las funciones de Lambda deben usar los tiempos de ejecución compatibles	Lambda.2 comprueba si la configuración de las AWS Lambda funciones para los tiempos de ejecución coincide con los valores esperados establecidos para los tiempos de ejecución compatibles en cada idioma. El CSPM de Security Hub ahora admite `ruby4.0` como parámetro y ya no lo incluye, ya que AWS Lambda ha dejado de estar disponible este tiempo de `nodejs20.x` ejecución.

Fecha del cambio	ID y título de control	Descripción del cambio
27 de abril de 2026	[EC2.4] Las instancias EC2 detenidas deben eliminarse después de un período de tiempo específico	Para simplificar la lógica de evaluación, Security Hub CSPM cambió la regla de respaldo de este control, que pasó de ser ec2-stopped-instance-days-check a una regla CSPM personalizada de Security Hub, denominada ec2-stopped-instance-days-check.

Fecha del cambio	ID y título de control	Descripción del cambio
7 de abril de 2026	[EC2.1] Las instantáneas de Amazon EBS no deben configurarse para que se puedan restaurar públicamente	El CSPM de Security Hub modificó el título y la descripción de este control. El nuevo título y la descripción reflejan con mayor precisión que el control comprueba si las instantáneas de Amazon EBS están configuradas para poder restaurar se públicamente. Anteriormente, el título de este control era: Las instantán eas de Amazon EBS no deberían poder restaurarse públicame nte.

Fecha del cambio	ID y título de control	Descripción del cambio
7 de abril de 2026	[EC2.182] La configuración de bloqueo de acceso público debe estar habilitada para las instantáneas de Amazon EBS	El CSPM de Security Hub modificó el título y la descripción de este control. El nuevo título y la descripción reflejan con mayor precisión que el control comprueba si el acceso público mediante bloqueos a nivel de cuenta está habilitado para las instantáneas de Amazon EBS. Anteriormente, el título de este control era: Las instantán eas de Amazon EBS no deberían ser de acceso público.
6 de abril de 2026	[ELB.17] Los balanceadores de cargas de aplicaciones y redes con oyentes deben usar las políticas de seguridad recomendadas	Security Hub CSPM actualizó el valor del parámetro de este control para reflejar las políticas de seguridad recomenda das.

Fecha del cambio	ID y título de control	Descripción del cambio
3 de abril de 2026	[Cognito.3] Las políticas de contraseñas para los grupos de usuarios de Cognito deben tener configuraciones sólidas	Security Hub CSPM amplió el rango de valores admitidos para el `temporaryPasswordValidity` parámetro de este control. Ahora puede especificar un valor que oscile entre 1 y 365 días. Anteriormente, el intervalo era de 7 a 365 días.
3 de abril de 2026	[EKS.2] Los clústeres de EKS deben ejecutarse en una versión de Kubernetes compatible	Este control comprueba si un clúster de Amazon EKS se ejecuta en una versión de Kubernetes compatible. El CSPM de Security Hub modificó el valor del parámetro de este control de `1.32` a `1.33`. El soporte estándar para la versión 1.32 de Kubernetes en Amazon EKS finalizó el 23 de marzo de 2026.

Fecha del cambio	ID y título de control	Descripción del cambio
3 de abril de 2026	[Lambda.2] Las funciones de Lambda deben usar los tiempos de ejecución compatibles	Lambda.2 el parámetro para los tiempos de ejecución compatibles ya no se incluye porque `ruby3.2` Lambda ha dejado de usar este tiempo de ejecución.
24 de marzo de 2026	[RDS.50] Los clústeres de bases de datos de RDS deben tener un período de retención de copias de seguridad suficiente	Security Hub CSPM actualizó el título del control para reflejar que el control comprueba todos los clústeres de bases de datos de RDS.

Fecha del cambio	ID y título de control	Descripción del cambio
24 de marzo de 2026	[ECS.5] Las definiciones de tareas de ECS deben configurar los contenedores para que se limiten al acceso de solo lectura a los sistemas de archivos raíz	Security Hub CSPM actualizó el título y la descripción del control para reflejar que el control comprueba las definiciones de las tareas de ECS. El CSPM de Security Hub también actualizó el control para que no generara resultados para las definiciones de tareas `runtimePlatform` configuradas para especificar una familia de sistemas operativos. `WINDOWS_SERVER`
9 de marzo de 2026	[AppSync.1] Las cachés de las AWS AppSync API deben cifrarse en reposo	Security Hub CSPM retiró este control y lo eliminó del estándar AWS Fundational Security Best Practices (FSBP). AWS AppSync ahora proporciona el cifrado predeterminado en todas las cachés de API actuales y futuras.

Fecha del cambio	ID y título de control	Descripción del cambio
9 de marzo de 2026	[AppSync.6] Las cachés de las AWS AppSync API deben cifrarse durante el tránsito	Security Hub CSPM retiró este control y lo eliminó del estándar AWS Fundational Security Best Practices (FSBP). AWS AppSync ahora proporciona el cifrado predeterminado en todas las cachés de API actuales y futuras.
4 de marzo de 2026	[ECS.1] Las definiciones de tareas de Amazon ECS deben tener modos de red y definiciones de usuario seguros	Security Hub CSPM retiró este control y lo retiró del estándar AWS Foundational Security Best Practices (FSBP) y del estándar NIST SP 800-53 Rev. 5.
5 de febrero de 2026	[AppSync.1]AWS AppSyncLas cachés de las API deben estar cifradas en reposo	Security Hub CSPM retirará este control y lo eliminará de todos los estándares CSPM de Security Hub aplicables el 9 de marzo de 2026. AWS AppSync proporciona el cifrado predeterminado en todas las cachés de API actuales y futuras.

Fecha del cambio	ID y título de control	Descripción del cambio
5 de febrero de 2026	[AppSync.6]AWS AppSyncLas cachés de las API deben cifrarse en tránsito	Security Hub CSPM retirará este control y lo eliminará de todos los estándare s CSPM de Security Hub aplicables el 9 de marzo de 2026. AWS AppSync proporciona el cifrado predeterm inado en todas las cachés de API actuales y futuras.
16 de enero de 2026	[ECS.1] Las definiciones de tareas de Amazon ECS deben tener modos de red y definiciones de usuario seguros	Security Hub CSPM notificó que este control se retirará y se eliminará de todos los estándares de CSPM de Security Hub aplicables a partir del 16 de febrero de 2026.
12 de enero de 2026	[Redshift.4] Los clústeres de Amazon Redshift deben tener habilitado el registro de auditoría	Security Hub CSPM actualizó este control para eliminar el `loggingEnabled` parámetro.

Fecha del cambio	ID y título de control	Descripción del cambio
12 de enero de 2026	[MQ.3] Los agentes de Amazon MQ deben tener habilitada la actualización automática de versiones secundarias	Security Hub CSPM retiró el control y lo eliminó de todos los estándares aplicable s. Security Hub CSPM retiró el control debido a los requisitos de Amazon MQ para actualizar automátic amente las versiones secundarias. Anteriormente, el control se aplicaba al estándar AWS Foundational Security Best Practices (FSBP), al estándar NIST SP 800-53 Rev. 5 y al estándar PCI DSS v4.0.1. https://docs.aws.amazon.com/securityhub/latest/userguide/pci-standard.html

Fecha del cambio	ID y título de control	Descripción del cambio
12 de enero de 2026	[Lambda.2] Las funciones de Lambda deben usar los tiempos de ejecución compatibles	Este control comprueba si la configuración de tiempo de ejecución de una AWS Lambda función coincide con los valores esperados para los tiempos de ejecución admitidos en cada idioma. El CSPM de Security Hub ahora admite este control `dotnet10` como valor de parámetro . AWS Lambda se agregó soporte para este tiempo de ejecución.

Fecha del cambio	ID y título de control	Descripción del cambio
15 de diciembre de 2025	[Lambda.2] Las funciones de Lambda deben usar los tiempos de ejecución compatibles	Este control comprueba si la configuración de tiempo de ejecución de una AWS Lambda función coincide con los valores esperados para los tiempos de ejecución admitidos en cada idioma. Security Hub CSPM ya no admite este control `python3.9` como valor de parámetro. AWS Lambda ya no admite este tiempo de ejecución.

Fecha del cambio	ID y título de control	Descripción del cambio
12 de diciembre de 2025	[EKS.2] Los clústeres de EKS deben ejecutarse en una versión de Kubernetes compatible	Este control comprueba si un clúster de Amazon EKS se ejecuta en una versión de Kubernetes compatible. El CSPM de Security Hub modificó el valor del parámetro de este control de `1.31` a `1.32`. El soporte estándar para la versión 1.31 de Kubernetes en Amazon EKS finalizó el 26 de noviembre de 2025.

Fecha del cambio	ID y título de control	Descripción del cambio
21 de noviembre de 2025	[Lambda.2] Las funciones de Lambda deben usar los tiempos de ejecución compatibles	Este control comprueba si la configuración de tiempo de ejecución de una AWS Lambda función coincide con los valores esperados para los tiempos de ejecución admitidos en cada idioma. El CSPM de Security Hub ahora admite `nodejs24.x` y `python3.14` como valores de parámetros para este control. AWS Lambda se agregó soporte para estos tiempos de ejecución.

Fecha del cambio	ID y título de control	Descripción del cambio
14 de noviembre de 2025	[EC2.15] Las subredes de Amazon EC2 no deben asignar automáticamente direcciones IP públicas	Security Hub CSPM actualizó la descripción y la justificación de este control. Anteriormente, el control solo comprobaba la asignación automática de IP públicas de IPv4 en las subredes de Amazon VPC mediante la marca. `MapPublicIpOnLaunch` Este control ahora comprueba la asignación automática de IP públicas de IPv4 e IPv6. La descripción y la justificación del control se han actualizado para reflejar estos cambios.

Fecha del cambio	ID y título de control	Descripción del cambio
14 de noviembre de 2025	[Lambda.2] Las funciones de Lambda deben usar los tiempos de ejecución compatibles	Este control comprueba si la configuración de tiempo de ejecución de una AWS Lambda función coincide con los valores esperados para los tiempos de ejecución admitidos en cada idioma. El CSPM de Security Hub ahora admite `java25` como valor de parámetro para este control. AWS Lambda ag regó compatibilidad para este tiempo de ejecución.
13 de noviembre de 2025	[SNS.4] Las políticas de acceso a los temas de SNS no deberían permitir el acceso público	Security Hub CSPM cambió la gravedad de este control de a`HIGH`. `CRITICAL` Permitir el acceso público a los temas de Amazon SNS representa un riesgo de seguridad importante.

Fecha del cambio	ID y título de control	Descripción del cambio
13 de noviembre de 2025	[SQS.3] Las políticas de acceso a las colas de SQS no deberían permitir el acceso público	Security Hub CSPM cambió la gravedad de este control de a`HIGH`. `CRITICAL` Permitir el acceso público a las colas de Amazon SQS representa un riesgo de seguridad importante.
13 de noviembre de 2025	[GuardDuty.7] La monitorización del tiempo de ejecución de GuardDuty EKS debe estar habilitada	Security Hub CSPM cambió la gravedad de este control de a`MEDIUM`. `HIGH` Este tipo de supervisión del tiempo de ejecución proporciona una detección de amenazas mejorada para los recursos de Amazon EKS.

Fecha del cambio	ID y título de control	Descripción del cambio
13 de noviembre de 2025	[MQ.3] Los agentes de Amazon MQ deben tener habilitada la actualización automática de versiones secundarias	Security Hub CSPM cambió la severidad de este control de a. `LOW` `MEDIUM` Las actualizaciones menores de la versión incluyen los parches de seguridad necesarios para mantener la seguridad de los agentes de Amazon MQ.
13 de noviembre de 2025	[Opensearch.10] OpenSearch los dominios deben tener instalada la última actualización de software	Security Hub CSPM cambió la gravedad de este control de a`LOW`. `MEDIUM` Las actualizaciones de software incluyen parches de seguridad que son necesario s para mantener la seguridad del OpenSearch dominio.

Fecha del cambio	ID y título de control	Descripción del cambio
13 de noviembre de 2025	[RDS.7] Los clústeres de RDS deben tener habilitada la protección contra eliminaciones	Security Hub CSPM cambió la gravedad de este control de a`LOW`. `MEDIUM` La protección contra la eliminación ayuda a evitar la eliminaci ón accidental de las bases de datos de Amazon RDS y la eliminación de bases de datos de RDS por parte de entidades no autorizadas.
13 de noviembre de 2025	[CloudTrail.5] los CloudTrail senderos deben estar integrados con Amazon CloudWatch Logs	Security Hub CSPM cambió la gravedad de este control de a`LOW`. `MEDIUM` AWS CloudTrail Los datos de registro de Amazon CloudWatch Logs se pueden usar para actividades de auditoría, alarmas y otras operaciones de seguridad important es.

Fecha del cambio	ID y título de control	Descripción del cambio
13 de noviembre de 2025	[ServiceCatalog.1] Las carteras de Service Catalog deben compartirse dentro de unAWSsolo una organización	Security Hub CSPM cambió la gravedad de este control de a`HIGH`. `MEDIUM` Compartir AWS Service Catalog carteras con cuentas específicas puede ser intencional y no necesariamente indica que una cartera sea de acceso público.
13 de noviembre de 2025	[CloudFront.7] CloudFront las distribuciones deben usar certificados personalizados SSL/TLS	Security Hub CSPM cambió la gravedad de este control de a`MEDIUM`. `LOW` Los nombres `cloudfront.net` de dominio predeterminados para CloudFront las distribuciones de Amazon se generan de forma aleatoria, lo que reduce el riesgo de seguridad.

Fecha del cambio	ID y título de control	Descripción del cambio
13 de noviembre de 2025	[ELB.7] Los balanceadores de carga clásicos deben tener activado el drenaje de conexiones	Security Hub CSPM cambió la gravedad de este control de a`MEDIUM`. `LOW` En las implementaciones de varias instancias, otras instancias en buen estado pueden gestionar las sesiones de usuario cuando una instancia finaliza sin agotar la conexión, lo que reduce el impacto operativo y los riesgos de disponibilidad.
13 de noviembre de 2025	[RedshiftServerless.5] Los espacios de nombres Redshift Serverless no deben usar el nombre de usuario de administrador predeterminado	Security Hub CSPM actualizó este control para eliminar el parámetro opcional`validAdminUserNames`.
23 de octubre de 2025	[ElastiCache.1] ElastiCache (Redis OSS) los clústeres deben tener habilitadas las copias de seguridad automáticas	El CSPM de Security Hub revirtió los cambios realizados al título, la descripción y la regla de este control el 14 de octubre de 2025.

Fecha del cambio	ID y título de control	Descripción del cambio
22 de octubre de 2025	[CloudFront.1] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado	Security Hub CSPM actualizó este control para que no generara resultados para CloudFront las distribuciones de Amazon que utilizan orígenes personali zados.
16 de octubre de 2025	[CloudFront.15] CloudFront las distribuciones deben usar la política de seguridad TLS recomendada	Este control comprueba si una CloudFront distribuc ión de Amazon está configurada para usar una política de seguridad TLS recomendada. El CSPM de Security Hub ahora admite `TLSv1.2_2025` y `TLSv1.3_2025` como valores de parámetros para este control.

Fecha del cambio	ID y título de control	Descripción del cambio
14 de octubre de 2025	[ElastiCache.1] ElastiCache (Redis OSS) los clústeres deben tener habilitadas las copias de seguridad automáticas	El CSPM de Security Hub modificó el título, la descripción y la regla de este control. Anteriormente, este control comprobaba los clústeres de Redis OSS y todos los grupos de replicación, con la regla elasticache-redis-cluster-automatic-backup-check. El título del control era: ElastiCache (Redis OSS) los clústeres deben tener habilitadas las copias de seguridad automáticas. Este control ahora comprueba también los clústeres Valkey, además de los clústeres Redis OSS y todos los grupos de replicación, con la regla elasticache-automatic-backup-check-enabled. El nuevo título y la nueva descripción reflejan que el control

Fecha del cambio	ID y título de control	Descripción del cambio
		evalúa ambos tipos de clústeres.
5 de octubre de 2025	[Opensearch.10] OpenSearch los dominios deben tener instalada la última actualización de software	La regla de este control se actualizó para detectar también si un `PASSED` dominio de Amazon OpenSearch Service no tiene actualizaciones de software disponibles y el estado de la actualización no es apto. Anteriormente, este control solo generaba un `PASSED` resultado si un OpenSearch dominio no tenía actualizaciones de software disponibles y el estado de la actualización estaba completo.

Fecha del cambio	ID y título de control	Descripción del cambio
24 de septiembre de 2025	[Redshift.9] Los clústeres de Redshift no deben usar el nombre de base de datos predeterm inado [RedshiftServerless.7] Los espacios de nombres sin servidor de Redshift no deben usar el nombre de base de datos predeterm inado	El CSPM de Security Hub retiró estos controles y los eliminó de todos los estándares aplicables. El CSPM de Security Hub retiró estos controles debido a limitaciones inherente s de Amazon Redshift que impedían una remediación efectiva de los resultados `FAILED` generados por estos controles. Anteriormente, los controles se aplicaban al estándar Prácticas recomendadas de seguridad básica de AWS (FSBP), así como al estándar NIST SP 800-53 Rev. 5. El Redshift. 9 control también se aplicó al estándar de administración de servicios. AWS Control Tower

Fecha del cambio	ID y título de control	Descripción del cambio
9 de septiembre de 2025	[Lambda.2] Las funciones de Lambda deben usar los tiempos de ejecución compatibles	Este control comprueba si la configuración de tiempo de ejecución de una AWS Lambda función coincide con los valores esperados para los tiempos de ejecución admitidos en cada idioma. Security Hub CSPM ya no admite este control `nodejs18.x` como valor de parámetro. AWS Lambda ya no admite Node.js 18 tiempos de ejecución.

Fecha del cambio	ID y título de control	Descripción del cambio
13 de agosto de 2025	SageMaker Los modelos [SageMaker.5] deben tener habilitado el aislamiento de red	El CSPM de Security Hub modificó el título y la descripción de este control. El nuevo título y la descripción reflejan con mayor precisión que el control comprueba la configuración del `EnableNetworkIsolation` parámetro de los modelos alojados en Amazon SageMaker AI. Anteriormente, el título de este control era: SageMaker models should block inbound traffic.

Fecha del cambio	ID y título de control	Descripción del cambio
13 de agosto de 2025	[EFS.6] Los destinos de montaje de EFS no deben asociarse a subredes que asignan direcciones IP públicas en el momento del lanzamiento	El CSPM de Security Hub modificó el título y la descripci ón de este control. El nuevo título y la nueva descripción describen con mayor exactitud el alcance y la naturaleza de la comprobación que realiza este control. Anteriormente, el título de este control era: EFS mount targets should not be associated with a public subnet.

Fecha del cambio	ID y título de control	Descripción del cambio
24 de julio de 2025	[EKS.2] Los clústeres de EKS deben ejecutarse en una versión de Kubernetes compatible	Este control comprueba si un clúster de Amazon EKS se ejecuta en una versión de Kubernetes compatible. El CSPM de Security Hub modificó el valor del parámetro de este control de `1.30` a `1.31`. La compatibilidad estándar con la versión 1.30 de Kubernetes en Amazon EKS finalizó el 23 de julio de 2025.

Fecha del cambio	ID y título de control	Descripción del cambio
23 de julio de 2025	[EC2.173] Las solicitudes de EC2 Spot Fleet con parámetros de lanzamiento deberían permitir el cifrado de los volúmenes de EBS adjuntos	El CSPM de Security Hub modificó el título de este control. El nuevo título refleja con mayor precisión que el control solo comprueba las solicitudes de la flota de spot de Amazon EC2 que especifican parámetros de lanzamiento. Anteriormente, el título de este control era: EC2 Spot Fleet requests should enable encryption for attached EBS volumes.
30 de junio de 2025	[IAM.13] Asegúrese de que la política de contraseñas de IAM requiera al menos un símbolo	El CSPM de Security Hub eliminó este control del estándar PCI DSS v4.0.1. PCI DSS v4.0.1 no exige explícitamente el uso de símbolos en las contraseñas.

Fecha del cambio	ID y título de control	Descripción del cambio
30 de junio de 2025	[IAM.17] Asegúrese de que la política de contraseñas de IAM haga caducar las contraseñas en un plazo de 90 días o menos	El CSPM de Security Hub eliminó este control del estándar NIST SP 800-171 Revisión 2. NIST SP 800-171 Revisión 2 no exige explícita mente periodos de expiración de contraseñas de 90 días o menos.
30 de junio de 2025	[RDS.16] Los clústeres de bases de datos de Aurora deben configurarse para copiar las etiquetas a las instantáneas de bases de datos	El CSPM de Security Hub modificó el título de este control. El nuevo título refleja con mayor precisión que el control solo comprueba los clústeres de bases de datos Amazon Aurora. Anteriorm ente, el título de este control era: RDS DB clusters should be configured to copy tags to snapshots.

Fecha del cambio	ID y título de control	Descripción del cambio
30 de junio de 2025	[SageMaker.8] las instancias de SageMaker notebooks deben ejecutarse en plataformas compatibles	Este control comprueba si una instancia de bloc de notas de Amazon SageMaker AI está configurada para ejecutarse en una plataforma compatible, en función del identificador de plataforma especificado para la instancia de bloc de notas. El CSPM de Security Hub dejó de admitir `notebook-al2-v1` y `notebook-al2-v2` como valores de parámetro para este control. Las instancias de bloc de notas que se ejecutan en estas plataformas llegaron al fin de su periodo de soporte el 30 de junio de 2025.

Fecha del cambio	ID y título de control	Descripción del cambio
30 de mayo de 2025	[IAM.10] Las políticas de contraseñas para los usuarios de IAM deben tener configuraciones sólidas	El CSPM de Security Hub eliminó este control del estándar PCI DSS v4.0.1. Este control verifica si las políticas de contraseñas de las cuentas de usuario de IAM cumplen los requisitos mínimos, incluida una longitud mínima de 7 caracteres. La versión 4.0.1 de PCI DSS ahora requiere que las contraseñas tengan un mínimo de 8 caracteres. Este control aún se aplica al estándar PCI DSS v3.2.1, el cual tiene requisitos distintos para contraseñas. Para evaluar las políticas de contraseñas de las cuentas en función de los requisitos de la versión 4.0.1 de PCI DSS, puede usar el control. IAM.7 Este control exige que las contraseñas tengan un mínimo

Fecha del cambio	ID y título de control	Descripción del cambio
		de 8 caracteres. También admite valores personali zados para la longitud de las contraseñas y otros parámetros. El IAM.7 control forma parte del estándar PCI DSS v4.0.1 de Security Hub CSPM.
8 de mayo de 2025	[RDS.46] Las instancias de bases de datos de RDS no deben implementarse en subredes públicas con rutas a pasarelas de Internet	Security Hub CSPM anuló por completo la versión del control. RDS.46 Regiones de AWS Anteriorm ente, este control era compatible con el estándar AWS Fundational Security Best Practices (FSBP).

Fecha del cambio	ID y título de control	Descripción del cambio
7 de abril de 2025	[ELB.17] Los balanceadores de cargas de aplicaciones y redes con oyentes deben usar las políticas de seguridad recomendadas	Este control comprueba si el oyente HTTPS de un equilibrador de carga de aplicación o el oyente TLS de un equilibrador de carga de red están configurados para cifrar los datos en tránsito mediante una política de seguridad recomendada. El CSPM de Security Hub ahora admite dos valores de parámetro adicionales para este control: `ELBSecurityPolicy-TLS13-1-2-Res-2021-06` y `ELBSecurityPolicy-TLS13-1-2-Res-FIPS-2023-04` .

Fecha del cambio	ID y título de control	Descripción del cambio
27 de marzo de 2025	[Lambda.2] Las funciones de Lambda deben usar los tiempos de ejecución compatibles	Este control comprueba si la configuración del tiempo de ejecución para una función de AWS Lambda co incide con los valores esperados para los tiempos de ejecución compatibles en cada lenguaje. El CSPM de Security Hub ahora admite este control `ruby3.4` como valor de parámetro. AWS Lambda se agregó soporte para este tiempo de ejecución.

Fecha del cambio	ID y título de control	Descripción del cambio
26 de marzo de 2025	[EKS.2] Los clústeres de EKS deben ejecutarse en una versión de Kubernetes compatible	Este control comprueba si un clúster de Amazon Elastic Kubernetes Service (Amazon EKS) se ejecuta en una versión de Kubernetes compatible. Para el parámetro `oldestVersionSupported`, el CSPM de Security Hub cambió el valor de `1.29` a `1.30`. `1.30` es ahora la versión más antigua de Kubernetes que aún es compatible.

Fecha del cambio	ID y título de control	Descripción del cambio
10 de marzo de 2025	[Lambda.2] Las funciones de Lambda deben usar los tiempos de ejecución compatibles	Este control comprueba si la configuración del tiempo de ejecución para una función de AWS Lambda co incide con los valores esperados para los tiempos de ejecución compatibles en cada lenguaje. Security Hub CSPM ya no admite `dotnet6` y `python3.8` como valores de parámetro s para este control. AWS Lambda ya no admite estos tiempos de ejecución.

Fecha del cambio	ID y título de control	Descripción del cambio
7 de marzo de 2025	[RDS.18] Las instancias de RDS deben implementarse en una VPC	El CSPM de Security Hub eliminó este control del estándar AWS fundamental de mejores prácticas de seguridad y verificó automáticamente los requisitos del SP 800-53 Rev. 5 del NIST. Desde que se retiró la EC2-Class ic red de Amazon, las instancias de Amazon Relationa l Database Service (Amazon RDS) ya no se pueden implement ar fuera de una VPC.
10 de enero de 2025	[Glue.2] Los trabajos de AWS Glue deben tener habilitado el registro	El CSPM de Security Hub retiró este control y lo eliminó de todos los estándares.
20 de diciembre de 2024	EC2.61 a través EC2.169	Security Hub CSPM anuló la versión de los controles directos EC2.61 . EC2.169

Fecha del cambio	ID y título de control	Descripción del cambio
12 de diciembre de 2024	[RDS.23] Las instancias de RDS no deben usar el puerto predeterminado de un motor de base de datos	RDS.23 comprueba si un clúster o una instancia de Amazon Relational Database Service (Amazon RDS) utiliza un puerto distinto del puerto predeterminado del motor de base de datos. Hemos actualizado el control para que la AWS Config regla subyacente arroje un resultado de `NOT_APPLICABLE` para las instancias de RDS que forman parte de un clúster.

Fecha del cambio	ID y título de control	Descripción del cambio
2 de diciembre de 2024	[Lambda.2] Las funciones de Lambda deben usar los tiempos de ejecución compatibles	Lambda.2 comprueba si la configuración de las AWS Lambda funciones para los tiempos de ejecución coincide con los valores esperados establecidos para los tiempos de ejecución compatibles en cada idioma. El CSPM de Security Hub ahora admite `nodejs22.x` como parámetro.
26 de noviembre de 2024	[EKS.2] Los clústeres de EKS deben ejecutarse en una versión de Kubernetes compatible	Este control comprueba si un clúster de Amazon Elastic Kubernete s Service (Amazon EKS) se ejecuta en una versión de Kubernetes compatibl e. `1.29` es ahora la versión más antigua compatible.

Fecha del cambio	ID y título de control	Descripción del cambio
20 de noviembre de 2024	[Config.1] AWS Config deben estar habilitados y usar la función vinculada al servicio para el registro de recursos	Config.1 comprueba si AWS Config está habilitada, usa la función vinculada al servicio y registra los recursos de los controles habilitados. El CSPM de Security Hub aumentó la gravedad de este control de `MEDIUM` a `CRITICAL`. El CSPM de Security Hub también agregó nuevos códigos de estado y motivos de estado para los hallazgos fallidos. Config.1 Estos cambios reflejan la importancia de los controles CSPM de Security Hub Config.1 para el funcionamiento. Si tiene AWS Config deshabilitada la grabación de recursos, puede recibir resultados de control inexactos. Para recibir una `PASSED` búsqueda Config.1, active el

Fecha del cambio	ID y título de control	Descripción del cambio
		registro de recursos para los recursos que corresponden a los controles CSPM de Security Hub habilitados y deshabilite los controles que no sean obligatorios en su organización. Para obtener instrucciones sobre la configuración del AWS Config CSPM de Security Hub, consulte. Activación y configuración AWS Config para Security Hub CSPM Para ver la lista de los controles del CSPM de Security Hub y sus recursos correspondientes, consulte ObligatorioAWS Configrecursos para hallazgos de control.

Fecha del cambio	ID y título de control	Descripción del cambio
12 de noviembre de 2024	[Lambda.2] Las funciones de Lambda deben usar los tiempos de ejecución compatibles	Lambda.2 comprueba si la configuración de las AWS Lambda funciones para los tiempos de ejecución coincide con los valores esperados establecidos para los tiempos de ejecución compatibles en cada idioma. El CSPM de Security Hub ahora admite `python3.13` como parámetro.
11 de octubre de 2024	ElastiCache controles	Se han modificado los títulos de los controles para ElastiCac he.3 ElastiCache.4 ElastiCache.5,, y ElastiCache.7. Los títulos ya no mencionan Redis OSS porque los controles también se aplican a ElastiCache Valkey.

Fecha del cambio	ID y título de control	Descripción del cambio
27 de septiembre de 2024	[ELB.4] El balanceador de carga de aplicaciones debe configurarse para eliminar los encabezados http no válidos	Se cambió el título del control de El equilibrador de carga de aplicación debe configurarse para eliminar los encabezados http a El equilibrador de carga de aplicación debe configurarse para eliminar los encabezados http no válidos.
19 de agosto de 2024	Cambios en el título y en los controles DMS.12 ElastiCache	Se han modificado los títulos de los controles DMS.12 de principio ElastiCache.1 a fin ElastiCache.7. Hemos cambiado estos títulos para reflejar un cambio de nombre en el servicio Amazon ElastiCache (Redis OSS).

Fecha del cambio	ID y título de control	Descripción del cambio
15 de agosto de 2024	[Config.1] AWS Config deben estar habilitados y usar la función vinculada al servicio para el registro de recursos	Config.1 comprueba si AWS Config está habilitado, usa el rol vinculado al servicio y registra los recursos de los controles habilitados. El CSPM de Security Hub agregó un parámetro personalizado para el control llamado `includeConfigServiceLinkedRoleCheck` . Si establece este parámetro en `false`, puede optar por no comprobar si AWS Config utiliza el rol vinculado al servicio.
31 de julio de 2024	[IoT.1]AWS IoT Device Defenderlos perfiles de seguridad deben estar etiquetados	Se cambió el título del control de Los perfiles de seguridad de AWS IoT Core deben estar etiquetados a Los perfiles de seguridad de AWS IoT Device Defender deben estar etiquetados.

Fecha del cambio	ID y título de control	Descripción del cambio
29 de julio de 2024	[Lambda.2] Las funciones de Lambda deben usar los tiempos de ejecución compatibles	Lambda.2 comprueba si la configuración de las AWS Lambda funciones para los tiempos de ejecución coincide con los valores esperados establecidos para los tiempos de ejecución admitidos en cada idioma. El CSPM de Security Hub dejó de admitir `nodejs16.x` como parámetro.
29 de julio de 2024	[EKS.2] Los clústeres de EKS deben ejecutarse en una versión de Kubernetes compatible	Este control comprueba si un clúster de Amazon Elastic Kubernete s Service (Amazon EKS) se ejecuta en una versión de Kubernetes compatible. La versión compatible más antigua es `1.28`.

Fecha del cambio	ID y título de control	Descripción del cambio
25 de junio de 2024	[Config.1] AWS Config deben estar habilitados y usar la función vinculada al servicio para el registro de recursos	Este control comprueba si AWS Config está habilitado, usa el rol vinculado al servicio y registra los recursos de los controles habilitados. El CSPM de Security Hub actualizó el título del control para reflejar lo que el control evalúa.
14 de junio de 2024	[RDS.34] Los clústeres de bases de datos Aurora MySQL deben publicar los registros de auditoría en Logs CloudWatch	Este control comprueba si un clúster de base de datos Amazon Aurora MySQL está configurado para publicar registros de auditoría en Amazon Logs. CloudWatch El CSPM de Security Hub actualizó el control para que no genere resultados para los clústeres de bases de datos de Aurora sin servidor v1.

Fecha del cambio	ID y título de control	Descripción del cambio
11 de junio de 2024	[EKS.2] Los clústeres de EKS deben ejecutarse en una versión de Kubernetes compatible	Este control comprueba si un clúster de Amazon Elastic Kubernete s Service (Amazon EKS) se ejecuta en una versión de Kubernetes compatible. La versión compatible más antigua es `1.27`.

Fecha del cambio	ID y título de control	Descripción del cambio
10 de junio de 2024	[Config.1] AWS Config deben estar habilitados y usar la función vinculada al servicio para el registro de recursos	Este control comprueba si AWS Config está habilitado y si el registro de AWS Config recursos está activado. Anteriormente, el control solo generaba un resultado `PASSED` si se configuraba el registro para todos los recursos. El CSPM de Security Hub actualizó el control para generar un resultado `PASSED` cuando el registro está activado para recursos que se requieren para controles habilitados. El control también se ha actualizado para comprobar si se utiliza la función AWS Config vinculada al servicio, que proporciona permisos para registrar los recursos necesarios.

Fecha del cambio	ID y título de control	Descripción del cambio
8 de mayo de 2024	[S3.20] Los cubos de uso general de S3 deben tener habilitada la eliminación de MFA	Este control comprueba si el bucket con control de versiones de uso general de Amazon S3 tiene habilitada la eliminación de la autenticación multifactor (MFA). Anteriormente, el control generaba un resultado `FAILED` para los buckets que tenían una configuración de ciclo de vida. Sin embargo, la eliminación de la MFA con el control de versiones no se puede habilitar en un bucket que tenga una configuración de ciclo de vida. El CSPM de Security Hub actualizó el control para que no genere resultados para los buckets que tienen una configuración de ciclo de vida. La descripción del control se actualizó para

Fecha del cambio	ID y título de control	Descripción del cambio
		reflejar el comportamiento actual.
2 de mayo de 2024	[EKS.2] Los clústeres de EKS deben ejecutarse en una versión de Kubernetes compatible	El CSPM de Security Hub actualizó la versión más antigua compatible de Kubernetes en la que un clúster de Amazon EKS se puede ejecutar para producir un resultado aprobado. La versión compatible más antigua actual es Kubernetes `1.26`.

Fecha del cambio	ID y título de control	Descripción del cambio
30 de abril de 2024	[CloudTrail.3] Debe estar habilitada al menos una CloudTrail ruta	Se cambió el título del control, de «CloudTrail Debería estar habilitado» a «Debe estar habilitado al menos una CloudTrail ruta». Este control produce actualmente una `PASSED` búsqueda si Cuenta de AWS tiene al menos una CloudTrail ruta habilitada. El título y la descripción se modificaron para reflejar con precisión el comportamiento actual.

Fecha del cambio	ID y título de control	Descripción del cambio
29 de abril de 2024	[AutoScaling.1] Los grupos de Auto Scaling asociados a un balanceador de cargas deben usar comprobaciones de estado del ELB	Se cambió el título del control de Los grupos de escalado automático asociados a un equilibrador de carga clásico deben usar las comprobac iones de estado a Los grupos de escalado automático asociados a un equilibrador de carga deben usar comprobaciones de estado de ELB. Actualmente, este control evalúa los equilibradores de carga clásicos, de red, de puerta de enlace y de aplicacio nes. El título y la descripción se modificaron para reflejar con precisión el comportamiento actual.

Fecha del cambio	ID y título de control	Descripción del cambio
19 de abril de 2024	[CloudTrail.1] CloudTrail debe estar habilitado y configurado con al menos un registro multirregional que incluya eventos de administración de lectura y escritura	El control comprueba si AWS CloudTrail está habilitado y configurado con al menos un registro multirregional que incluya eventos de administración de lectura y escritura. Anteriormente, el control generaba `PASSED` resultados de forma incorrecta cuando una cuenta estaba CloudTrail habilitada y configurada con al menos un registro multirregional, incluso si ningún registro capturaba eventos de administración de lectura y escritura. El control ahora genera una `PASSED` búsqueda solo cuando CloudTrail está habilitado y configurado con al menos un registro multirregional que captura los eventos

Fecha del cambio	ID y título de control	Descripción del cambio
		de administración de lectura y escritura.
10 de abril de 2024	[Athena.1] Los grupos de trabajo de Athena deben estar cifrados cuando están en reposo	El CSPM de Security Hub retiró este control y lo eliminó de todos los estándare s. Los grupos de trabajo de Athena envían registros a buckets de Amazon Simple Storage Service (Amazon S3). Amazon S3 ahora proporciona el cifrado predeterminado con claves administradas de S3 (SS3-S3) en los buckets S3 nuevos y existentes.
10 de abril de 2024	[AutoScaling.4] La configuración de inicio grupal de Auto Scaling no debe tener un límite de salto de respuesta de metadatos superior a 1	El CSPM de Security Hub retiró este control y lo eliminó de todos los estándares. Los límites de saltos de respuesta de metadatos para instancias de Amazon Elastic Compute Cloud (Amazon EC2) dependen de las cargas de trabajo.

Fecha del cambio	ID y título de control	Descripción del cambio
10 de abril de 2024	[CloudFormation.1] las CloudFormation pilas deben integrarse con Simple Notification Service (SNS)	El CSPM de Security Hub retiró este control y lo eliminó de todos los estándares. Integrar pilas de AWS CloudFormation con temas de Amazon SNS ya no es una práctica de seguridad recomendada. Aunque la integraci ón de las CloudForm ation pilas important es con los temas del SNS puede resultar útil, no es necesaria para todas las pilas.
10 de abril de 2024	[CodeBuild.5] los entornos de CodeBuild proyectos no deberían tener habilitado el modo privilegiado	El CSPM de Security Hub retiró este control y lo eliminó de todos los estándares. Habilitar el modo privilegiado en un CodeBuild proyecto no supone un riesgo adicional para el entorno del cliente.

Fecha del cambio	ID y título de control	Descripción del cambio
10 de abril de 2024	[IAM.20] Evite el uso del usuario raíz	El CSPM de Security Hub retiró este control y lo eliminó de todos los estándares. El propósito de este control está cubierto por otro control, [CloudWatch.1] Debe existir un registro, un filtro métrico y una alarma para el uso del usuario «raíz».
10 de abril de 2024	[SNS.2] El registro del estado de entrega debe estar habilitado para los mensajes de notificac ión enviados a un tema	El CSPM de Security Hub retiró este control y lo eliminó de todos los estándares. Registrar el estado de entrega de los temas de SNS ya no es una práctica de seguridad recomendada. Aunque registrar el estado de entrega de los temas important es del SNS puede resultar útil, no es obligatorio para todos los temas.

Fecha del cambio	ID y título de control	Descripción del cambio
10 de abril de 2024	[S3.10] Los cubos de uso general de S3 con el control de versiones habilitado deben tener configuraciones de ciclo de vida	Security Hub CSPM eliminó este control de las mejores prácticas y AWS Service-Managed estándares de seguridad fundament ales:. AWS Control Tower El propósito de este control está cubierto por otros dos controles: [S3.13] Los cubos de uso general de S3 deben tener configuraciones de ciclo de vida y [S3.14] Los cubos de uso general de S3 deben tener habilitado el control de versiones . Este control sigue siendo parte del NIST SP 800-53 Rev. 5.

Fecha del cambio	ID y título de control	Descripción del cambio
10 de abril de 2024	[S3.11] Los cubos de uso general de S3 deben tener habilitadas las notificaciones de eventos	Security Hub CSPM eliminó este control de AWS Foundatio nal Security Best Practices and Standard:. Service-M anaged AWS Control Tower Si bien hay algunos casos en los que las notificac iones de eventos para los buckets de S3 son útiles, no se trata de una práctica de seguridad universal recomendada. Este control sigue siendo parte del NIST SP 800-53 Rev. 5.

Fecha del cambio	ID y título de control	Descripción del cambio
10 de abril de 2024	[SNS.1] Los temas de SNS deben cifrarse en reposo medianteAWS KMS	Security Hub CSPM eliminó este control de AWS Foundatio nal Security Best Practices and Standard:. Service-M anaged AWS Control Tower De forma predeterminada, SNS cifra los temas en reposo mediante el cifrado de disco. Para más información, consulte Cifrado de datos. Ya no AWS KMS se recomiend a su uso para cifrar temas como práctica recomendada de seguridad. Este control sigue siendo parte del NIST SP 800-53 Rev. 5.

Fecha del cambio	ID y título de control	Descripción del cambio
8 de abril de 2024	[ELB.6] Los balanceadores de cargas de aplicaciones, puertas de enlace y red deben tener habilitada la protección contra eliminaciones	Se cambió el título del control de El equilibrador de carga de aplicación debe tener habilitada la protección contra eliminaciones a Los equilibradores de carga de red, de las aplicaciones y de la puerta de enlace deben tener habilitada la protección contra eliminaciones. Actualmente, este control evalúa los equilibradores de carga de red, puertas de enlace y aplicaciones. El título y la descripción se modificaron para reflejar con precisión el comportamiento actual.

Fecha del cambio	ID y título de control	Descripción del cambio
22 de marzo de 2024	[Opensearch.8] Las conexiones a los OpenSearch dominios deben cifrarse con la última política de seguridad de TLS	El título del control, que pasó de Conexiones a OpenSearch dominios, debe cifrarse mediante TLS 1.2 a Conexiones a OpenSearch dominios, debe cifrarse mediante la política de seguridad TLS más reciente. Anteriormente, el control solo comprobaba si las conexiones a los OpenSearch dominios utilizaban TLS 1.2. El control ahora determina si los OpenSearch dominios están cifrados con la política de seguridad TLS más reciente. `PASSED` El título y la descripción del control se actualizaron para reflejar el comportamiento actual.

Fecha del cambio	ID y título de control	Descripción del cambio
22 de marzo de 2024	[ES.8] Las conexiones a los dominios de Elasticsearch deben cifrarse con la política de seguridad TLS más reciente	Se cambió el título del control de Las conexiones a dominios de Elasticsearch deben estar cifradas a través de TLS 1.2 a Las conexiones a los dominios de Elasticsearch deben estar cifrados a través de la última política de seguridad de TLS. Anteriormente, el control solo comprobaba si las conexiones a los dominios de Elasticsearch utilizaban TLS 1.2. El control ahora genera un resultado `PASSED` si los dominios de Elasticsearch están cifrados a través de la última política de seguridad de TLS. El título y la descripción del control se actualizaron para reflejar el comportamiento actual.

Fecha del cambio	ID y título de control	Descripción del cambio
12 de marzo de 2024	[S3.1] Los cubos de uso general de S3 deben tener habilitada la configuración de bloqueo del acceso público	El título cambió de La configuración del bloqueo de acceso público de S3 debe estar habilitada a Los buckets de uso general de S3 deben tener el bloqueo de acceso público habilitado. El CSPM de Security Hub cambió el título para considerar un nuevo tipo de bucket de S3.
12 de marzo de 2024	[S3.2] Los cubos de uso general de S3 deberían bloquear el acceso de lectura pública	Se cambió el título de Los buckets de S3 deben prohibir el acceso de lectura público a Los buckets de uso general de S3 deben bloquear el acceso de lectura público. El CSPM de Security Hub cambió el título para considerar un nuevo tipo de bucket de S3.

Fecha del cambio	ID y título de control	Descripción del cambio
12 de marzo de 2024	[S3.3] Los cubos S3 de uso general deberían bloquear el acceso público a la escritura	Se cambió el título de Los buckets de S3 deben prohibir el acceso de escritura público a Los buckets de uso general de S3 deben bloquear el acceso de escritura público. El CSPM de Security Hub cambió el título para considerar un nuevo tipo de bucket de S3.
12 de marzo de 2024	[S3.5] Los cubos de uso general de S3 deberían requerir que las solicitudes usen TLS	Se cambió el título de Los buckets de S3 deben requerir solicitudes para usar Secure Socket Layer a Los buckets de uso general de S3 deben requerir solicitudes para usar SSL. El CSPM de Security Hub cambió el título para considerar un nuevo tipo de bucket de S3.

Fecha del cambio	ID y título de control	Descripción del cambio
12 de marzo de 2024	[S3.6] Las políticas de bucket de uso general de S3 deberían restringir el acceso a otros Cuentas de AWS	Se cambió el título de Los permisos de S3 concedidos a otras Cuentas de AWS en las políticas de bucket deben restringirse a Las políticas de bucket de uso general de S3 deben restringir el acceso a otras Cuentas de AWS. El CSPM de Security Hub cambió el título para considerar un nuevo tipo de bucket de S3.
12 de marzo de 2024	[S3.7] Los cubos de uso general de S3 deben utilizar la replicación entre regiones	Se cambió el título de Los buckets de S3 deben tener la replicación entre regiones habilitada a Los buckets de uso general de S3 deben usar la replicación entre regiones. El CSPM de Security Hub cambió el título para considerar un nuevo tipo de bucket de S3.

Fecha del cambio	ID y título de control	Descripción del cambio
12 de marzo de 2024	[S3.7] Los cubos de uso general de S3 deben utilizar la replicación entre regiones	Se cambió el título de Los buckets de S3 deben tener la replicación entre regiones habilitada a Los buckets de uso general de S3 deben usar la replicación entre regiones. El CSPM de Security Hub cambió el título para considerar un nuevo tipo de bucket de S3.
12 de marzo de 2024	[S3.8] Los cubos de uso general de S3 deben bloquear el acceso público	Se cambió el título de La configuración de acceso público al bloque S3 debe estar habilitada en el nivel de bucket a Los buckets de uso general de S3 deben bloquear el acceso público. El CSPM de Security Hub cambió el título para considerar un nuevo tipo de bucket de S3.

Fecha del cambio	ID y título de control	Descripción del cambio
12 de marzo de 2024	[S3.9] Los cubos de uso general de S3 deben tener habilitado el registro de acceso al servidor	Se cambió el título de Se debe habilitar el registro de acceso al bucket de S3 a Se debe habilitar el registro de acceso al servidor para los buckets de uso general de S3. El CSPM de Security Hub cambió el título para considerar un nuevo tipo de bucket de S3.
12 de marzo de 2024	[S3.10] Los cubos de uso general de S3 con el control de versiones habilitado deben tener configuraciones de ciclo de vida	Se cambió el título de Los buckets de S3 con el control de versiones habilitado deben tener configura das las políticas de ciclo de vida a Los buckets de uso general de S3 con el control de versiones habilitado deben tener configuraciones de ciclo de vida. El CSPM de Security Hub cambió el título para considerar un nuevo tipo de bucket de S3.

Fecha del cambio	ID y título de control	Descripción del cambio
12 de marzo de 2024	[S3.11] Los cubos de uso general de S3 deben tener habilitadas las notificaciones de eventos	Se cambió el título de Los buckets de S3 deben tener las notificaciones de eventos habilitadas a Los buckets de uso general de S3 deben tener las notificac iones de eventos habilitadas. El CSPM de Security Hub cambió el título para considerar un nuevo tipo de bucket de S3.
12 de marzo de 2024	[S3.12] Las ACL no deben usarse para administrar el acceso de los usuarios a los cubos de uso general de S3	Se cambió el título de Las listas de control de acceso (ACL) de S3 no se deben utilizar para administrar el acceso de los usuarios a los buckets a Las ACL no se deben usar para administrar el acceso de los usuarios a los buckets de uso general de S3. El CSPM de Security Hub cambió el título para considerar un nuevo tipo de bucket de S3.

Fecha del cambio	ID y título de control	Descripción del cambio
12 de marzo de 2024	[S3.13] Los cubos de uso general de S3 deben tener configuraciones de ciclo de vida	Se cambió el título de Los buckets de S3 deben tener configuradas las políticas de ciclo de vida a Los buckets de uso general de S3 deben tener configuraciones de ciclo de vida. El CSPM de Security Hub cambió el título para considerar un nuevo tipo de bucket de S3.
12 de marzo de 2024	[S3.14] Los cubos de uso general de S3 deben tener habilitado el control de versiones	Se cambió el título de Los buckets de S3 deben utilizar el control de versiones a Los buckets de uso general de S3 deben tener el control de versiones habilitado. El CSPM de Security Hub cambió el título para considerar un nuevo tipo de bucket de S3.

Fecha del cambio	ID y título de control	Descripción del cambio
12 de marzo de 2024	[S3.15] Los cubos de uso general de S3 deben tener activado el bloqueo de objetos	Se cambió el título de Los buckets de S3 deben configura rse para usar el Bloqueo de objetos a Los buckets de uso general de S3 deben tener Bloqueo de objetos habilitado. El CSPM de Security Hub cambió el título para considerar un nuevo tipo de bucket de S3.
12 de marzo de 2024	[S3.17] Los cubos de uso general de S3 deben cifrarse en reposo con AWS KMS keys	Se cambió el título de Los buckets de S3 deben estar cifrados en reposo a través de AWS KMS keys a Los buckets de uso general de S3 deben estar cifrados en reposo a través de AWS KMS keys. El CSPM de Security Hub cambió el título para considerar un nuevo tipo de bucket de S3.

Fecha del cambio	ID y título de control	Descripción del cambio
7 de marzo de 2024	[Lambda.2] Las funciones de Lambda deben usar los tiempos de ejecución compatibles	Lambda.2 comprueba si la configuración de las AWS Lambda funciones para los tiempos de ejecución coincide con los valores esperados establecidos para los tiempos de ejecución compatibles en cada idioma. El CSPM de Security Hub admite ahora `nodejs20.x` y `ruby3.3` como parámetros.
22 de febrero de 2024	[Lambda.2] Las funciones de Lambda deben usar los tiempos de ejecución compatibles	Lambda.2 comprueba si la configuración de las AWS Lambda funciones para los tiempos de ejecución coincide con los valores esperados establecidos para los tiempos de ejecución compatibles en cada idioma. El CSPM de Security Hub ahora admite `dotnet8` como parámetro.

Fecha del cambio	ID y título de control	Descripción del cambio
5 de febrero de 2024	[EKS.2] Los clústeres de EKS deben ejecutarse en una versión de Kubernetes compatible	El CSPM de Security Hub actualizó la versión más antigua compatible de Kubernetes en la que un clúster de Amazon EKS se puede ejecutar para producir un resultado aprobado. La versión compatible más antigua actual es Kubernetes `1.25`.

Fecha del cambio	ID y título de control	Descripción del cambio
10 de enero de 2024	[CodeBuild.1] Las URL del repositorio fuente de CodeBuild Bitbucket no deben contener credenciales confidenciales	El título modificado CodeBuild GitHub o las URL del repositor io fuente de Bitbucket deben usar OAuth, ya que las URL del repositorio fuente de CodeBuild Bitbucket no deben contener credencia les confidenciales. El CSPM de Security Hub eliminó la mención de OAuth porque otros métodos de conexión también pueden ser seguros. Security Hub CSPM ha eliminado la mención « GitHubpor que ya no es posible tener un token de acceso personal o un nombre de usuario y contraseña» en las URL del repositorio de origen. GitHub

Fecha del cambio	ID y título de control	Descripción del cambio
8 de enero de 2024	[Lambda.2] Las funciones de Lambda deben usar los tiempos de ejecución compatibles	Lambda.2 comprueba si la configuración de las AWS Lambda funciones para los tiempos de ejecución coincide con los valores esperados establecidos para los tiempos de ejecución compatibles en cada idioma. El CSPM de Security Hub ya no admite `go1.x` ni `java8` como parámetros porque se trata de tiempos de ejecución retirados.

Fecha del cambio	ID y título de control	Descripción del cambio
29 de diciembre de 2023	[RDS.8] Las instancias de base de datos de RDS deben tener habilitada la protección contra eliminaciones	RDS.8 comprueba si una instancia de base de datos de Amazon RDS que utiliza uno de los motores de base de datos compatibles tiene habilitada la protección contra la eliminación. El CSPM de Security Hub admite ahora `custom-oracle-ee`, `oracle-ee-cdb` y `oracle-se2-cdb` como motores de bases de datos.

Fecha del cambio	ID y título de control	Descripción del cambio
22 de diciembre de 2023	[Lambda.2] Las funciones de Lambda deben usar los tiempos de ejecución compatibles	Lambda.2 comprueba si la configuración de las AWS Lambda funciones para los tiempos de ejecución coincide con los valores esperados establecidos para los tiempos de ejecución admitidos en cada idioma. El CSPM de Security Hub admite ahora `java21` y `python3.12` como parámetros. El CSPM de Security Hub dejó de admitir `ruby2.7` como parámetro.

Fecha del cambio	ID y título de control	Descripción del cambio
15 de diciembre de 2023	[CloudFront.1] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado	CloudFront.1 comprueba si una CloudFront distribución de Amazon tiene configurado un objeto raíz predeterminado. El CSPM de Security Hub redujo la gravedad de este control de CRÍTICA a ALTA porque agregar el objeto raíz predeterminado es una recomendación que depende de la aplicación del usuario y de sus requisitos específicos.
5 de diciembre de 2023	[EC2.13] Los grupos de seguridad no deberían permitir la entrada desde la versión 0.0.0. 0/0 o: :/0 al puerto 22	El título de control modificado de los grupos de seguridad no debería permitir la entrada desde la versión 0.0.0. 0/0 Al puerto 22, los grupos de seguridad no deberían permitir el ingreso desde la versión 0.0.0. 0/0 o: :/0 al puerto 22.

Fecha del cambio	ID y título de control	Descripción del cambio
5 de diciembre de 2023	[EC2.14] Los grupos de seguridad no deberían permitir la entrada desde la versión 0.0.0. 0/0 o: :/0 al puerto 3389	Se cambió el título del control de la versión 0.0.0 de Garantiza r que ningún grupo de seguridad permita la entrada. 0/0 Al puerto 3389, los grupos de seguridad no deberían permitir la entrada desde la versión 0.0.0. 0/0 o: :/0 al puerto 3389.

Fecha del cambio	ID y título de control	Descripción del cambio
5 de diciembre de 2023	[RDS.9] Las instancias de base de datos de RDS deben publicar los registros en Logs CloudWatch	El título de control modificado del registro de la base de datos debe habilitarse para que las instancias de base de datos de RDS publiquen los registros en Logs. CloudWatch El CSPM de Security Hub identificó que este control solo comprueba si los registros están publicados en Amazon CloudWatch Logs y no comprueba si los registros de RDS están habilitados. El control determina si las instancias de `PASSED` base de datos de RDS están configuradas para publicar registros en Logs. CloudWatch El título del control se ha actualizado para reflejar el comportamiento actual.

Fecha del cambio	ID y título de control	Descripción del cambio
5 de diciembre de 2023	[EKS.8] Los clústeres de EKS deben tener habilitado el registro de auditoría	Este control comprueba si los clústeres de Amazon EKS tienen habilitado el registro de auditoría . La AWS Config regla que usa Security Hub CSPM para evaluar este control cambió de a. `eks-cluster-logging-enabled` `eks-cluster-log-enabled`

Fecha del cambio	ID y título de control	Descripción del cambio
17 de noviembre de 2023	[EC2.19] Los grupos de seguridad no deben permitir el acceso irrestricto a los puertos de alto riesgo	EC2.19 comprueba si los puertos especificados que se consideran de alto riesgo pueden acceder al tráfico entrante sin restricciones de un grupo de seguridad. El CSPM de Security Hub actualizó este control para tener en cuenta las listas de prefijos administradas cuando se suministran como origen en una regla de grupo de seguridad. El control produce una `FAILED` búsqueda si las listas de prefijos contienen las cadenas «0.0.0». 0/0' o ': :/0'.

Fecha del cambio	ID y título de control	Descripción del cambio
16 de noviembre de 2023	[CloudWatch.15] CloudWatch las alarmas deben tener configuradas acciones específicas	Se cambió el título de control, que pasó de ser CloudWatch las alarmas, que deberían tener una acción configurada para el estado de ALARMA, a CloudWatch las alarmas, que deberían tener configuradas acciones específicas.
16 de noviembre de 2023	[CloudWatch.16] los grupos de CloudWatch registros deben conservarse durante un período de tiempo específico	El título de control modificado de los grupos de CloudWatch registro debe conservarse durante al menos 1 año, mientras que los grupos de CloudWatch registros deben conservarse durante un período de tiempo específico.

Fecha del cambio	ID y título de control	Descripción del cambio
16 de noviembre de 2023	[Lambda.5] Las funciones de VPC Lambda deben funcionar en varias zonas de disponibilidad	Se ha cambiado el título de control de Las funciones de Lambda de la VPC deben funcionar en más de una zona de disponibilidad a Las funciones de Lambda de la VPC deben funcionar en varias zonas de disponibilidad.
16 de noviembre de 2023	[AppSync.2]AWS AppSyncdebe tener habilitado el registro a nivel de campo	Se ha cambiado el título de control de AWS AppSync debe tener activado el registro a nivel de solicitud y a nivel de campo a AWS AppSync debe tener habilitado el registro a nivel de campo.
16 de noviembre de 2023	[EMR.1] Los nodos principales del clúster de Amazon EMR no deben tener direcciones IP públicas	Los nodos maestros del MapReduce clúster de Amazon Elastic no deben tener direcciones IP públicas y los nodos principales del clúster de Amazon EMR no deben tener direcciones IP públicas.

Fecha del cambio	ID y título de control	Descripción del cambio
16 de noviembre de 2023	[Opensearch.2] OpenSearch los dominios no deben ser de acceso público	El título de control cambiado, de OpenSearch los dominios debe estar en una VPC a los OpenSearch dominios no deben ser de acceso público.
16 de noviembre de 2023	[ES.2] Los dominios de Elasticsearch no deben ser de acceso público	Se ha cambiado el título de control de Los dominios de Elasticsearch deben estar en una VPC a Los dominios de Elasticsearch no deben ser de acceso público.

Fecha del cambio	ID y título de control	Descripción del cambio
31 de octubre de 2023	[ES.4] Debería estar habilitado el registro de errores de dominio de Elasticsearch en Logs CloudWatch	ES.4 comprueba si los dominios de Elasticsearch están configurados para enviar registros de errores a Amazon Logs. CloudWatc h Anteriormente, el control detectó un `PASSED` dominio de Elasticsearch que tenía algún registro configurado para enviarse a Logs. CloudWatch El CSPM de Security Hub actualizó el control para generar una `PASSED` búsqueda únicamente para un dominio de Elasticsearch que esté configurado para enviar registros de errores a Logs. CloudWatch El control también se actualizó para excluir de la evaluación versiones de Elasticsearch que no admiten registros de errores.

Fecha del cambio	ID y título de control	Descripción del cambio
16 de octubre de 2023	[EC2.13] Los grupos de seguridad no deberían permitir la entrada desde la versión 0.0.0. 0/0 o: :/0 al puerto 22	EC2.13 comprueba si los grupos de seguridad permiten el acceso sin restricciones al puerto 22. El CSPM de Security Hub actualizó este control para tener en cuenta las listas de prefijos administradas cuando se suministran como origen en una regla de grupo de seguridad. El control determina si las listas `FAILED` de prefijos contienen las cadenas «0.0.0». 0/0' o ': :/0'.

Fecha del cambio	ID y título de control	Descripción del cambio
16 de octubre de 2023	[EC2.14] Los grupos de seguridad no deberían permitir la entrada desde la versión 0.0.0. 0/0 o: :/0 al puerto 3389	EC2.14 comprueba si los grupos de seguridad permiten el acceso de entrada sin restricciones al puerto 3389. El CSPM de Security Hub actualizó este control para tener en cuenta las listas de prefijos administradas cuando se suministr an como origen en una regla de grupo de seguridad. El control produce una `FAILED` búsqueda si las listas de prefijos contienen las cadenas «0.0.0». 0/0' o ': :/0'.

Fecha del cambio	ID y título de control	Descripción del cambio
16 de octubre de 2023	[EC2.18] Los grupos de seguridad solo deben permitir el tráfico entrante sin restricciones en los puertos autorizados	EC2.18 comprueba si los grupos de seguridad que están en uso permiten el tráfico entrante sin restricciones. El CSPM de Security Hub actualizó este control para tener en cuenta las listas de prefijos administradas cuando se suministr an como origen en una regla de grupo de seguridad. El control produce una `FAILED` búsqueda si las listas de prefijos contienen las cadenas «0.0.0». 0/0' o ': :/0'.

Fecha del cambio	ID y título de control	Descripción del cambio
16 de octubre de 2023	[Lambda.2] Las funciones de Lambda deben usar los tiempos de ejecución compatibles	Lambda.2 comprueba si la configuración de las AWS Lambda funciones para los tiempos de ejecución coincide con los valores esperados establecidos para los tiempos de ejecución compatibles en cada idioma. El CSPM de Security Hub ahora admite `python3.11` como parámetro.
4 de octubre de 2023	[S3.7] Los cubos de uso general de S3 deben utilizar la replicación entre regiones	El CSPM de Security Hub agregó el parámetro `ReplicationType` con un valor `CROSS-REGION` para garantizar que los buckets de S3 tengan habilitada la replicación entre regiones en lugar de la replicación en la misma región.

Fecha del cambio	ID y título de control	Descripción del cambio
27 de septiembre de 2023	[EKS.2] Los clústeres de EKS deben ejecutarse en una versión de Kubernetes compatible	El CSPM de Security Hub actualizó la versión más antigua compatible de Kubernetes en la que un clúster de Amazon EKS se puede ejecutar para producir un resultado aprobado. La versión compatible más antigua actual es Kubernetes `1.24`.
20 de septiembre de 2023	[CloudFront.2] CloudFront las distribuciones deben tener habilitada la identidad de acceso al origen	El CSPM de Security Hub retiró este control y lo eliminó de todos los estándares. En su lugar, consulte [CloudFront.13] CloudFront las distribuciones deben usar el control de acceso al origen. El control de acceso de Origin es la mejor práctica de seguridad actual. Este control se eliminará de la documentación en 90 días.

Fecha del cambio	ID y título de control	Descripción del cambio
20 de septiembre de 2023	[EC2.22] Deben eliminarse los grupos de seguridad de Amazon EC2 no utilizados	Security Hub CSPM eliminó este control del SP 800-53 Rev. AWS 5 de Foundatio nal Security Best Practices (FSBP) y del National Institute of Standards and Technology (NIST). Sigue siendo parte de Standard:. Service-M anaged AWS Control Tower Este control de produce un resultado aprobado si los grupos de seguridad están conectados a instancias EC2 o a una interfaz de red elástica. Sin embargo, en algunos casos de uso, los grupos de seguridad independi entes no represent an un riesgo para la seguridad. Puede usar otros controles de EC2 EC2.2, como,, y EC2.13 EC2.14 EC2.18, EC2.19 para monitorear sus grupos de seguridad.

Fecha del cambio	ID y título de control	Descripción del cambio
20 de septiembre de 2023	[EC2.29] Las instancias EC2 deben lanzarse en una VPC	El CSPM de Security Hub retiró este control y lo eliminó de todos los estándares. Amazon EC2 ha migrado EC2-Class ic instancias a una VPC. Este control se eliminará de la documentación en 90 días.

Fecha del cambio	ID y título de control	Descripción del cambio
20 de septiembre de 2023	[S3.4] Los buckets S3 deben tener habilitado el cifrado del lado del servidor	El CSPM de Security Hub retiró este control y lo eliminó de todos los estándares. Amazon S3 ahora proporciona el cifrado predeterminado con claves administradas de S3 (SS3-S3) en los buckets de S3 nuevos y existentes. La configuración de cifrado permanece inalterada para los buckets existentes que están cifrados con cifrado del lado SS3-KMS del servidor SS3-S3 o del lado del servidor. Este control se eliminará de la documentación en 90 días.

Fecha del cambio	ID y título de control	Descripción del cambio
14 de septiembre de 2023	[EC2.2] Los grupos de seguridad predeterminados de VPC no deben permitir el tráfico entrante o saliente	Se cambió el título de control de El grupo de seguridad predeterminado de VPC no debe permitir el tráfico entrante ni saliente a Los grupos de seguridad predeterminados de VPC no deben permitir el tráfico entrante ni saliente.
14 de septiembre de 2023	[IAM.9] La MFA debe estar habilitada para el usuario root	Se cambió el título de control de La MFA virtual debe estar habilitada para el usuario raíz a La MFA debe estar habilitada para el usuario raíz.

Fecha del cambio	ID y título de control	Descripción del cambio
14 de septiembre de 2023	[RDS.19] Las suscripciones de notificación de eventos de RDS existentes deben configurarse para los eventos críticos del clúster	Se cambió el título de control de Se debe configurar una suscripción a las notificaciones de eventos de RDS para los eventos de clúster críticos a Las suscripciones de notificación de eventos de RDS existentes deben configurarse para los eventos de clúster críticos.
14 de septiembre de 2023	[RDS.20] Las suscripciones de notificación de eventos de RDS existentes deben configurarse para los eventos críticos de las instancias de bases de datos	Se cambió el título de control de Se debe configurar una suscripción a las notificaciones de eventos de RDS para los eventos críticos de instancias de bases de datos a Las suscripciones de notificación de eventos de RDS existentes deben configurarse para los eventos críticos de instancias de bases de datos.

Fecha del cambio	ID y título de control	Descripción del cambio
14 de septiembre de 2023	[WAF.2]AWS WAFLas reglas regionales clásicas deben tener al menos una condición	Se cambió el título de control de Una regla regional de WAF debe tener al menos una condición a Las reglas regionales de AWS WAF Classic deben tener al menos una condición.
14 de septiembre de 2023	[WAF.3]AWS WAFLos grupos de reglas regionales clásicos deben tener al menos una regla	Se cambió el título de control de Un grupo de reglas regionales de WAF debe tener al menos una regla a Los grupos de reglas regionales de AWS WAF Classic deben tener al menos una regla.
14 de septiembre de 2023	[WAF.4]AWS WAFLas ACL web regionales clásicas deben tener al menos una regla o grupo de reglas	Se cambió el título de control de Una ACL web regional de WAF debe tener al menos una regla o grupo de reglas a Las ACL web regionales de AWS WAF Classic deben tener al menos una regla o grupo de reglas.

Fecha del cambio	ID y título de control	Descripción del cambio
14 de septiembre de 2023	[WAF.6]AWS WAFLas reglas globales clásicas deben tener al menos una condición	Se cambió el título de control de Una regla global de WAF debe tener al menos una condición a Las reglas globales de AWS WAF Classic deben tener al menos una condición.
14 de septiembre de 2023	[WAF.7]AWS WAFLos grupos de reglas globales clásicos deben tener al menos una regla	Se cambió el título de control de Un grupo de reglas globales de WAF debe tener al menos una regla a Los grupos de reglas globales de AWS WAF Classic deben tener al menos una regla.
14 de septiembre de 2023	[WAF.8]AWS WAFLas ACL web globales clásicas deben tener al menos una regla o grupo de reglas	Se cambió el título de control de Una ACL web global de WAF debe tener al menos una regla o grupo de reglas a Las ACL web globales de AWS WAF Classic deben tener al menos una regla o grupo de reglas.

Fecha del cambio	ID y título de control	Descripción del cambio
14 de septiembre de 2023	[WAF.10]AWS WAFLas ACL web deben tener al menos una regla o grupo de reglas	Se cambió el título de control de Una ACL web de WAFv2 debe tener al menos una regla o grupo de reglas a Las ACL de AWS WAF deben tener al menos una regla o grupo de reglas.
14 de septiembre de 2023	[WAF.11]AWS WAFEl registro de ACL web debe estar habilitado	Se cambió el título de control de El registro de la ACL web de AWS WAF v2 debe estar activado a El registro de la ACL web de AWS WAF debe estar habilitado.

Fecha del cambio	ID y título de control	Descripción del cambio
20 de julio de 2023	[S3.4] Los buckets S3 deben tener habilitado el cifrado del lado del servidor	S3.4 comprueba si un bucket de Amazon S3 tiene habilitado el cifrado del lado del servidor o si la política de cubos de S3 deniega `PutObject` explícitamente las solicitudes sin el cifrado del lado del servidor. Security Hub CSPM actualizó este control para incluir el cifrado de doble capa del lado del servidor con claves KMS (). DSSE-KMS El control produce un resultado aprobado cuando un bucket de S3 se cifra con SSE-S3, SSE-KMS o. DSSE-KMS

Fecha del cambio	ID y título de control	Descripción del cambio
17 de julio de 2023	[S3.17] Los cubos de uso general de S3 deben cifrarse en reposo con AWS KMS keys	S3.17 comprueba si un bucket de Amazon S3 está cifrado con un AWS KMS key. Security Hub CSPM actualizó este control para incluir el cifrado de doble capa en el lado del servidor con claves KMS (). DSSE-KMS El control produce un resultado aprobado cuando un bucket de S3 se cifra con o. SSE-KMS DSSE-KMS
9 de junio de 2023	[EKS.2] Los clústeres de EKS deben ejecutarse en una versión de Kubernetes compatible	EKS.2 comprueba si un clúster de Amazon EKS se ejecuta en una versión de Kubernete s compatible. La versión compatible más antigua es ahora. `1.23`

Fecha del cambio	ID y título de control	Descripción del cambio
9 de junio de 2023	[Lambda.2] Las funciones de Lambda deben usar los tiempos de ejecución compatibles	Lambda.2 comprueba si la configuración de las AWS Lambda funciones para los tiempos de ejecución coincide con los valores esperados establecidos para los tiempos de ejecución compatibles en cada idioma. El CSPM de Security Hub ahora admite `ruby3.2` como parámetro.
5 de junio de 2023	[APIGateway.5] Los datos de la caché de la API REST de API Gateway deben cifrarse en reposo	APIGateway.5.checks si todos los métodos de las etapas de la API REST de Amazon API Gateway están cifrados en reposo. El CSPM de Security Hub actualizó el control para evaluar el cifrado de un método específico únicamente cuando el almacenamiento en caché está habilitado para ese método.

Fecha del cambio	ID y título de control	Descripción del cambio
18 de mayo de 2023	[Lambda.2] Las funciones de Lambda deben usar los tiempos de ejecución compatibles	Lambda.2 comprueba si la configuración de las AWS Lambda funciones para los tiempos de ejecución coincide con los valores esperados establecidos para los tiempos de ejecución admitidos en cada idioma. El CSPM de Security Hub ahora admite `java17` como parámetro.
18 de mayo de 2023	[Lambda.2] Las funciones de Lambda deben usar los tiempos de ejecución compatibles	Lambda.2 comprueba si la configuración de las AWS Lambda funciones para los tiempos de ejecución coincide con los valores esperados establecidos para los tiempos de ejecución compatibles en cada idioma. El CSPM de Security Hub dejó de admitir `nodejs12.x` como parámetro.

Fecha del cambio	ID y título de control	Descripción del cambio
23 de abril de 2023	[ECS.10] Los servicios Fargate de ECS deberían ejecutarse en la última versión de la plataforma Fargate	ECS.10 comprueba si los servicios Fargate de Amazon ECS ejecutan la versión más reciente de la plataforma Fargate. Los clientes pueden implementar Amazon ECS a través de ECS directamente o mediante el uso de. CodeDeploy Security Hub CSPM actualizó este control para obtener resultados aprobados cuando se utilizan CodeDeplo y para implementar los servicios de ECS Fargate.

Fecha del cambio	ID y título de control	Descripción del cambio
20 de abril de 2023	[S3.6] Las políticas de bucket de uso general de S3 deberían restringir el acceso a otros Cuentas de AWS	S3.6 comprueba si una política de depósitos de Amazon Simple Storage Service (Amazon S3) impide que otras personas ejecuten acciones denegadas en los recursos Cuentas de AWS del depósito S3. El CSPM de Security Hub actualizó el control para tener en cuenta los condicion ales de una política de bucket.
18 de abril de 2023	[Lambda.2] Las funciones de Lambda deben usar los tiempos de ejecución compatibles	Lambda.2 comprueba si la configuración de las AWS Lambda funciones para los tiempos de ejecución coincide con los valores esperados establecidos para los tiempos de ejecución admitidos en cada idioma. El CSPM de Security Hub ahora admite `python3.10` como parámetro.

Fecha del cambio	ID y título de control	Descripción del cambio
18 de abril de 2023	[Lambda.2] Las funciones de Lambda deben usar los tiempos de ejecución compatibles	Lambda.2 comprueba si la configuración de las AWS Lambda funciones para los tiempos de ejecución coincide con los valores esperados establecidos para los tiempos de ejecución compatibl es en cada idioma. El CSPM de Security Hub dejó de admitir `dotnetcore3.1` como parámetro.

Fecha del cambio	ID y título de control	Descripción del cambio
17 de abril de 2023	[RDS.11] Las instancias de RDS deben tener habilitadas las copias de seguridad automáticas	RDS.11 comprueba si las instancias de Amazon RDS tienen habilitadas las copias de seguridad automatizadas, con un período de retención de las copias de seguridad superior o igual a siete días. El CSPM de Security Hub actualizó este control para excluir las réplicas de lectura de la evaluación, ya que no todos los motores admiten copias de seguridad automatizadas en las réplicas de lectura. Además, RDS no ofrece la opción de especificar un periodo de retención de las copias de seguridad al crear réplicas de lectura. Las réplicas de lectura se crean con un periodo de retención predeterminado de la copia de seguridad de `0`.

Controles CSPM de Security Hub paraCuentas de AWS

Estos controles CSPM de Security Hub evalúan. Cuentas de AWS

Es posible que estos controles no estén disponibles en todos. Regiones de AWS Para obtener más información, consulte Disponibilidad de los controles por región.

[Account.1] La información de contacto de seguridad debe proporcionarse para unCuenta de AWS

Requisitos relacionados: CIS AWS Foundations Benchmark v5.0. 0/1.2 NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoría: Identificar > Configuración de recursos

Gravedad: media

Tipo de recurso: `AWS::::Account`

Regla de AWS Config: `security-account-information-provided`

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si una cuenta de Amazon Web Services (AWS) tiene información de contacto de seguridad. El control falla si no se proporciona la información de contacto de seguridad de la cuenta.

Los contactos de seguridad alternativos te AWS permiten ponerte en contacto con otra persona en caso de que no estés disponible para resolver problemas con tu cuenta. Las notificaciones pueden provenir de Soporte otros equipos o de otros Servicio de AWS equipos sobre temas relacionados con la seguridad relacionados con tu Cuenta de AWS uso.

Corrección

Para añadir un contacto alternativo como contacto de seguridad al tuyoCuenta de AWS, consulta Actualizar tus contactos alternativos Cuenta de AWS en la Guía de referencia sobre administración de AWS cuentas.

[Account.2]Cuentas de AWSdebe formar parte de unAWS Organizationsorganización

Categoría: Proteger - Administración de acceso seguro > Control de acceso

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Gravedad: alta

Tipo de recurso: `AWS::::Account`

Regla de AWS Config: `account-part-of-organizations`

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si una Cuenta de AWS forma parte de una organización gestionada a través de ellaAWS Organizations. El control falla si la cuenta no forma parte de una organización.

Organizations le ayuda a administrar su entorno de forma centralizada a medida que amplía sus cargas de trabajo. AWS Puede usar varias Cuentas de AWS para aislar las cargas de trabajo que tienen requisitos de seguridad específicos o para cumplir con marcos como la HIPAA o la PCI. Al crear una organización, puede administrar varias cuentas como una sola unidad y administrar de forma centralizada su acceso a Servicios de AWS los recursos y las regiones.

Corrección

Para crear una nueva organización y Cuentas de AWS añadirla automáticamente, consulte Creación de una organización en la Guía del AWS Organizations usuario. Para añadir cuentas a una organización existente, consulte Invitar a un usuario Cuenta de AWS a unirse a su organización en la Guía del AWS Organizations usuario.

Controles CSPM de Security Hub paraAWS Amplify

Estos controles CSPM de Security Hub evalúan el AWS Amplify servicio y los recursos. Es posible que los controles no estén disponibles en todos. Regiones de AWS Para obtener más información, consulte Disponibilidad de los controles por región.

[Amplify.1] Las aplicaciones Amplify deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::Amplify::App`

Regla de AWS Config: amplify-app-tagged

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredKeyTags`	Una lista de claves de etiqueta que no son del sistema y que se deben asignar a un recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si una AWS Amplify aplicación tiene las claves de etiqueta especificadas por el `requiredKeyTags` parámetro. El control falla si la aplicación no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas por el parámetro `requiredKeyTags`. Si no especifica ningún valor para el parámetro `requiredKeyTags`, el control solo verifica la existencia de una clave de etiqueta y falla si la aplicación no tiene ninguna clave de etiqueta. El control ignora las etiquetas del sistema, que se aplican automáticamente y tienen el prefijo `aws:`.

Una etiqueta es una etiqueta que se crea y se asigna a un AWS recurso. Cada etiqueta consta de una clave de etiqueta necesaria y un valor de etiqueta opcional. Utilice etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. También pueden ayudar a identificar, organizar, buscar y filtrar recursos. También pueden ayudar a rastrear propietarios de recursos para acciones y notificaciones. También puede usar etiquetas para implementar control de acceso basado en atributos (ABAC) como estrategia de autorización. Para obtener más información sobre estrategias ABAC, consulte Definición de permisos basados en atributos con autorización ABAC en la Guía del usuario de IAM. Para obtener más información sobre las etiquetas, consulte los AWSrecursos de etiquetado y la Guía del usuario del editor de etiquetas.

> **Note**
>
> No almacene información de identificación personal (PII) ni otra información confidencial en las etiquetas. Se puede acceder a las etiquetas desde muchos Servicios de AWS sitios. No están destinadas a usarse para datos privados o información confidencial.

Corrección

Para obtener información sobre cómo añadir etiquetas a una AWS Amplify aplicación, consulta la compatibilidad con el etiquetado de recursos en la Guía del usuario de AWS Amplify hosting.

[Amplify.2] Amplify branches debe estar etiquetado

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::Amplify::Branch`

Regla de AWS Config: amplify-branch-tagged

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredKeyTags`	Una lista de claves de etiqueta que no son del sistema y que se deben asignar a un recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si una AWS Amplify rama tiene las claves de etiqueta especificadas por el `requiredKeyTags` parámetro. El control falla si la rama no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas por el parámetro `requiredKeyTags`. Si no especifica ningún valor para el parámetro `requiredKeyTags`, el control solo verifica la existencia de una clave de etiqueta y falla si la rama no tiene ninguna clave de etiqueta. El control ignora las etiquetas del sistema, que se aplican automáticamente y tienen el prefijo `aws:`.

Una etiqueta es una etiqueta que se crea y se asigna a un AWS recurso. Cada etiqueta consta de una clave de etiqueta necesaria y un valor de etiqueta opcional. Utilice etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. También pueden ayudar a identificar, organizar, buscar y filtrar recursos. También pueden ayudar a rastrear propietarios de recursos para acciones y notificaciones. También puede usar etiquetas para implementar control de acceso basado en atributos (ABAC) como estrategia de autorización. Para obtener más información sobre estrategias ABAC, consulte Definición de permisos basados en atributos con autorización ABAC en la Guía del usuario de IAM. Para obtener más información sobre las etiquetas, consulte los AWSrecursos de etiquetado y la Guía del usuario del editor de etiquetas.

> **Note**
>
> No almacene información de identificación personal (PII) ni otra información confidencial en las etiquetas. Se puede acceder a las etiquetas desde muchos Servicios de AWS sitios. No están destinadas a usarse para datos privados o información confidencial.

Corrección

Para obtener información sobre cómo añadir etiquetas a una AWS Amplify sucursal, consulta la compatibilidad con el etiquetado de recursos en la Guía del usuario de AWS Amplify hosting.

Controles de CSPM de Security Hub para Amazon API Gateway

Estos AWS Security Hub CSPM controles evalúan el servicio y los recursos de Amazon API Gateway. Es posible que los controles no estén disponibles en todos los casos Regiones de AWS. Para obtener más información, consulte Disponibilidad de los controles por región.

[APIGateway.1] El registro de ejecución de API y REST de WebSocket API Gateway deben estar habilitados.

Requisitos relacionados: NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-7 (8)

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: `AWS::ApiGateway::Stage`, `AWS::ApiGatewayV2::Stage`

Regla de AWS Config : [api-gw-execution-logging-enabled]

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub CSPM
`loggingLevel`	Nivel de registro	Enum	`ERROR`, `INFO`	`No default value`

Este control comprueba si todas las etapas de una API o REST de Amazon API Gateway tienen WebSocket habilitado el registro. Se produce un error en el control si `loggingLevel` no figura como `ERROR` o `INFO` en todas las etapas de la API. A menos que proporcione valores de parámetros personalizados para indicar que se debe habilitar un tipo de registro específico, Security Hub CSPM produce un resultado satisfactorio si el nivel de registro es o`ERROR`. `INFO`

Las etapas REST o WebSocket API de API Gateway deben tener habilitados los registros pertinentes. Los registros de ejecución de WebSocket API y REST de API de API Gateway proporcionan registros detallados de las solicitudes realizadas a las etapas REST y API de API de WebSocket API Gateway. Las etapas incluyen las respuestas del backend de la integración de

API, las respuestas del autorizador de Lambda y las de los puntos finales `requestId` de AWS integración.

Corrección

Para habilitar el registro de las operaciones de WebSocket REST y API, consulte Configurar el registro de CloudWatch API mediante la consola de API Gateway en la Guía para desarrolladores de API Gateway.

[APIGateway.2] Las etapas de la API REST de API Gateway deben configurarse para usar certificados SSL para la autenticación de backend

Requisitos relacionados: NIST.800-53.r5 AC-17 (2) NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), NIST.800-53.r5 SC-12 (3),, (3) NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (3), NIST.800-53.r5 SC-7 (4) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (1), (2), NIST.800-53.r5 SC-8 NIST.800-53.r5 SI-7 (6), NIST.800-171.r2 3.13.15

Categoría: Proteger > Protección de datos > Cifrado de datos en tránsito

Gravedad: media

Tipo de recurso: `AWS::ApiGateway::Stage`

Regla de AWS Config : api-gw-ssl-enabled

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si las etapas de la API de REST de Amazon API Gateway tienen certificados SSL configurados. Los sistemas de backend utilizan estos certificados para autenticar que las solicitudes entrantes provienen de API Gateway.

Las etapas de la API de REST de API Gateway deben configurarse con certificados SSL para permitir que los sistemas de backend autentiquen que las solicitudes se originan en API Gateway.

Corrección

Para obtener instrucciones detalladas sobre cómo generar y configurar los certificados SSL de la API de REST de API Gateway, consulte Generar y configurar un certificado SSL para la autenticación de backend en la Guía para desarrolladores de API Gateway.

[APIGateway.3] Las etapas de la API REST de API Gateway deben tener AWS X-Ray rastreo habilitado

Requisitos relacionados: NIST.800-53.r5 CA-7

Categoría: Detectar - Servicios de detección

Gravedad: baja

Tipo de recurso: `AWS::ApiGateway::Stage`

Regla de AWS Config : api-gw-xray-enabled

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si el rastreo AWS X-Ray activo está activado en las etapas de la API REST de Amazon API Gateway.

X-Ray el rastreo activo permite una respuesta más rápida a los cambios de rendimiento en la infraestructura subyacente. Los cambios en el rendimiento pueden provocar una falta de disponibilidad de la API. X-RayEl rastreo activo proporciona métricas en tiempo real de las solicitudes de los usuarios que fluyen a través de las operaciones de la API REST de API Gateway y los servicios conectados.

Corrección

Para obtener instrucciones detalladas sobre cómo habilitar el rastreo X-Ray activo para las operaciones de la API REST de API Gateway, consulte el soporte de rastreo activo de Amazon API Gateway AWS X-Ray en la Guía para AWS X-Ray desarrolladores.

[APIGateway.4] API Gateway debe estar asociada a una ACL web de WAF

Requisitos relacionados: NIST.800-53.r5 AC-4 (21)

Categoría: Proteger > Servicios de protección

Gravedad: media

Tipo de recurso: `AWS::ApiGateway::Stage`

Regla de AWS Config : api-gw-associated-with-waf

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una etapa de API Gateway usa una lista de control de acceso (ACL) a la AWS WAF web. Este control falla si una ACL AWS WAF web no está conectada a una etapa de REST API Gateway.

AWS WAF es un firewall de aplicaciones web que ayuda a proteger las aplicaciones web y las API de los ataques. Le permite configurar una web ACL, que son un conjunto de reglas que permiten, bloquean o cuentan solicitudes web en función de las reglas y condiciones de seguridad web personalizables que defina. Asegúrese de que su etapa de API Gateway esté asociada a una ACL AWS WAF web para protegerla de ataques malintencionados.

Corrección

Para obtener información sobre cómo usar la consola de API Gateway para asociar una ACL web AWS WAF regional a una etapa de API Gateway existente, consulte Using AWS WAF to protect your API en la Guía para desarrolladores de API Gateway.

[APIGateway.5] Los datos de la caché de la API REST de API Gateway deben cifrarse en reposo

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6) NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6)

Categoría: Proteger - Protección de datos - Cifrado de datos en reposo

Gravedad: media

Tipo de recurso: `AWS::ApiGateway::Stage`

AWS Config regla: `api-gw-cache-encrypted` (regla CSPM personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si todos los métodos de las etapas de la API de REST de API Gateway que tienen la caché habilitada están cifrados. El control falla si algún método de una etapa de API de REST de API Gateway está configurado para almacenar en caché y la caché no está cifrada. El CSPM de Security Hub evalúa el cifrado de un método determinado solo cuando el almacenamiento en caché está habilitado para ese método.

El cifrado de los datos en reposo reduce el riesgo de que un usuario no autenticado acceda a los datos almacenados en el disco. AWS Añade otro conjunto de controles de acceso para limitar la capacidad de los usuarios no autorizados de acceder a los datos. Por ejemplo, se requieren permisos de API para descifrar los datos antes de que puedan leerse.

Las cachés de la API de REST de API Gateway deben cifrarse en reposo para ofrecer una capa de seguridad adicional.

Corrección

Para configurar el almacenamiento en caché de API para una etapa, consulte Habilitar el almacenamiento en caché de Amazon API Gateway en la Guía para desarrolladores de API Gateway. En Configuración de caché, seleccione Cifrar datos de caché.

[APIGateway.8] Las rutas de API Gateway deben especificar un tipo de autorización

Requisitos relacionados: NIST.800-53.r5 AC-3, NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoría: Proteger > Administración de acceso seguro

Gravedad: media

Tipo de recurso: `AWS::ApiGatewayV2::Route`

Regla de AWS Config : api-gwv2-authorization-type-configured

Tipo de programa: Periódico

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub CSPM
`authorizationType`	Tipo de autorización de las rutas de API	Enum	`AWS_IAM`, `CUSTOM`, `JWT`	Sin valor predeterminado

Este control comprueba si las rutas de Amazon API Gateway tienen un tipo de autorización. Se produce un error en el control si la ruta de API Gateway no tiene ningún tipo de autorización. También, puede proporcionar un valor personalizado de parámetro si quiere que el control pase únicamente si la ruta utiliza el tipo de autorización especificado en el parámetro `authorizationType`.

API Gateway admite varios mecanismos para controlar y administrar el acceso a la API. Al especificar un tipo de autorización, puede restringir el acceso a tu API solo a los usuarios o procesos autorizados.

Corrección

Para establecer un tipo de autorización para las API HTTP, consulte Controlar y administrar el acceso a una API HTTP en API Gateway en la Guía para desarrolladores de API Gateway. Para establecer un tipo de autorización para WebSocket las API, consulte Controlar y administrar el acceso a una WebSocket API en API Gateway en la Guía para desarrolladores de API Gateway.

[APIGateway.9] El registro de acceso debe configurarse para las etapas V2 de API Gateway

Requisitos relacionados: NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AU-10,, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2 NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 SC-7 (9) NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-7 (8), PCI DSS v4.0. 1/10.4.2

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: `AWS::ApiGatewayV2::Stage`

Regla de AWS Config : api-gwv2-access-logs-enabled

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si las etapas de Amazon API Gateway V2 tienen configurado el registro de acceso. Este control falla si no se ha definido la configuración del registro de acceso.

Los registros de acceso a API Gateway proporcionan información detallada sobre quién ha obtenido acceso a la API y cómo la persona que llama ha obtenido acceso a la API. Estos registros son útiles

para aplicaciones como las auditorías de seguridad y acceso y la investigación forense. Habilite estos registros de acceso para analizar los patrones de tráfico y solucionar problemas.

Para obtener más información sobre las prácticas recomendadas, consulte Supervisión de las API de REST en la Guía para desarrolladores de API Gateway.

Corrección

Para configurar el registro de acceso, consulte Configurar el registro de CloudWatch API mediante la consola de API Gateway en la Guía para desarrolladores de API Gateway.

[APIGateway.10] Las integraciones de API Gateway V2 deben usar HTTPS para las conexiones privadas

Categoría: Proteger > Protección de datos > Cifrado de datos en tránsito

Gravedad: media

Tipo de recurso: `AWS::ApiGatewayV2::Integration`

Regla de AWS Config : apigatewayv2-integration-private-https-enabled

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una integración de API Gateway V2 tiene HTTPS habilitado para las conexiones privadas. El control falla si una conexión privada no tiene TLS configurado.

Los enlaces de VPC conectan API Gateway con recursos privados. Si bien los enlaces de VPC crean conectividad privada, no cifran los datos de forma inherente. La configuración de TLS garantiza el uso de HTTPS para el cifrado de extremo a extremo desde el cliente, pasando por API Gateway, hasta el backend. Sin TLS, el tráfico confidencial de la API fluye sin cifrar a través de conexiones privadas. El cifrado HTTPS protege el tráfico que pasa por las conexiones privadas frente a la interceptación de datos, los ataques interpersonales y la exposición de credenciales.

Corrección

Para habilitar el cifrado en tránsito para conexiones privadas en una integración de API Gateway v2, consulte Actualizar una integración privada en la Guía para desarrolladores de Amazon API

Gateway. Configure la configuración de TLS para que la integración privada utilice el protocolo HTTPS.

[APIGateway.11] Los nombres de dominio de API Gateway deben usar las políticas de seguridad recomendadas

Categoría: Proteger > Cifrado de datos en tránsito

Gravedad: media

Tipo de recurso: `AWS::ApiGateway::DomainName`

Regla de AWS Config : apigateway-domain-name-tls-check

Tipo de horario: provocado por un cambio

Parámetros:

- `allowedSecurityPolicies`: `SecurityPolicy_TLS13_1_3_2025_09`, `SecurityPolicy_TLS13_1_3_FIPS_2025_09`, `SecurityPolicy_TLS13_1_2_PFS_PQ_2025_09`, `SecurityPolicy_TLS13_2025_EDGE`, `SecurityPolicy_TLS12_PFS_2025_EDGE` (no personalizable)

Este control comprueba si un nombre de dominio de API Gateway está configurado para cifrar los datos en tránsito mediante una política de seguridad recomendada. El control falla si el nombre de dominio de API Gateway no está configurado para usar una política de seguridad recomendada.

Este control genera una `FAILED` búsqueda de los nombres de dominio personalizados que se adjuntan a las API HTTP. Si tiene un caso de uso legítimo para las API HTTP, puede suprimir el hallazgo.

Una política de seguridad es una combinación predefinida de versión mínima de TLS y conjuntos de cifrado que ofrece API Gateway. Cuando los clientes realizan un establecimiento de comunicación de TLS en la API o el nombre de dominio personalizado, la política de seguridad aplica la versión de TLS y el conjunto de cifrado aceptado por API Gateway. Las políticas de seguridad protegen las API y los nombres de dominio personalizados de los problemas de seguridad de red como, por ejemplo, la manipulación y el espionaje entre un cliente y el servidor. El uso de una política de seguridad recomendada ayuda a garantizar que los nombres de dominio de API Gateway utilicen configuraciones de TLS modernas y seguras que protejan los datos en tránsito entre los clientes y su API.

Corrección

Para actualizar la política de seguridad TLS de un nombre de dominio de API Gateway, consulte Cómo cambiar una política de seguridad en la Guía para desarrolladores de Amazon API Gateway.

Controles CSPM de Security Hub paraAWS AppConfig

Estos controles CSPM de Security Hub evalúan el AWS AppConfig servicio y los recursos.

Es posible que estos controles no estén disponibles en todos. Regiones de AWS Para obtener más información, consulte Disponibilidad de los controles por región.

[AppConfig.1]AWS AppConfiglas aplicaciones deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::AppConfig::Application`

Regla de AWS Config: `appconfig-application-tagged`

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredKeyTags`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si una AWS AppConfig aplicación tiene etiquetas con las claves específicas definidas en el parámetro`requiredKeyTags`. El control falla si la aplicación no tiene ninguna clave

de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredKeyTags`. Si no se proporciona el parámetro `requiredKeyTags`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si la aplicación no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte Definición de permisos basados en atributos con autorización ABAC en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte las mejores prácticas y estrategias en los AWSrecursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para añadir etiquetas a una AWS AppConfig aplicación, consulte la referencia TagResourcede la AWS AppConfigAPI.

[AppConfig.2]AWS AppConfiglos perfiles de configuración deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::AppConfig::ConfigurationProfile`

Regla de AWS Config: `appconfig-configuration-profile-tagged`

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredKeyTags`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si un perfil de AWS AppConfig configuración tiene etiquetas con las claves específicas definidas en el parámetro`requiredKeyTags`. El control falla si el perfil de configuración no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredKeyTags`. Si no se proporciona el parámetro `requiredKeyTags`, el control solo verifica la existencia de una clave de etiqueta y falla si el perfil de configuración no tiene ninguna clave de etiqueta. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para

obtener más información, consulte Definición de permisos basados en atributos con autorización ABAC en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte las mejores prácticas y estrategias en los AWSrecursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para añadir etiquetas a un perfil AWS AppConfig de configuración, consulte la referencia TagResourcede la AWS AppConfigAPI.

[AppConfig.3]AWS AppConfiglos entornos deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::AppConfig::Environment`

Regla de AWS Config: `appconfig-environment-tagged`

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredKeyTags`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los	Sin valor predeterminado

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
	de etiquetas distinguen entre mayúsculas y minúsculas.		requisitos de AWS.	

Este control comprueba si un AWS AppConfig entorno tiene etiquetas con las claves específicas definidas en el parámetro`requiredKeyTags`. El control falla si el entorno no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredKeyTags`. Si no se proporciona el parámetro `requiredKeyTags`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si el entorno no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte Definición de permisos basados en atributos con autorización ABAC en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte las mejores prácticas y estrategias en los AWSrecursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para añadir etiquetas a un AWS AppConfig entorno, consulta la referencia TagResourcede la AWS AppConfigAPI.

[AppConfig.4]AWS AppConfiglas asociaciones de extensiones deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::AppConfig::ExtensionAssociation`

Regla de AWS Config: `appconfig-extension-association-tagged`

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredKeyTags`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si una asociación de AWS AppConfig extensiones tiene etiquetas con las claves específicas definidas en el parámetro`requiredKeyTags`. El control falla si la asociación de extensión no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredKeyTags`. Si no se proporciona el parámetro `requiredKeyTags`, el control solo verifica la existencia de una clave de etiqueta y falla si la asociación de extensión no tiene ninguna clave de etiqueta. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte Definición de permisos basados en atributos con autorización ABAC en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte las mejores prácticas y estrategias en los AWSrecursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para añadir etiquetas a una asociación de AWS AppConfig extensiones, consulta la referencia TagResourcede la AWS AppConfigAPI.

Controles CSPM de Security Hub para Amazon AppFlow

Estos controles CSPM de Security Hub evalúan el AppFlow servicio y los recursos de Amazon.

Es posible que estos controles no estén disponibles en todos. Regiones de AWS Para obtener más información, consulte Disponibilidad de los controles por región.

[AppFlow.1] AppFlow Los flujos de Amazon deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::AppFlow::Flow`

Regla de AWS Config: `appflow-flow-tagged`

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredKeyTags`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si un AppFlow flujo de Amazon tiene etiquetas con las claves específicas definidas en el parámetro`requiredKeyTags`. El control falla si el flujo no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredKeyTags`. Si no se proporciona el parámetro `requiredKeyTags`, el control solo comprueba la existencia de una clave de etiqueta y falla si el flujo no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para

obtener más información, consulte Definición de permisos basados en atributos con autorización ABAC en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte las mejores prácticas y estrategias en los AWSrecursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para añadir etiquetas a un AppFlow flujo de Amazon, consulta Crear flujos en Amazon AppFlow en la Guía del AppFlow usuario de Amazon.

Controles CSPM de Security Hub paraAWS App Runner

Estos AWS Security Hub CSPM controles evalúan el AWS App Runner servicio y los recursos. Es posible que los controles no estén disponibles en todosRegiones de AWS. Para obtener más información, consulte Disponibilidad de los controles por región.

[AppRunner.1] Los servicios de App Runner deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::AppRunner::Service`

Regla de AWS Config: apprunner-service-tagged

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredKeyTags`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si un AWS App Runner servicio tiene etiquetas con las claves específicas definidas en el parámetro`requiredKeyTags`. El control falla si el servicio de App Runner no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredKeyTags`. Si no se proporciona el parámetro `requiredKeyTags`, el control solo comprueba la existencia de una clave de etiqueta y falla si el servicio de App Runner no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte Definición de permisos basados en atributos con autorización ABAC en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte las mejores prácticas y estrategias en los AWSrecursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para obtener información sobre cómo añadir etiquetas a un AWS App Runner servicio, consulta la referencia TagResourcede la AWS App RunnerAPI.

[AppRunner.2] Los conectores VPC de App Runner deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::AppRunner::VpcConnector`

Regla de AWS Config: apprunner-vpc-connector-tagged

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredKeyTags`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si un conector de AWS App Runner VPC tiene etiquetas con las claves específicas definidas en el parámetro. `requiredKeyTags` El control falla si el conector de VPC no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredKeyTags`. Si no se proporciona el parámetro `requiredKeyTags`, el control solo comprueba la existencia de una clave de etiqueta y falla si el conector de VPC no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte Definición de permisos basados en atributos con autorización ABAC en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte las mejores prácticas y estrategias en los AWSrecursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para obtener información sobre cómo añadir etiquetas a un conector de AWS App Runner VPC, consulte la referencia TagResourcede la AWS App RunnerAPI.

Controles CSPM de Security Hub paraAWS AppSync

Estos controles CSPM de Security Hub evalúan el AWS AppSync servicio y los recursos.

Es posible que estos controles no estén disponibles en todos. Regiones de AWS Para obtener más información, consulte Disponibilidad de los controles por región.

[AppSync.1]AWS AppSyncLas cachés de las API deben estar cifradas en reposo

> **Important**
>
> Security Hub CSPM retiró este control el 9 de marzo de 2026. Para obtener más información, consulte. Registro de cambios de los controles del CSPM de Security Hub AWS AppSyncahora proporciona cifrado predeterminado en todas las cachés de API actuales y futuras.

Categoría: Proteger > Protección de datos > Cifrado de datos en reposo

Gravedad: media

Tipo de recurso: `AWS::AppSync::GraphQLApi`

Regla de AWS Config: appsync-cache-ct-encryption-at-rest

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una caché de AWS AppSync API está cifrada en reposo. El control falla si la caché de la API no está cifrada en reposo.

Los datos en reposo hacen referencia a los datos que se almacenan en un almacenamiento persistente y no volátil durante cualquier periodo de tiempo. El cifrado de datos en reposo permite proteger la confidencialidad de los datos, lo que reduce el riesgo de que un usuario no autorizado pueda acceder a ellos.

Corrección

No puedes cambiar la configuración de cifrado después de habilitar el almacenamiento en caché para tu AWS AppSync API. En su lugar, debe eliminar la caché y volver a crearla con el cifrado habilitado. Para obtener más información, consulte Cifrado de caché, en la Guía para desarrolladores de AWS AppSync.

[AppSync.2]AWS AppSyncdebe tener habilitado el registro a nivel de campo

Requisitos relacionados: PCI DSS v4.0. 1/104.4.2

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: `AWS::AppSync::GraphQLApi`

Regla de AWS Config: `appsync-logging-enabled`

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`fieldLoggingLevel`	Nivel de registro del campo	Enum	`ERROR`, `ALL`, `INFO`, `DEBUG`	`No default value`

Este control comprueba si una AWS AppSync API tiene activado el registro a nivel de campo. Se produce un error en el control si el nivel de registro del solucionador de campos está establecido en Ninguno. A menos que proporcione valores de parámetros personalizados para indicar que se debe habilitar un tipo de registro específico, el CSPM de Security Hub produce una conclusión válida si el nivel de registro del solucionador de campos es o`ERROR`. `ALL`

Puede utilizar el registro y las métricas para identificar, solucionar problemas y optimizar sus consultas de GraphQL. Activar el registro en AWS AppSync GraphQL te ayuda a obtener información detallada sobre las solicitudes y respuestas de la API, a identificar y responder a los problemas y a cumplir con los requisitos reglamentarios.

Corrección

Para activar el registroAWS AppSync, consulta Instalación y configuración en la Guía para AWS AppSync desarrolladores.

[AppSync.4]AWS AppSyncLas API de GraphQL deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::AppSync::GraphQLApi`

AWS Configregla: `tagged-appsync-graphqlapi` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si una API de AWS AppSync GraphQL tiene etiquetas con las claves específicas definidas en el parámetro. `requiredTagKeys` El control falla si la API de GraphQL no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si la API de GraphQL no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El

etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte Etiquetar sus AWS recursos en el. Referencia general de AWS

Corrección

Para añadir etiquetas a una API de AWS AppSync GraphQL, consulta la referencia TagResourcede la AWS AppSyncAPI.

[AppSync.5]AWS AppSyncLas API de GraphQL no deben autenticarse con claves de API

Requisitos relacionados: NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-6

Categoría: Proteger > Gestión del acceso seguro > Autenticación sin contraseña

Gravedad: alta

Tipo de recurso: `AWS::AppSync::GraphQLApi`

Regla de AWS Config: `appsync-authorization-check`

Tipo de horario: provocado por un cambio

Parámetros:

- `AllowedAuthorizationTypes: AWS_LAMBDA,AWS_IAM, OPENID_CONNECT, AMAZON_COGNITO_USER_POOLS` (no personalizable)

Este control comprueba si la aplicación utiliza una clave de API para interactuar con una API de AWS AppSync GraphQL. El control falla si una API de AWS AppSync GraphQL se autentica con una clave de API.

Una clave de API es un valor codificado en tu aplicación que genera el AWS AppSync servicio al crear un punto final de GraphQL no autenticado. Si esta clave de API se ve comprometida, su punto de conexión es vulnerable a un acceso no deseado. A menos que respalde una aplicación o un sitio web de acceso público, no recomendamos usar una clave de API para la autenticación.

Corrección

Para configurar una opción de autorización para tu API de AWS AppSync GraphQL, consulta Autorización y autenticación en la Guía para AWS AppSyncdesarrolladores.

[AppSync.6]AWS AppSyncLas cachés de las API deben cifrarse en tránsito

> **Important**
>
> Security Hub CSPM retiró este control el 9 de marzo de 2026. Para obtener más información, consulte. Registro de cambios de los controles del CSPM de Security Hub AWS AppSyncahora proporciona cifrado predeterminado en todas las cachés de API actuales y futuras.

Categoría: Proteger > Protección de datos > Cifrado de datos en tránsito

Gravedad: media

Tipo de recurso: `AWS::AppSync::ApiCache`

Regla de AWS Config: appsync-cache-ct-encryption-in-transit

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una caché de AWS AppSync API está cifrada en tránsito. El control falla si la caché de la API no está cifrada en tránsito.

Los datos en tránsito hacen referencia a los datos que se mueven de una ubicación a otra, por ejemplo, entre los nodos del clúster o entre el clúster y la aplicación. Los datos pueden moverse a

través de Internet o dentro de una red privada. El cifrado de los datos en tránsito reduce el riesgo de que un usuario no autorizado pueda espiar el tráfico de la red.

Corrección

No puedes cambiar la configuración de cifrado después de habilitar el almacenamiento en caché para tu AWS AppSync API. En su lugar, debe eliminar la caché y volver a crearla con el cifrado habilitado. Para obtener más información, consulte Cifrado de caché, en la Guía para desarrolladores de AWS AppSync.

Controles CSPM de Security Hub para Amazon Athena

Estos AWS Security Hub CSPM controles evalúan el servicio y los recursos de Amazon Athena. Es posible que los controles no estén disponibles en todosRegiones de AWS. Para obtener más información, consulte Disponibilidad de los controles por región.

[Athena.1] Los grupos de trabajo de Athena deben estar cifrados en reposo

> **Important**
>
> Security Hub CSPM retiró este control en abril de 2024. Para obtener más información, consulte Registro de cambios de los controles del CSPM de Security Hub.

Categoría: Proteger - Protección de datos - Cifrado de datos en reposo

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6)

Gravedad: media

Tipo de recurso: `AWS::Athena::WorkGroup`

Regla de AWS Config: athena-workgroup-encrypted-at-rest

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un grupo de trabajo de Athena está cifrado en reposo. El control falla si un grupo de trabajo de Athena no está cifrado en reposo.

En Athena, puede crear grupos de trabajo para ejecutar consultas para equipos, aplicaciones o diferentes cargas de trabajo. Cada grupo de trabajo tiene una configuración que permite el cifrado de todas las consultas. Tiene la opción de utilizar el cifrado del lado del servidor con las claves administradas por Amazon Simple Storage Service (Amazon S3), el cifrado del lado del servidor con claves AWS Key Management Service (AWS KMS) o el cifrado del lado del cliente con claves de KMS administradas por el cliente. Los datos en reposo se refieren a cualquier dato que se almacene en un almacenamiento persistente y no volátil durante cualquier período de tiempo. El cifrado le ayuda a proteger la confidencialidad de dichos datos, reduciendo el riesgo de que un usuario no autorizado pueda acceder a ellos.

Corrección

Para habilitar el cifrado en reposo para los grupos de trabajo de Athena, consulte Editar un grupo de trabajo en la Guía del usuario de Amazon Athena. En la sección Configuración de los resultados de la consulta, seleccione Cifrar los resultados de la consulta.

[Athena.2] Los catálogos de datos de Athena deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::Athena::DataCatalog`

AWS Configregla: `tagged-athena-datacatalog` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que	`No default value`

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
	recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.		cumplan los requisitos de AWS.	

Este control comprueba si el catálogo de datos de Amazon Athena tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control falla si el catálogo de datos no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si el catálogo de datos no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte Etiquetar sus AWS recursos en el. Referencia general de AWS

Corrección

Para agregar etiquetas a un catálogo de datos de Athena, consulte Etiquetado de los recursos de Athena en la Guía del usuario de Amazon Athena.

[Athena.3] Los grupos de trabajo de Athena deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::Athena::WorkGroup`

AWS Configregla: `tagged-athena-workgroup` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	`No default value`

Este control comprueba si el grupo de trabajo de Amazon Athena tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control falla si el grupo de trabajo no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si el grupo de trabajo no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte Etiquetar sus AWS recursos en el. Referencia general de AWS

Corrección

Para agregar etiquetas a un grupo de trabajo de Athena, consulte Agregar y eliminar etiquetas en un grupo de trabajo individual en la Guía del usuario de Amazon Athena.

[Athena.4] Los grupos de trabajo de Athena deberían tener habilitado el registro

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: `AWS::Athena::WorkGroup`

Regla de AWS Config: athena-workgroup-logging-enabled

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un grupo de trabajo de Amazon Athena tiene el registro habilitado. El control falla si el grupo de trabajo no tiene el registro habilitado.

Los registros de auditoría rastrean y supervisan las actividades del sistema. Proporcionan un registro de los eventos que puede ayudarlo a detectar brechas de seguridad, investigar incidentes y cumplir con las normativas. Los registros de auditoría también mejoran la responsabilidad y la transparencia generales de su organización.

Corrección

Para obtener información sobre cómo habilitar el registro para un grupo de trabajo de Athena, consulte Habilitar las métricas de CloudWatch consulta en Athena en la Guía del usuario de Amazon Athena.

Controles CSPM de Security Hub paraAWS Backup

Estos controles CSPM de Security Hub evalúan el AWS Backup servicio y los recursos.

Es posible que estos controles no estén disponibles en todos. Regiones de AWS Para obtener más información, consulte Disponibilidad de los controles por región.

[Backup.1]AWS Backuplos puntos de recuperación deben estar cifrados en reposo

Requisitos relacionados: NIST.800-53.r5 CP-9 (8), NIST.800-53.r5 SI-12

Categoría: Proteger > Protección de datos > Cifrado de datos en reposo

Gravedad: media

Tipo de recurso: `AWS::Backup::RecoveryPoint`

Regla de AWS Config: `backup-recovery-point-encrypted`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un punto AWS Backup de recuperación está cifrado en reposo. Se produce un error en el control si el punto de recuperación no está cifrado en reposo.

Un punto de AWS Backup recuperación hace referencia a una copia o instantánea específica de los datos que se crea como parte de un proceso de copia de seguridad. Representa un momento concreto en el que se hizo una copia de seguridad de los datos y sirve como punto de restauración en caso de que los datos originales se pierdan, se dañen o sean inaccesibles. El cifrado de los

puntos de recuperación de la copia de seguridad agrega una capa adicional de protección contra el acceso no autorizado. El cifrado es la práctica recomendada para proteger la confidencialidad, la integridad y la seguridad de los datos de la copia de seguridad.

Corrección

Para cifrar un punto de AWS Backup recuperación, consulte Cifrado de copias de seguridad AWS Backup en la Guía para AWS Backup desarrolladores.

[Backup.2]AWS Backuplos puntos de recuperación deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::Backup::RecoveryPoint`

AWS Configregla: `tagged-backup-recoverypoint` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si un punto de AWS Backup recuperación tiene etiquetas con las claves específicas definidas en el parámetro`requiredTagKeys`. El control lanza error si el punto de

recuperación no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si el punto de recuperación no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte Etiquetar sus AWS recursos en el. Referencia general de AWS

Corrección

Para copiar etiquetas de los recursos fuente en el momento de crear la copia de seguridad, consulte Copiar etiquetas en las copias de seguridad en la Guía AWS Backuppara desarrolladores.

Las etiquetas no se copian en el momento de la creación para los puntos de parent/composite recuperación. Para añadir etiquetas a los puntos de recuperación existentes, incluidos los puntos de parent/composite recuperación, consulte Añadir o eliminar etiquetas en los puntos de recuperación existentes en la Guía para AWS Backup desarrolladores.

[Backup.3]AWS Backuplas bóvedas deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::Backup::BackupVault`

AWS Configregla: `tagged-backup-backupvault` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si una AWS Backup bóveda tiene etiquetas con las claves específicas definidas en el parámetro`requiredTagKeys`. El control lanza error si el punto de recuperación no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si el punto de recuperación no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS

los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte Etiquetar sus AWS recursos en el. Referencia general de AWS

Corrección

Para añadir etiquetas a unAWS Backupalmacén

1. Abra la AWS Backup consola en https://console.aws.amazon.com/backup.
2. En el panel de navegación, elija Backup vaults (Almacenes de copia de seguridad).
3. Seleccione un almacén de copias de seguridad de la lista.
4. En la sección Etiquetas del almacén de copias de seguridad, elija Administrar etiquetas.
5. Escriba la clave y el valor de para la etiqueta. Seleccione Agregar etiqueta nueva para agregar pares de clave-valor adicionales.
6. Cuando haya terminado de agregar etiquetas, elija Save (Guardar).

[Backup.4]AWS Backuplos planes de informes deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::Backup::ReportPlan`

AWS Configregla: `tagged-backup-reportplan` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si un plan de AWS Backup informes tiene etiquetas con las claves específicas definidas en el parámetro`requiredTagKeys`. El control lanza error si el plan de informes no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si el plan de informes no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte Etiquetar sus AWS recursos en el. Referencia general de AWS

Corrección

Para añadir etiquetas a unAWS Backupplan de informes

1. Abra la AWS Backup consola en https://console.aws.amazon.com/backup.
2. En el panel de navegación, elija Backup vaults (Almacenes de copia de seguridad).
3. Seleccione un almacén de copias de seguridad de la lista.
4. En la sección Etiquetas del almacén de copias de seguridad, elija Administrar etiquetas.
5. Elija Añadir nueva etiqueta. Escriba la clave y el valor de para la etiqueta. Repita la acción para pares de clave-valor adicionales.
6. Cuando haya terminado de agregar etiquetas, elija Save (Guardar).

[Backup.5]AWS Backuplos planes de respaldo deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::Backup::BackupPlan`

AWS Configregla: `tagged-backup-backupplan` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si un plan AWS Backup de respaldo tiene etiquetas con las claves específicas definidas en el parámetro`requiredTagKeys`. El control lanza error si el plan de copias de seguridad no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si el plan de copias de seguridad no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte Etiquetar sus AWS recursos en el. Referencia general de AWS

Corrección

Para añadir etiquetas a unAWS Backupplan de respaldo

1. Abra la AWS Backup consola en https://console.aws.amazon.com/backup.
2. En el panel de navegación, elija Backup vaults (Almacenes de copia de seguridad).
3. Seleccione un almacén de copias de seguridad de la lista.
4. En la sección Etiquetas del almacén de copias de seguridad, elija Administrar etiquetas.
5. Elija Añadir nueva etiqueta. Escriba la clave y el valor de para la etiqueta. Repita la acción para pares de clave-valor adicionales.
6. Cuando haya terminado de agregar etiquetas, elija Save (Guardar).

Controles CSPM de Security Hub paraAWS Batch

Estos controles CSPM de Security Hub evalúan el AWS Batch servicio y los recursos. Es posible que los controles no estén disponibles en todos. Regiones de AWS Para obtener más información, consulte Disponibilidad de los controles por región.

[Batch.1] Las colas de trabajos por lotes deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::Batch::JobQueue`

Regla de AWS Config: batch-job-queue-tagged

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredKeyTags`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si una cola de AWS Batch trabajos tiene etiquetas con las claves específicas definidas en el parámetro`requiredKeyTags`. El control falla si la cola de trabajo no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredKeyTags`. Si no se proporciona el parámetro `requiredKeyTags`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si la cola de trabajo no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte Definición de permisos basados en atributos con autorización ABAC en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte las mejores prácticas y estrategias en los AWSrecursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para agregar etiquetas a una cola de trabajos de Batch, consulte Etiquetar los recursos en la Guía del usuario de AWS Batch.

[Batch.2] Las políticas de programación de lotes deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::Batch::SchedulingPolicy`

Regla de AWS Config: batch-scheduling-policy-tagged

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredKeyTags`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si una política de AWS Batch programación tiene etiquetas con las claves específicas definidas en el parámetro`requiredKeyTags`. El control lanza un error si la política de programación no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredKeyTags`. Si no se proporciona el parámetro `requiredKeyTags`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si la política de programación no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte Definición de permisos basados en atributos con autorización ABAC en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte las mejores prácticas y estrategias en los AWSrecursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para agregar etiquetas a una política de programación de Batch, consulte Etiquetado de los recursos en la Guía del usuario de AWS Batch.

[Batch.3] Los entornos de procesamiento por lotes deben etiquetarse

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::Batch::ComputeEnvironment`

Regla de AWS Config: batch-compute-environment-tagged

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredKeyTags`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si un entorno AWS Batch informático tiene etiquetas con las claves específicas definidas en el parámetro`requiredKeyTags`. El control falla si el entorno de computación no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredKeyTags`. Si no se proporciona el parámetro `requiredKeyTags`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si el entorno de computación no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS

los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte Definición de permisos basados en atributos con autorización ABAC en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte las mejores prácticas y estrategias en los AWSrecursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para agregar etiquetas a un entorno de computación de Batch, consulte Etiquetado de los recursos en la Guía del usuario de AWS Batch.

[Batch.4] Las propiedades de los recursos de cómputo en los entornos de cómputo por lotes gestionados deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::Batch::ComputeEnvironment`

Regla de AWS Config: batch-managed-compute-env-compute-resources-tagged

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredKeyTags`	Una lista de claves de etiqueta que no son del sistema y que se deben asignar a un recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si la propiedad de recursos de computación en un entorno de computación administrado de AWS Batch tiene las claves de etiqueta especificadas por el parámetro `requiredKeyTags`. El control falla si la propiedad recursos de computación no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredKeyTags`. Si no especifica ningún valor para el parámetro `requiredKeyTags`, el control solo comprueba la existencia de una clave de etiqueta y falla si la propiedad de recursos de computación no tiene ninguna clave de etiqueta. El control ignora las etiquetas del sistema, que se aplican automáticamente y tienen el prefijo `aws:`. Este control no evalúa los entornos informáticos no gestionados ni los entornos gestionados que utilizan AWS Fargate recursos.

Una etiqueta es una etiqueta que se crea y se asigna a un AWS recurso. Cada etiqueta consta de una clave de etiqueta necesaria y un valor de etiqueta opcional. Utilice etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. También pueden ayudar a identificar, organizar, buscar y filtrar recursos. También pueden ayudar a rastrear propietarios de recursos para acciones y notificaciones. También puede usar etiquetas para implementar control de acceso basado en atributos (ABAC) como estrategia de autorización. Para obtener más información sobre estrategias ABAC, consulte Definición de permisos basados en atributos con autorización ABAC en la Guía del usuario de IAM. Para obtener más información sobre las etiquetas, consulte los AWSrecursos de etiquetado y la Guía del usuario del editor de etiquetas.

> **Note**
>
> No almacene información de identificación personal (PII) ni otra información confidencial en las etiquetas. Se puede acceder a las etiquetas desde muchos Servicios de AWS sitios. No están destinadas a usarse para datos privados o información confidencial.

Corrección

Para obtener información sobre cómo añadir etiquetas a los recursos informáticos en un entorno AWS Batch informático gestionado, consulte Etiquetar los recursos en la Guía del AWS Batch usuario.

Controles CSPM de Security Hub para Amazon Bedrock

Estos AWS Security Hub CSPM controles evalúan el servicio y los recursos de Amazon Bedrock. Es posible que los controles no estén disponibles en todosRegiones de AWS. Para obtener más información, consulte Disponibilidad de los controles por región.

[Bedrock.1] Las fuentes de datos de Amazon Bedrock deben cifrarse de forma gestionada por el clienteAWS KMSclaves

Categoría: Proteger - Protección de datos - Cifrado de datos en reposo

Gravedad: media

Tipo de recurso: `AWS::Bedrock::DataSource`

Regla de AWS Config: bedrock-data-source-encryption-enabled

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una fuente de datos de Amazon Bedrock está cifrada en reposo con una AWS KMS clave gestionada por el cliente. El control falla si la fuente de datos no está cifrada con una clave KMS administrada por el cliente.

De forma predeterminada, Amazon Bedrock cifra el contenido de la fuente de datos con claves AWS administradas. El uso de una clave KMS administrada por el cliente le brinda un control total sobre

el ciclo de vida de la clave de cifrado, incluida la rotación, las políticas de acceso y la auditoría. AWS CloudTrail Esto ayuda a cumplir con los requisitos de conformidad que exigen el cifrado controlado por el cliente para los datos confidenciales introducidos en las bases de conocimiento.

Corrección

Para cifrar su fuente de datos de Amazon Bedrock con una clave de KMS gestionada por el cliente, consulte Modificar una fuente de datos para su base de conocimientos de Amazon Bedrock en la Guía del usuario de Amazon Bedrock.

Controles CSPM de Security Hub para Amazon Bedrock AgentCore

Estos AWS Security Hub CSPM controles evalúan el AgentCore servicio y los recursos de Amazon Bedrock. Es posible que los controles no estén disponibles en todosRegiones de AWS. Para obtener más información, consulte Disponibilidad de los controles por región.

[BedrockAgentCore.1] Los AgentCore tiempos de ejecución de Bedrock deben configurarse con el modo de red VPC

Categoría: Proteger > Gestión del acceso seguro > Recurso no accesible públicamente

Gravedad: alta

Tipo de recurso: `AWS::BedrockAgentCore::Runtime`

Regla de AWS Config: bedrockagentcore-runtime-private-network-required

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un entorno de AgentCore ejecución de Amazon Bedrock está configurado con el modo de red VPC. El control falla si el modo de red del motor de ejecución está establecido en PUBLIC.

El uso del modo de red pública para los AgentCore tiempos de ejecución de Amazon Bedrock expone el tiempo de ejecución directamente a Internet, lo que aumenta la superficie de ataque y el riesgo de acceso no autorizado. La configuración de los tiempos de ejecución con el modo de red de VPC garantiza que el tráfico en tiempo de ejecución se limite a su red privada, lo que le permite aplicar controles de seguridad a nivel de red, como grupos de seguridad, ACL de red y registros de flujo de VPC.

Corrección

Para solucionar este problema, actualiza el tiempo de AgentCore ejecución de Bedrock que no es compatible y configúralo con el modo de red de VPC. Para obtener instrucciones, consulte Configurar el tiempo de AgentCore ejecución y las herramientas de Amazon Bedrock para VPC en la Guía para desarrolladores de Amazon AgentCore Bedrock.

[BedrockAgentCore.2] Bedrock AgentCore Gateways debería requerir autorización para las solicitudes entrantes

Categoría: Proteger - Administración de acceso seguro

Gravedad: alta

Tipo de recurso: `AWS::BedrockAgentCore::Gateway`

Regla de AWS Config: bedrockagentcore-gateway-authorizer-enabled

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si Amazon Bedrock AgentCore Gateway requiere autorización para las solicitudes entrantes. El control falla si Bedrock AgentCore Gateway no tiene configurada la autorización de entrada.

La configuración de la autenticación en AgentCore las pasarelas de Amazon Bedrock garantiza que solo los clientes autorizados puedan enviar solicitudes a sus agentes de IA. Sin un autorizador, cualquier entidad con acceso de red al punto final de la puerta de enlace puede recurrir a sus agentes, lo que podría provocar un acceso no autorizado a los datos, un uso indebido de los recursos o costes inesperados. La autorización entrante valida a los usuarios que intentan acceder a los objetivos a través de su puerta de enlace. AgentCore

Corrección

Para configurar la autorización de AgentCore entrada para una puerta de enlace de Amazon Bedrock, consulte Configurar la autorización de entrada para una puerta de enlace en la Guía para desarrolladores de Amazon Bedrock AgentCore .

[BedrockAgentCore.3] Bedrock AgentCore Memory debe estar cifrada y gestionada por el clienteAWS KMSclaves

Requisitos relacionados: NIST.800-53.r5 AU-9 NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SC-12 (2), NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SI-7 (6)

Categoría: Proteger - Protección de datos - Cifrado de datos en reposo

Gravedad: media

Tipo de recurso: `AWS::BedrockAgentCore::Memory`

Regla de AWS Config: bedrock-agentcore-memory-encryption-enabled

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una AgentCore memoria Amazon Bedrock está cifrada en reposo con una AWS KMS clave gestionada por el cliente. El control falla si la AgentCore memoria Bedrock no está cifrada con una clave KMS administrada por el cliente.

El uso de una clave de KMS gestionada por el cliente para el cifrado de la AgentCore memoria de Amazon Bedrock proporciona una seguridad mejorada con respecto a la clave gestionada por el servicio predeterminada. Las claves KMS administradas por el cliente le proporcionan un control total sobre el ciclo de vida de las claves de cifrado y las políticas de acceso. Además, todo el uso de claves de cifrado se puede registrar y supervisar AWS CloudTrail para garantizar su auditabilidad.

Corrección

Para cifrar la AgentCore memoria de Amazon Bedrock con una clave de KMS gestionada por el cliente, consulte Cifrar la memoria de Amazon Bedrock AgentCore en la Guía para desarrolladores de Amazon Bedrock. AgentCore

[BedrockAgentCore.4] Bedrock AgentCore Gateway debe cifrarse de forma que sea gestionada por el clienteAWS KMSclaves

Requisitos relacionados: NIST.800-53.r5 AU-9 NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SC-12 (2), NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SI-7 (6)

Categoría: Proteger - Protección de datos - Cifrado de datos en reposo

Gravedad: media

Tipo de recurso: `AWS::BedrockAgentCore::Gateway`

Regla de AWS Config: bedrockagentcore-gateway-encryption-enabled

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una AgentCore puerta de enlace de Amazon Bedrock está cifrada en reposo con una AWS KMS clave gestionada por el cliente. El control falla si el Bedrock AgentCore Gateway no está cifrado con una clave KMS administrada por el cliente.

De forma predeterminada, Amazon Bedrock AgentCore cifra los datos de la puerta de enlace con claves AWS gestionadas. El uso de una clave KMS gestionada por el cliente le proporciona un control total sobre el ciclo de vida de la clave de cifrado, incluida la rotación, las políticas de acceso y la auditoría. AWS CloudTrail Esto ayuda a cumplir los requisitos de conformidad que exigen el cifrado controlado por el cliente para las cargas de trabajo de IA confidenciales.

Corrección

Para cifrar su AgentCore puerta de enlace de Bedrock con una clave de KMS administrada por el cliente, consulte Cifrar su AgentCore puerta de enlace con una clave de KMS administrada por el cliente en la Guía para desarrolladores de Amazon Bedrock. AgentCore

[BedrockAgentCore.5] Los navegadores AgentCore personalizados de Bedrock no deberían usar el modo de red pública

Categoría: Proteger > Configuración de red segura > Recursos dentro de VPC

Gravedad: alta

Tipo de recurso: `AWS::BedrockAgentCore::BrowserCustom`

Regla de AWS Config: bedrockagentcore-browsercustom-network-mode-not-public

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un navegador AgentCore personalizado de Amazon Bedrock está configurado con el modo de red pública. El control falla si el modo de red está configurado como público.

El uso del modo de red PÚBLICA para los navegadores AgentCore personalizados de Amazon Bedrock expone las sesiones del navegador directamente a Internet, lo que aumenta la superficie de ataque y el riesgo de acceso no autorizado. La configuración de los navegadores con el modo de red de VPC garantiza que el tráfico del navegador se limite a su red privada, lo que le permite aplicar controles de seguridad a nivel de red, como grupos de seguridad, ACL de red y registros de flujo de VPC.

Corrección

Para solucionar este problema, elimine el navegador AgentCore personalizado Bedrock que no cumple con las normas y vuelva a crearlo con el modo de red VPC. Para obtener instrucciones, consulte Configurar el tiempo de AgentCore ejecución y las herramientas de Amazon Bedrock para VPC en la Guía para desarrolladores de Amazon AgentCore Bedrock.

[BedrockAgentCore.6] Los navegadores AgentCore personalizados de Bedrock deberían tener habilitada la grabación de sesiones

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: `AWS::BedrockAgentCore::BrowserCustom`

Regla de AWS Config: bedrockagentcore-browsercustom-recording-enabled

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un navegador AgentCore personalizado de Amazon Bedrock tiene habilitada la grabación de sesiones con un destino S3 configurado. El control falla si un navegador personalizado no tiene habilitada la grabación o no tiene una ubicación S3 configurada para almacenar las grabaciones.

La grabación de sesiones para los navegadores AgentCore personalizados de Bedrock garantiza la total auditabilidad de las interacciones del navegador, lo que permite detectar el acceso no autorizado, la exfiltración de datos o la actividad maliciosa durante las sesiones de navegación automatizadas.

Corrección

Para obtener instrucciones sobre cómo habilitar la grabación de sesiones del navegador, consulte Grabación y reproducción de sesiones en la Guía para AgentCore desarrolladores de Amazon Bedrock.

[BedrockAgentCore.7] Los intérpretes de código AgentCore personalizados de Bedrock deben usar una configuración de red privada

Categoría: Proteger > Configuración de red segura > Recursos dentro de VPC

Gravedad: alta

Tipo de recurso: `AWS::BedrockAgentCore::CodeInterpreterCustom`

Regla de AWS Config: bedrockagentcore-codeinterpreter-networkmode-check

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un intérprete de código AgentCore personalizado de Amazon Bedrock está configurado con un modo de red privada. El control falla si el modo de red está configurado en `PUBLIC` o`SANDBOX`.

La configuración de los intérpretes de código AgentCore personalizados de Bedrock con un modo de red privada garantiza que los entornos de ejecución de código estén aislados dentro de la VPC. Los modos de red pública o aislada exponen al intérprete de código a Internet, lo que aumenta el riesgo de acceso no autorizado y exfiltración de datos. El uso del modo de red privada restringe el acceso a la red y ayuda a proteger los datos confidenciales procesados durante la interpretación del código.

Corrección

Para solucionar este problema, elimine el intérprete de código AgentCore personalizado Bedrock que no cumple las normas y vuelva a crearlo con el modo de red VPC. Para obtener instrucciones, consulte Configuración del acceso a la VPC para el tiempo de ejecución y las herramientas en la Guía para desarrolladores de Amazon Bedrock AgentCore .

Controles CSPM de Security Hub paraAWS Gestor de certificados

Estos AWS Security Hub CSPM controles evalúan el servicio y los recursos AWS Gestor de certificados (ACM). Es posible que los controles no estén disponibles en todosRegiones de AWS. Para obtener más información, consulte Disponibilidad de los controles por región.

[ACM.1] ACM-issued Los certificados importados y renovados deben renovarse después de un período de tiempo específico

Requisitos relacionados: NIST.800-53.r5 SC-28 (3), NIST.800-53.r5 SC-7 (16), NIST.800-171.r2 3.13.15, PCI DSS v4.0. 1/42.2.1

Categoría: Proteger > Protección de datos > Cifrado de datos en tránsito

Gravedad: media

Tipo de recurso: `AWS::ACM::Certificate`

Regla de AWS Config: acm-certificate-expiration-check

Tipo de programa: activado por cambios y periódico

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`daysToExpiration`	Número de días en los que se debe renovar el certificado de ACM	Entero	De `14` a `365`	`30`

Este control comprueba si un certificado AWS Gestor de certificados (ACM) se renueva dentro del período de tiempo especificado. Comprueba tanto los certificados importados como los certificados que proporciona ACM. Se produce un error en el control si el certificado no se renueva en el periodo especificado. A menos que proporciones un valor de parámetro personalizado para el período de renovación, Security Hub CSPM utiliza un valor predeterminado de 30 días.

ACM puede renovar automáticamente los certificados que utilizan la validación de DNS. En el caso de los certificados que utilizan la validación por correo electrónico, debe responder a un correo electrónico de validación de dominio. ACM no renueva automáticamente los certificados que se importan. Debe renovar los certificados importados manualmente.

Corrección

ACM ofrece la renovación gestionada de sus SSL/TLS certificados emitidos por Amazon. Esto significa que ACM renueva sus certificados de forma automática (si utiliza la validación por DNS) o le envía avisos por correo electrónico cuando se acerque la fecha de vencimiento. Estos servicios se prestan tanto para certificados de ACM públicos como privados.

Para dominios validados por correo electrónico

Cuando un certificado expira 45 días, ACM envía al propietario del dominio un correo electrónico para cada nombre de dominio. Para validar los dominios y completar la renovación, debe responder a las notificaciones por correo electrónico.

Para obtener más información, consulte Renovación de dominios validados por correo electrónico en la Guía del usuario de AWS Gestor de certificados.

Para dominios validados por DNS

ACM renueva automáticamente los certificados que utilizan la validación de DNS. 60 días antes del vencimiento, ACM verifica que el certificado se pueda renovar.

Si no puede validar un nombre de dominio, ACM envía una notificación indicando que es necesaria la validación manual. Envía estas notificaciones 45 días, 30 días, 7 días y 1 día antes de la fecha de vencimiento.

Para obtener más información, consulte Renovación de dominios validados por DNS en la AWS Gestor de certificados Guía del usuario de .

[ACM.2] Los certificados RSA gestionados por ACM deben utilizar una longitud de clave de al menos 2048 bits

Requisitos relacionados: PCI DSS v4.0. 1/42.2.1

Categoría: Identificar > Inventario > Servicios de inventario

Gravedad: alta

Tipo de recurso: `AWS::ACM::Certificate`

Regla de AWS Config: acm-certificate-rsa-check

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si los certificados RSA gestionados AWS Gestor de certificados utilizan una longitud de clave de al menos 2048 bits. El control falla si la longitud de la clave es inferior a 2048 bits.

La fuerza del cifrado se correlaciona directamente con el tamaño de la clave. Recomendamos una longitud de clave de al menos 2048 bits para proteger sus AWS recursos, ya que la potencia de cálculo se abarata y los servidores se vuelven más avanzados.

Corrección

La longitud mínima de clave para los certificados RSA emitidos por ACM ya es de 2048 bits. Para obtener instrucciones sobre cómo emitir nuevos certificados RSA con ACM, consulte Emisión y administración de certificados en la Guía del usuario de AWS Gestor de certificados.

Si bien ACM le permite importar certificados con longitudes de clave más cortas, debe utilizar claves de al menos 2048 bits para pasar este control. No se puede cambiar la longitud de la clave después de importar un certificado. En su lugar, debe eliminar los certificados con una longitud de clave inferior a 2048 bits. Para obtener más información sobre la importación de certificados en ACM, consulte Prerrequisitos para importar certificados en la Guía del usuario de AWS Gestor de certificados.

[ACM.3] Los certificados ACM deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::ACM::Certificate`

AWS Configregla: `tagged-acm-certificate` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si un certificado AWS Gestor de certificados (ACM) tiene etiquetas con las claves específicas definidas en el parámetro`requiredTagKeys`. El control falla si el certificado no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y falla si el certificado no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, incluidasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte Etiquetar sus AWS recursos en el. Referencia general de AWS

Corrección

Para añadir etiquetas a un certificado ACM, consulte Etiquetado de AWS Gestor de certificados certificados en la Guía del usuario. AWS Gestor de certificados

Controles CSPM de Security Hub paraCloudFormation

Estos controles CSPM de Security Hub evalúan el AWS CloudFormation servicio y los recursos.

Es posible que estos controles no estén disponibles en todos. Regiones de AWS Para obtener más información, consulte Disponibilidad de los controles por región.

[CloudFormation.1] las CloudFormation pilas deben integrarse con Simple Notification Service (SNS)

> **Important**
>
> Security Hub CSPM retiró este control en abril de 2024. Para obtener más información, consulte Registro de cambios de los controles del CSPM de Security Hub.

Requisitos relacionados: NIST.800-53.r5 SI-4 (12), NIST.800-53.r5 SI-4 (5)

Categoría: Detectar > Servicios de detección > Supervisión de aplicaciones

Gravedad: baja

Tipo de recurso: `AWS::CloudFormation::Stack`

Regla de AWS Config: `cloudformation-stack-notification-check`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una notificación de Amazon Simple Notification Service está integrada con una pila de CloudFormation. El control de una CloudFormation pila falla si no hay ninguna notificación de SNS asociada a ella.

La configuración de una notificación de SNS con su CloudFormation pila ayuda a notificar inmediatamente a las partes interesadas cualquier evento o cambio que se produzca en la pila.

Corrección

Para integrar una CloudFormation pila y un tema de SNS, consulte Actualización de pilas directamente en la Guía del AWS CloudFormation usuario.

[CloudFormation.2] las CloudFormation pilas deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::CloudFormation::Stack`

AWS Configregla: `tagged-cloudformation-stack` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si una AWS CloudFormation pila tiene etiquetas con las claves específicas definidas en el parámetro`requiredTagKeys`. El control lanza error si la pila no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si la pila no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte Etiquetar sus AWS recursos en el. Referencia general de AWS

Corrección

Para añadir etiquetas a una CloudFormation pila, consulta la referencia CreateStackde la AWS CloudFormationAPI.

[CloudFormation.3] las CloudFormation pilas deben tener habilitada la protección de terminación

Categoría: Proteger > Protección de datos > Protección contra la eliminación de datos

Gravedad: media

Tipo de recurso: `AWS::CloudFormation::Stack`

Regla de AWS Config: cloudformation-termination-protection-check

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una AWS CloudFormation pila tiene habilitada la protección de terminación. El control falla si la protección de terminación no está habilitada en una CloudFormation pila.

CloudFormation ayuda a gestionar los recursos relacionados como una sola unidad denominada pila. Es posible evitar que una pila se elimine de manera accidental; para ello, habilite la protección de terminación en la pila. Si un usuario intenta eliminar una pila con la protección de terminación habilitada, la eliminación fallará y la pila junto con su estado no cambiarán. Puede configurar la protección de terminación en una pila con cualquier estado excepto `DELETE_IN_PROGRESS` o `DELETE_COMPLETE`.

> **Note**
>
> Al habilitar o deshabilitar la protección de terminación en una pila, también se habilita o deshabilita en las pilas anidadas. No se puede habilitar o deshabilitar la protección de terminación directamente en una pila anidada. No puedes eliminar directamente una pila anidada que pertenezca a una pila que tenga habilitada la protección de terminación. Si aparece el texto NESTED junto al nombre de la pila, es una pila anidada. Solo es posible cambiar la protección de terminación de la pila raíz a la que pertenece la pila anidada.

Corrección

Para habilitar la protección de terminación en una CloudFormation pila, consulte Proteger las CloudFormation pilas para que no se eliminen en la Guía del AWS CloudFormationusuario.

[CloudFormation.4] las CloudFormation pilas deben tener funciones de servicio asociadas

Categoría: Detectar > Gestión de acceso seguro

Gravedad: media

Tipo de recurso: `AWS::CloudFormation::Stack`

Regla de AWS Config: cloudformation-stack-service-role-check

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una AWS CloudFormation pila tiene asociada una función de servicio. El control de una CloudFormation pila falla si no hay ninguna función de servicio asociada a ella.

Service-managed StackSets utilice funciones de ejecución a través de AWS la integración de acceso confiable de Organizations. El control también genera un error al encontrar una AWS CloudFormation pila creada por un servicio gestionado StackSets porque no tiene ningún rol de servicio asociado. Debido a la forma en que los servicios gestionados se StackSets autentican, el `roleARN` campo no se puede rellenar para estas pilas.

El uso de funciones de servicio con CloudFormation pilas ayuda a implementar el acceso con privilegios mínimos al separar los permisos entre el usuario que las creates/updates acumula y los permisos que necesitan los recursos. CloudFormation create/update Esto reduce el riesgo de una escalada de privilegios y ayuda a mantener los límites de seguridad entre las distintas funciones operativas.

> **Note**
>
> No es posible eliminar un rol de servicio asociado a una pila después de crear la pila. Otros usuarios que tengan permisos para realizar operaciones en esta pila podrán usar este rol, sin importar si esos usuarios tienen o no el permiso `iam:PassRole`. Si el rol incluye permisos que el usuario no debería tener, puede escalar involuntariamente los permisos de un usuario. Asegúrese de que el rol concede privilegios mínimos.

Corrección

Para asociar una función de servicio a una CloudFormation pila, consulte la función CloudFormation de servicio en la Guía del AWS CloudFormation usuario.

Controles de CSPM de Security Hub para Amazon CloudFront

Estos AWS Security Hub CSPM controles evalúan el CloudFront servicio y los recursos de Amazon. Es posible que los controles no estén disponibles en todos los casos Regiones de AWS. Para obtener más información, consulte Disponibilidad de los controles por región.

[CloudFront.1] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado

Requisitos relacionados: NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), PCI DSS v4.0. 1/22.6.

Categoría: Proteger > Gestión del acceso seguro > Recursos que no son de acceso público

Gravedad: alta

Tipo de recurso: `AWS::CloudFront::Distribution`

Regla de AWS Config : cloudfront-default-root-object-configured

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una CloudFront distribución de Amazon con orígenes en S3 está configurada para devolver un objeto específico que es el objeto raíz predeterminado. El control falla si la CloudFront distribución usa orígenes de S3 y no tiene configurado un objeto raíz predeterminado. Este control no se aplica a CloudFront las distribuciones que utilizan orígenes personalizados.

A veces, un usuario puede solicitar la URL raíz de la distribución en lugar de un objeto de la distribución. Cuando esto ocurre, especificar un objeto raíz predeterminado puede ayudarle a evitar la exposición del contenido de su distribución web.

Corrección

Para configurar un objeto raíz predeterminado para una CloudFront distribución, consulte Cómo especificar un objeto raíz predeterminado en la Guía para CloudFront desarrolladores de Amazon.

[CloudFront.3] CloudFront las distribuciones deben requerir el cifrado durante el tránsito

Requisitos relacionados: NIST.800-53.r5 AC-17 (2) NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), (3), NIST.800-53.r5 SC-12 (3) NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-8 (1) NIST.800-53.r5 SC-8, (2), NIST.800-53.r5 SC-8 NIST.800-53.r5 SI-7 (6), PCI DSS v4.0. 1/42.2.1

Categoría: Proteger > Protección de datos > Cifrado de datos en tránsito

Gravedad: media

Tipo de recurso: `AWS::CloudFront::Distribution`

Regla de AWS Config : cloudfront-viewer-policy-https

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una CloudFront distribución de Amazon requiere que los espectadores usen HTTPS directamente o si utiliza la redirección. El control falla si `ViewerProtocolPolicy` está configurado como `allow-all` para `defaultCacheBehavior` o para `cacheBehaviors`.

Se puede utilizar HTTPS (TLS) para ayudar a evitar posibles ataques de «persona en medio» o similares para espiar o manipular el tráfico de red. Solo se deben permitir las conexiones cifradas a través de HTTPS (TLS). El cifrado de los datos en tránsito puede afectar al rendimiento. Debe probar su aplicación con esta característica para comprender el perfil de rendimiento y el impacto del TLS.

Corrección

Para cifrar una CloudFront distribución en tránsito, consulta la sección Cómo exigir el HTTPS para la comunicación entre los espectadores y CloudFront en la Guía para CloudFront desarrolladores de Amazon.

[CloudFront.4] CloudFront las distribuciones deben tener configurada la conmutación por error de origen

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoría: Recuperación > Resiliencia > Alta disponibilidad

Gravedad: baja

Tipo de recurso: `AWS::CloudFront::Distribution`

Regla de AWS Config : cloudfront-origin-failover-enabled

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una CloudFront distribución de Amazon está configurada con un grupo de origen que tiene dos o más orígenes.

CloudFront La conmutación por error en el origen puede aumentar la disponibilidad. La conmutación por error de Origin redirige automáticamente el tráfico a un origen secundario si el origen principal no está disponible o si devuelve códigos de estado de respuesta HTTP específicos.

Corrección

Para configurar la conmutación por error de origen para una CloudFront distribución, consulte Creación de un grupo de origen en la Guía para CloudFront desarrolladores de Amazon.

[CloudFront.5] CloudFront las distribuciones deben tener habilitado el registro

Requisitos relacionados: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9),, NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12 NIST.800-53.r5 AU-2 NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), (9) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (8), NIST.800-53.r5 SI-3 (20), NIST.800-53.r5 SI-4 NIST.800-53.r5 SI-7 (8), PCI DSS v4.0. 1/104.2.2

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: `AWS::CloudFront::Distribution`

Regla de AWS Config : cloudfront-accesslogs-enabled

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si el registro de acceso al servidor está habilitado en las CloudFront distribuciones. El control falla si el registro de acceso no está habilitado para una distribución. Este control solo evalúa si el registro estándar (heredado) está habilitado para una distribución.

CloudFront los registros de acceso proporcionan información detallada sobre cada solicitud de usuario que CloudFront recibe. Cada registro contiene información como la fecha y la hora en que se recibió la solicitud, la dirección IP del espectador que realizó la solicitud, el origen de la solicitud y el número de puerto de la solicitud del espectador. Estos registros son útiles para aplicaciones como auditorías de seguridad y acceso y para investigaciones forenses. Para obtener más información

sobre el análisis de los registros de acceso, consulte la sección Consulta CloudFront los registros de Amazon en la guía del usuario de Amazon Athena.

Corrección

Para configurar el registro estándar (heredado) para una CloudFront distribución, consulte Configurar el registro estándar (heredado) en la Guía para CloudFront desarrolladores de Amazon.

[CloudFront.6] CloudFront las distribuciones deben tener WAF activado

Requisitos relacionados: NIST.800-53.r5 AC-4 (21), PCI DSS v4.0. 1/64.2.2

Categoría: Proteger > Servicios de protección

Gravedad: media

Tipo de recurso: `AWS::CloudFront::Distribution`

Regla de AWS Config : cloudfront-associated-with-waf

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si CloudFront las distribuciones están asociadas a las ACL AWS WAF clásicas o AWS WAF web. El control falla si la distribución no está asociada a una ACL web.

AWS WAF es un firewall de aplicaciones web que ayuda a proteger las aplicaciones web y las API de los ataques. Le permite configurar un conjunto de reglas denominadas lista de control de acceso web (Web ACL) que permiten, bloquean o cuentan solicitudes web en función de las reglas y condiciones de seguridad web personalizables que defina. Asegúrese de que su CloudFront distribución esté asociada a una ACL AWS WAF web para protegerla de ataques malintencionados.

Corrección

Para asociar una ACL AWS WAF web a una CloudFront distribución, consulte Utilización AWS WAF para controlar el acceso a su contenido en la Guía para CloudFront desarrolladores de Amazon.

[CloudFront.7] CloudFront las distribuciones deben usar certificados personalizados SSL/TLS

Requisitos relacionados: NIST.800-53.r5 AC-17 (2) NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), NIST.800-53.r5 SC-12 (3),, (3) NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23

(3), NIST.800-53.r5 SC-7 (4) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (1), (2), NIST.800-53.r5 SC-8 NIST.800-53.r5 SI-7 (6), NIST.800-171.r2 3.13.15

Categoría: Proteger > Protección de datos > Cifrado de datos en tránsito

Gravedad: baja

Tipo de recurso: `AWS::CloudFront::Distribution`

Regla de AWS Config : cloudfront-custom-ssl-certificate

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si CloudFront las distribuciones utilizan los certificados predeterminados SSL/TLS que proporciona el certificado. CloudFront Este control se aprueba si la CloudFront distribución usa un SSL/TLS certificado personalizado. Este control falla si la CloudFront distribución usa el SSL/TLS certificado predeterminado.

De SSL/TLS forma personalizada, permite a los usuarios acceder al contenido mediante nombres de dominio alternativos. Puede almacenar los certificados personalizados en AWS Gestor de certificados (recomendado) o en IAM.

Corrección

Para añadir un nombre de dominio alternativo a una CloudFront distribución mediante un SSL/TLS certificado personalizado, consulte Añadir un nombre de dominio alternativo en la Guía para CloudFront desarrolladores de Amazon.

[CloudFront.8] CloudFront las distribuciones deben usar el SNI para atender las solicitudes HTTPS

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Categoría: Proteger - Configuración de red segura

Gravedad: baja

Tipo de recurso: `AWS::CloudFront::Distribution`

Regla de AWS Config : cloudfront-sni-enabled

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si CloudFront las distribuciones de Amazon utilizan un SSL/TLS certificado personalizado y están configuradas para utilizar el SNI para atender las solicitudes HTTPS. Este control falla si se asocia un SSL/TLS certificado personalizado pero el método de SSL/TLS soporte es una dirección IP dedicada. El control también falla si la distribución usa el CloudFront SSL/TLS certificado predeterminado.

Server Name Indication (SNI) (Indicación de nombre de servidor [SNI]) es una extensión del protocolo TLS que admiten los navegadores y clientes disponibles desde 2010. Si lo configuras CloudFront para atender las solicitudes HTTPS mediante SNI, CloudFront asocia tu nombre de dominio alternativo a una dirección IP para cada ubicación perimetral. Cuando un espectador envía una solicitud HTTPS de contenido, el servicio DNS dirige la solicitud a la dirección IP de la ubicación de borde correcta. La dirección IP de tu nombre de dominio se determina durante la negociación del SSL/TLS protocolo de enlace; la dirección IP no está dedicada a tu distribución.

Corrección

Si quieres configurar una CloudFront distribución para que utilice el SNI para atender las solicitudes HTTPS, consulta Cómo utilizar el SNI para atender las solicitudes HTTPS (funciona para la mayoría de los clientes) en la CloudFront Guía para desarrolladores. Para obtener información sobre los certificados SSL personalizados, consulta los requisitos para usar SSL/TLS certificados con. CloudFront

[CloudFront.9] CloudFront las distribuciones deben cifrar el tráfico para convertirlo en orígenes personalizados

Requisitos relacionados: NIST.800-53.r5 AC-17 (2) NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), (3), NIST.800-53.r5 SC-12 (3) NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (3), NIST.800-53.r5 SC-7 (4), (1) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SC-8 NIST.800-53.r5 SI-7 (6), PCI DSS v4.0. 1/42.2.1

Categoría: Proteger > Protección de datos > Cifrado de datos en tránsito

Gravedad: media

Tipo de recurso: `AWS::CloudFront::Distribution`

Regla de AWS Config : cloudfront-traffic-to-origin-encrypted

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si CloudFront las distribuciones de Amazon cifran el tráfico con orígenes personalizados. Este control falla en una CloudFront distribución cuya política de protocolo de origen permite «solo HTTP». Este control también falla si la política de protocolo de origen de la distribución es “match-viewer”, mientras que la política de protocolo de visor es “permisible para todos”.

El protocolo HTTPS (TLS) se puede utilizar para evitar el espionaje o la manipulación del tráfico de la red. Solo se deben permitir las conexiones cifradas a través de HTTPS (TLS).

Corrección

Para actualizar la política de protocolo de origen para exigir el cifrado de una CloudFront conexión, consulta la sección sobre cómo exigir el HTTPS para la comunicación entre tu origen personalizado CloudFront y tu origen personalizado en la Guía para desarrolladores de Amazon. CloudFront

[CloudFront.10] CloudFront las distribuciones no deben usar protocolos SSL obsoletos entre ubicaciones de borde y orígenes personalizados

Requisitos relacionados: NIST.800-53.r5 AC-17 (2), NIST.800-53.r5 IA-5 (1) NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-12 (3),,, (4) NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-7 (1) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SC-8 NIST.800-53.r5 SI-7 (6), NIST.800-171.r2 3.13.15, PCI DSS v4.0. 1/42.2.1

Categoría: Proteger > Protección de datos > Cifrado de datos en tránsito

Gravedad: media

Tipo de recurso: `AWS::CloudFront::Distribution`

Regla de AWS Config : cloudfront-no-deprecated-ssl-protocols

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si CloudFront las distribuciones de Amazon utilizan protocolos SSL obsoletos para la comunicación HTTPS entre las ubicaciones de CloudFront borde y tus orígenes personalizados. Este control falla si una CloudFront distribución tiene un `CustomOriginConfig` lugar donde se `OriginSslProtocols` incluye. `SSLv3`

En 2015, el Internet Engineering Task Force (IETF) anunció oficialmente que el SSL 3.0 debería quedar obsoleto debido a que el protocolo no era lo suficientemente seguro. Se recomienda usar TLSv1.2 o más adelante para la comunicación HTTPS con sus orígenes personalizados.

Corrección

Para actualizar los protocolos SSL de Origin para una CloudFront distribución, consulte la Guía para CloudFront desarrolladores de Amazon sobre cómo exigir HTTPS para la comunicación entre su origen personalizado CloudFront y su origen personalizado.

[CloudFront.12] CloudFront las distribuciones no deben apuntar a orígenes de S3 inexistentes

Requisitos relacionados: NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2), PCI DSS v4.0. 1/22.6.

Categoría: Identificar > Configuración de recursos

Gravedad: alta

Tipo de recurso: `AWS::CloudFront::Distribution`

Regla de AWS Config : cloudfront-s3-origin-non-existent-bucket

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si CloudFront las distribuciones de Amazon apuntan a orígenes inexistentes de Amazon S3. El control falla en una CloudFront distribución si el origen está configurado para apuntar a un bucket inexistente. Este control solo se aplica a CloudFront las distribuciones en las que el origen de S3 es un bucket de S3 sin alojamiento estático de sitios web.

Cuando una CloudFront distribución de tu cuenta está configurada para que apunte a un bucket inexistente, un tercero malintencionado puede crear el bucket al que se hace referencia y publicar su propio contenido a través de tu distribución. Recomendamos comprobar todos los orígenes, independientemente del comportamiento de enrutamiento, para asegurarse de que sus distribuciones apuntan a los orígenes adecuados.

Corrección

Para modificar una CloudFront distribución para que apunte a un nuevo origen, consulta Cómo actualizar una distribución en la Guía para CloudFront desarrolladores de Amazon.

[CloudFront.13] CloudFront las distribuciones deben usar el control de acceso al origen

Categoría: Proteger > Gestión del acceso seguro > Recurso no accesible públicamente

Gravedad: media

Tipo de recurso: `AWS::CloudFront::Distribution`

Regla de AWS Config : cloudfront-s3-origin-access-control-enabled

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una CloudFront distribución de Amazon con un origen en Amazon S3 tiene configurado el control de acceso al origen (OAC). El control falla si OAC no está configurado para la CloudFront distribución.

Cuando utilices un bucket de S3 como origen para tu CloudFront distribución, puedes habilitar el OAC. Esto permite el acceso al contenido del depósito solo a través de la CloudFront distribución especificada y prohíbe el acceso directo desde el depósito u otra distribución. Si bien CloudFront es compatible con Origin Access Identity (OAI), OAC ofrece funciones adicionales y las distribuciones que utilizan OAI pueden migrar a OAC. Si bien OAI proporciona una forma segura de acceder a los orígenes de S3, tiene limitaciones, como la falta de soporte para configuraciones de políticas granulares y para las HTTP/HTTPS solicitudes que utilizan el método POST y Regiones de AWS que requieren la versión 4 de la AWS firma (SIGv4). OAI tampoco admite el cifrado con. AWS Key Management Service El OAC se basa en la práctica AWS recomendada de utilizar los principios de servicio de IAM para autenticarse con los orígenes de S3.

Corrección

Para configurar OAC para una CloudFront distribución con orígenes en S3, consulte Restringir el acceso a un origen de Amazon S3 en la Guía para desarrolladores de Amazon. CloudFront

[CloudFront.14] CloudFront las distribuciones deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::CloudFront::Distribution`

AWS Config regla: `tagged-cloudfront-distribution` (regla CSPM personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub CSPM
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si una CloudFront distribución de Amazon tiene etiquetas con las claves específicas definidas en el parámetro`requiredTagKeys`. El control lanza un error si la distribución no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si la distribución no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y se compone de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan

operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWSen la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Las etiquetas son accesibles para muchos Servicios de AWS, incluso AWS Billing. Para conocer más prácticas recomendadas para el etiquetado, consulte Etiquetado de recursos de AWS en la Referencia general de AWS.

Corrección

Para añadir etiquetas a una CloudFront distribución, consulte Etiquetar CloudFront distribuciones de Amazon en la Guía para CloudFront desarrolladores de Amazon.

[CloudFront.15] CloudFront las distribuciones deben usar la política de seguridad TLS recomendada

Categoría: Proteger > Protección de datos > Cifrado de datos en tránsito

Gravedad: media

Tipo de recurso: `AWS::CloudFront::Distribution`

Regla de AWS Config : cloudfront-ssl-policy-check

Tipo de horario: provocado por un cambio

Parámetros: `securityPolicies`: `TLSv1.2_2021,TLSv1.2_2025,TLSv1.3_2025` (no personalizables)

Este control comprueba si una CloudFront distribución de Amazon está configurada para usar una política de seguridad TLS recomendada. El control falla si la CloudFront distribución no está configurada para usar una política de seguridad TLS recomendada.

Si configuras una CloudFront distribución de Amazon para que exija a los espectadores que usen HTTPS para acceder al contenido, debes elegir una política de seguridad y especificar la versión mínima del SSL/TLS protocolo que se va a utilizar. Esto determina la versión del protocolo que se CloudFront utiliza para comunicarse con los espectadores y los cifrados que se CloudFront utilizan para cifrar las comunicaciones. Se recomienda utilizar la política de seguridad más reciente que

CloudFront proporciona. Esto garantiza que CloudFront utilice los conjuntos de cifrado más recientes para cifrar los datos en tránsito entre un espectador y una CloudFront distribución.

> **Note**
>
> Este control genera resultados solo para CloudFront las distribuciones que están configuradas para usar certificados SSL personalizados y no están configuradas para admitir clientes antiguos.

Corrección

Para obtener información sobre la configuración de la política de seguridad de una CloudFront distribución, consulte Actualizar una distribución en la Guía para CloudFront desarrolladores de Amazon. Cuando configure la política de seguridad para una distribución, elija la política de seguridad más reciente.

[CloudFront.16] CloudFront las distribuciones deben usar el control de acceso de origen para los orígenes de las URL de las funciones de Lambda

Categoría: Proteger - Administración de acceso seguro > Control de acceso

Gravedad: media

Tipo de recurso: `AWS::CloudFront::Distribution`

Regla de AWS Config : cloudfront-origin-lambda-url-oac-enabled

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una CloudFront distribución de Amazon con una URL de AWS Lambda función como origen tiene activado el control de acceso al origen (OAC). El control falla si la CloudFront distribución tiene una URL de función Lambda como origen y el OAC no está habilitado.

AWS Lambda La URL de una función es un punto final HTTPS dedicado para una función de Lambda. Si la URL de una función de Lambda es el origen de una CloudFront distribución, la URL de la función debe ser de acceso público. Por lo tanto, como práctica recomendada de seguridad, debe crear un OAC y agregarlo a la URL de función de Lambda en una distribución. OAC usa los principios de servicio de IAM para autenticar las solicitudes entre CloudFront la URL de la función

y la misma. También admite el uso de políticas basadas en recursos para permitir la invocación de una función solo si la solicitud se realiza en nombre de una distribución especificada en la política. CloudFront

Corrección

Para obtener información sobre la configuración de OAC para una CloudFront distribución de Amazon que utilice la URL de una función de Lambda como origen, consulte Restringir el acceso al origen de la URL de una AWS Lambda función en la Guía para desarrolladores de Amazon. CloudFront

[CloudFront.17] CloudFront las distribuciones deben usar grupos de claves confiables para las URL y cookies firmadas

Categoría: Proteger - Administración de acceso seguro > Control de acceso

Gravedad: media

Tipo de recurso: `AWS::CloudFront::Distribution`

Regla de AWS Config : cloudfront-distribution-key-group-enabled

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una CloudFront distribución de Amazon está configurada para usar grupos de claves de confianza para la autenticación de URL firmadas o cookies firmadas. El control falla si la CloudFront distribución usa firmantes de confianza o si la distribución no tiene configurada la autenticación.

Para utilizar URL firmadas o cookies firmadas, necesita un signatario. Un firmante es un grupo de claves de confianza en CloudFront el que se crea o una AWS cuenta que contiene un par de CloudFront claves. Te recomendamos que utilices grupos de claves de confianza, ya que con los grupos de CloudFront claves no necesitas usar el usuario raíz de la AWS cuenta para administrar las claves públicas de las URL CloudFront firmadas y las cookies firmadas.

> **Note**
>
> Este control no evalúa las distribuciones de varios inquilinos CloudFront . `(connectionMode=tenant-only)`

Corrección

Para obtener información sobre el uso de grupos de claves de confianza con URL y cookies firmadas, consulte Uso de grupos de claves de confianza en la Guía para desarrolladores de Amazon CloudFront .

Controles CSPM de Security Hub paraAWS CloudTrail

Estos AWS Security Hub CSPM controles evalúan el AWS CloudTrail servicio y los recursos. Es posible que los controles no estén disponibles en todosRegiones de AWS. Para obtener más información, consulte Disponibilidad de los controles por región.

[CloudTrail.1] CloudTrail debe estar habilitado y configurado con al menos un registro multirregional que incluya eventos de administración de lectura y escritura

Requisitos relacionados: CIS AWS Foundations Benchmark v5.0. 0/3.1, Punto de referencia sobre AWS los fundamentos de la CEI v1.2. 0/2.1, Punto de referencia sobre AWS los fundamentos de la CEI v1.4. 0/3.1, Criterio de referencia sobre AWS los fundamentos de la CEI v3.0. 0/3.1, NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2 NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 AU-14 (1) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8), NIST.800-53.r5 SA-8 (22)

Categoría: Identificar - Registro

Gravedad: alta

Tipo de recurso: `AWS::::Account`

Regla de AWS Config: multi-region-cloudtrail-enabled

Tipo de programa: Periódico

Parámetros:

- `readWriteType`: `ALL` (no personalizable)

  `includeManagementEvents`: `true` (no personalizable)

Este control comprueba si hay al menos un AWS CloudTrail registro multirregional que capture los eventos de gestión de lectura y escritura. El control falla si CloudTrail está deshabilitado o si no hay al menos un CloudTrail registro que capture los eventos de administración de lectura y escritura.

AWS CloudTrailregistra las llamadas a la AWS API de tu cuenta y te entrega los archivos de registro. La información registrada incluye lo siguiente:

- Identidad del intermediario de la API
- Hora de la llamada a la API
- Dirección IP de origen de la persona que llama a la API
- Parámetros de solicitud
- Elementos de respuesta devueltos por el Servicio de AWS

CloudTrail proporciona un historial de las llamadas a la AWS API de una cuenta, incluidas las llamadas a la API realizadas desde los Consola de administración de AWS AWS SDK y las herramientas de línea de comandos. El historial también incluye las llamadas a la API de niveles superioresServicios de AWS, como. AWS CloudFormation

El historial de llamadas a la AWS API generado por CloudTrail permite el análisis de seguridad, el seguimiento de los cambios en los recursos y la auditoría de conformidad. Multi-Region Las rutas también ofrecen las siguientes ventajas.

- Un registro de seguimiento de varias regiones ayuda a detectar la actividad inesperada que ocurre en regiones que no se utilizan.
- Un registro de seguimiento de eventos de varias regiones garantiza que el registro de servicios globales esté habilitado para un registro de seguimiento de forma predeterminada. El registro de eventos del servicio global registra los eventos generados por los servicios AWS globales.
- Para un registro multirregional, los eventos de administración de todas las operaciones de lectura y escritura garantizan que las operaciones de administración de CloudTrail registros de todos los recursos de una Cuenta de AWS sola vez.

De forma predeterminada, las CloudTrail rutas que se crean con ellas Consola de administración de AWS son rutas multirregionales.

Corrección

Para crear un nuevo sendero multirregional CloudTrail, consulte Creación de un sendero en la Guía del AWS CloudTrailusuario. Use los siguientes valores:

Campo	Valor
Configuración adicional: validación de archivos de registro	Habilitado
Elija los eventos de registro, los eventos de administración y la actividad de la API	Leer y Escribir. Desactive las casillas de verificación de las exclusiones.

Para actualizar una ruta existente, consulte Actualización de una ruta en la Guía del usuario de AWS CloudTrail. En Eventos de administración, para la actividad de la API, seleccione Leer y Escribir.

[CloudTrail.2] CloudTrail debe tener activado el cifrado en reposo

Requisitos relacionados: CIS AWS Foundations Benchmark v5.0. 0/3.5, Criterio de referencia sobre los AWS fundamentos de la CEI v1.2. 0/2.7, Punto de referencia sobre los AWS fundamentos de la CEI v1.4. 0/3.7, Criterio de referencia sobre los AWS fundamentos de la CEI v3.0. 0/3.5 NIST.800-53.r5 AU-9, NIST.800-53.r5 CA-9 (1), (6),, NIST.800-53.r5 CM-3 (1) NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (10), NIST.800-53.r5 SC-7 NIST.800-53.r5 SI-7 (6), NIST.800-171.r2 3.3.8, PCI DSS v3.2. 1/34.4, PCI DSS v4.0. 1/10.3.2

Categoría: Proteger > Protección de datos > Cifrado de datos en reposo

Gravedad: media

Tipo de recurso: `AWS::CloudTrail::Trail`

Regla de AWS Config: cloud-trail-encryption-enabled

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si CloudTrail está configurado para utilizar el cifrado del lado del servidor (SSE). AWS KMS key El control falla si no se ha definido `KmsKeyId`.

Para aumentar la seguridad de sus archivos de CloudTrail registro confidenciales, debe utilizar el cifrado del lado del servidor con AWS KMS keys (SSE-KMS) en los archivos de CloudTrail registro para cifrarlos en reposo. Tenga en cuenta que, de forma predeterminada, los archivos de registro que envían CloudTrail a sus depósitos se cifran mediante el cifrado del lado del servidor de Amazon con claves de S3-managed cifrado de Amazon (). SSE-S3

Corrección

Para habilitar el SSE-KMS cifrado de los archivos de CloudTrail registro, consulte Actualizar un registro para usar una clave KMS en la Guía del AWS CloudTrail usuario.

[CloudTrail.3] Debe estar habilitada al menos una CloudTrail ruta

Requisitos relacionados: NIST.800-171.r2 3.3.1, NIST.800-171.r2 3.14.6, NIST.800-171.r2 3.14.7, PCI DSS v3.2. 1/101.1, PCI DSS v3.2. 1/10.2.1, PCI DSS v3.2. 1/10.2.2, PCI DSS v3.2. 1/10.2.3, PCI DSS v3.2. 1/10.2.4, PCI DSS v3.2. 1/10.2.5, PCI DSS v3.2. 1/10.2.6, PCI DSS v3.2. 1/10.2.7, PCI DSS v3.2. 1/10.3.1, PCI DSS v3.2. 1/10.3.2, PCI DSS v3.2. 1/10.3.3, PCI DSS v3.2. 1/10.3.4, PCI DSS v3.2. 1/10.3.5, PCI DSS v3.2. 1/10.3.6, PCI DSS v4.0. 1/10.2.1

Categoría: Identificar - Registro

Gravedad: alta

Tipo de recurso: `AWS::::Account`

Regla de AWS Config: cloudtrail-enabled

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si hay alguna AWS CloudTrail ruta habilitada en su Cuenta de AWS interior. El control falla si tu cuenta no tiene al menos una CloudTrail ruta habilitada.

Sin embargo, algunos AWS servicios no permiten el registro de todas las API y eventos. Debe implementar cualquier registro de auditoría adicional que no sea CloudTrail revisar la documentación de cada servicio en los servicios e integraciones CloudTrail compatibles.

Corrección

Para empezar CloudTrail a crear un registro, consulte el AWS CloudTrailtutorial Cómo empezar a usarlo en la Guía del AWS CloudTrail usuario.

[CloudTrail.4] La validación del archivo de CloudTrail registro debe estar habilitada

Requisitos relacionados: CIS AWS Foundations Benchmark v5.0. 0/3.2, Punto de referencia sobre AWS los fundamentos de la CEI v1.2. 0/2.2, Punto de referencia sobre AWS los fundamentos de la CEI v1.4. 0/3.2, Criterio de referencia sobre AWS los fundamentos de la CEI v3.0. 0/3.2, NIST.800-53.r5 AU-9 NIST.800-53.r5 SI-4, NIST.800-53.r5 SI-7 (1), (3), NIST.800-53.r5 SI-7

NIST.800-53.r5 SI-7 (7), NIST.800-171.r2 3.3.8, PCI DSS v3.2. 1/102.5.2, PCI DSS v3.2. 1/10.5.5, PCI DSS v4.0. 1/10.3.2

Categoría: Protección de datos > Integridad de los datos

Gravedad: baja

Tipo de recurso: `AWS::CloudTrail::Trail`

Regla de AWS Config: cloud-trail-log-file-validation-enabled

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si la validación de la integridad de los archivos de registro está habilitada en un CloudTrail registro.

CloudTrail la validación del archivo de registro crea un archivo de resumen firmado digitalmente que contiene un hash de cada registro que se CloudTrail escribe en Amazon S3. Puede utilizar estos archivos de resumen para determinar si un archivo de registro se modificó, se eliminó o no se modificó después de CloudTrail entregar el registro.

Security Hub CSPM recomienda activar la validación de archivos en todas las rutas. La validación de los archivos de registro proporciona comprobaciones adicionales de integridad de CloudTrail los registros.

Corrección

Para habilitar la validación de los archivos de CloudTrail registro, consulte Habilitar la validación de la integridad de los archivos de registro CloudTrail en la Guía del AWS CloudTrail usuario.

[CloudTrail.5] los CloudTrail senderos deben estar integrados con Amazon CloudWatch Logs

Requisitos relacionados: CIS AWS Foundations Benchmark v5.0. 0/34.4, PCI DSS v3.2. 1/10.5.3, Criterio de referencia sobre los AWS fundamentos de la CEI v1.2. 0/2.4, Punto de referencia sobre los AWS fundamentos de la CEI v1.4. 0/3.4, NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2 NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (1), NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 AU-6 (5), NIST.800-53.r5 AU-7 (1) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), (8) NIST.800-53.r5 SI-20, NIST.800-53.r5 SI-3 (20), NIST.800-53.r5 SI-4 (5), NIST.800-53.r5 SI-4 (8) NIST.800-53.r5 SI-7

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: `AWS::CloudTrail::Trail`

Regla de AWS Config: cloud-trail-cloud-watch-logs-enabled

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si las CloudTrail rutas están configuradas para enviar CloudWatch registros a Logs. El control falla si la propiedad `CloudWatchLogsLogGroupArn` de la ruta está vacía.

CloudTrail registra las llamadas a la AWS API que se realizan en una cuenta determinada. La información registrada incluye lo siguiente:

- Identidad de la persona que llama a la API
- Hora de la llamada a la API
- Dirección IP de origen de la persona que llama a la API
- Parámetros de solicitudes
- Los elementos de respuesta devueltos por el Servicio de AWS

CloudTrail utiliza Amazon S3 para el almacenamiento y la entrega de archivos de registro. Puede capturar CloudTrail los registros en un depósito de S3 específico para analizarlos a largo plazo. Para realizar un análisis en tiempo real, puede configurar CloudTrail el envío de CloudWatch registros a Logs.

En el caso de un registro que esté habilitado en todas las regiones de una cuenta, CloudTrail envía los archivos de registro de todas esas regiones a un grupo de CloudWatch registros.

Security Hub CSPM recomienda enviar CloudTrail registros a CloudWatch Logs. Tenga en cuenta que esta recomendación tiene por objeto garantizar que la actividad de la cuenta se capture, supervise y se genere la alarma adecuada. Puede usar CloudWatch los registros para configurar esto con su. Servicios de AWS Esta recomendación no impide el uso de una solución diferente.

El envío de CloudTrail CloudWatch registros a Logs facilita el registro de actividades históricas y en tiempo real en función del usuario, la API, el recurso y la dirección IP. Puede utilizar este abordaje

para establecer alarmas y notificaciones en caso de que se produzcan actividades de la cuenta anómalas o delicadas.

Corrección

Para integrarlo CloudTrail con CloudWatch los registros, consulte Enviar eventos a CloudWatch los registros en la Guía del AWS CloudTrail usuario.

[CloudTrail.6] Asegúrese de que el depósito de S3 que se utiliza para almacenar CloudTrail los registros no sea de acceso público

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2. 0/2.3, Punto de referencia sobre AWS los fundamentos de la CEI v1.4. 0/3.3, PCI DSS v4.0. 1/13.4.4

Categoría: Identificar - Registro

Gravedad: crítica

Tipo de recurso: `AWS::S3::Bucket`

AWS Configregla: Ninguna (regla CSPM de Security Hub personalizada)

Tipo de programa: periódico y activado por cambios

Parámetros: ninguno

CloudTrail registra un registro de todas las llamadas a la API realizadas en su cuenta. Los archivos de registro se almacenan en un bucket de S3. El CIS recomienda aplicar la política de bucket de S3, o lista de control de acceso (ACL), al bucket de S3 que CloudTrail registra para impedir el acceso público a los CloudTrail registros. Permitir el acceso público al contenido de los CloudTrail registros podría ayudar a un adversario a identificar puntos débiles en el uso o la configuración de la cuenta afectada.

Para ejecutar esta comprobación, Security Hub CSPM utiliza primero una lógica personalizada para buscar el depósito de S3 en el que se almacenan CloudTrail los registros. A continuación, utiliza las reglas AWS Config administradas para comprobar que el depósito es de acceso público.

Si agregas tus registros en un único depósito de S3 centralizado, Security Hub CSPM solo realizará la comprobación de la cuenta y la región en las que se encuentra el depósito de S3 centralizado. En el caso de otras cuentas y regiones, el estado de control es Sin datos.

Si el bucket está accesible públicamente, la comprobación genera un resultado de error.

Corrección

Para bloquear el acceso público a su depósito de CloudTrail S3, consulte Configuración de los ajustes de bloqueo de acceso público para sus depósitos de S3 en la Guía del usuario de Amazon Simple Storage Service. Seleccione las cuatro configuraciones de Bloqueo de acceso público de Amazon S3.

[CloudTrail.7] Asegúrese de que el registro de acceso al bucket de S3 esté habilitado en el CloudTrail bucket de S3

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2. 0/2.6, Punto de referencia sobre los AWS fundamentos de la CEI v1.4. 0/3.6, Criterio de referencia sobre los AWS fundamentos de la CEI v3.0. 0/3.4, PCI DSS v4.0. 1/10.2.1

Categoría: Identificar - Registro

Gravedad: baja

Tipo de recurso: `AWS::S3::Bucket`

AWS Configregla: Ninguna (regla CSPM de Security Hub personalizada)

Tipo de programa: Periódico

Parámetros: ninguno

El registro de acceso al bucket S3 genera un registro que contiene registros de acceso para cada solicitud realizada a su bucket S3. Un registro de acceso contiene detalles sobre la solicitud, como el tipo de solicitud, los recursos especificados en la solicitud con los que se ha trabajado y la fecha y hora en que se procesó la solicitud.

El CIS recomienda habilitar el registro de acceso al bucket en el bucket CloudTrail S3.

Al habilitar el registro del bucket de S3 en los buckets de S3 de destino, puede capturar todos los eventos que podrían afectar a los objetos en el bucket de destino. Configurar los registros para que se coloquen en un bucket independiente permite el acceso a la información de registro, lo que puede resultar útil en flujos de trabajo de respuesta a incidentes y seguridad.

Para ejecutar esta comprobación, Security Hub CSPM utiliza primero una lógica personalizada para buscar el depósito en el que se almacenan CloudTrail los registros y, a continuación, utiliza la regla AWS Config administrada para comprobar si el registro está habilitado.

Si CloudTrail entrega archivos de registro de varios depósitos de Amazon S3 Cuentas de AWS a un único bucket de destino, Security Hub CSPM evalúa este control únicamente con respecto al depósito de destino de la región en la que se encuentra. Esto optimiza sus resultados. Sin embargo, debes activar todas CloudTrail las cuentas que envían registros al depósito de destino. Para todas las cuentas, excepto la que contiene el bucket de destino, el estado de control es Sin datos.

Corrección

Para habilitar el registro de acceso al servidor para su bucket de CloudTrail S3, consulte Habilitar el registro de acceso al servidor Amazon S3 en la Guía del usuario de Amazon Simple Storage Service.

[CloudTrail.9] las CloudTrail rutas deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::CloudTrail::Trail`

AWS Configregla: `tagged-cloudtrail-trail` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	`No default value`

Este control comprueba si un AWS CloudTrail sendero tiene etiquetas con las claves específicas definidas en el parámetro`requiredTagKeys`. El control lanza error si el registro de seguimiento

no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si el registro de seguimiento no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte Etiquetar sus AWS recursos en el. Referencia general de AWS

Corrección

Para añadir etiquetas a una CloudTrail ruta, consulta la referencia AddTagsde la AWS CloudTrailAPI.

[CloudTrail.10] Los almacenes de datos de eventos de CloudTrail Lake deben estar cifrados y gestionados por el clienteAWS KMS keys

Requisitos relacionados: NIST.800-53.r5 AU-9 NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SC-12 (2), NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SI-7 (6)

Categoría: Proteger > Protección de datos > Cifrado de datos en reposo

Gravedad: media

Tipo de recurso: `AWS::CloudTrail::EventDataStore`

Regla de AWS Config: event-data-store-cmk-encryption-enabled

Tipo de programa: Periódico

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`kmsKeyArns`	Una lista de nombres de recursos de Amazon (ARN) AWS KMS keys para incluirlos en la evaluación. El control genera un resultado `FAILED` si un almacén de datos de eventos no está cifrado con una clave de KMS de la lista.	StringList (máximo de 3 elementos)	Entre 1 y 3 ARN de claves de KMS existentes. Por ejemplo: `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab` .	Sin valor predeterminado

Este control comprueba si un almacén de datos de eventos de AWS CloudTrail Lake está cifrado en reposo y gestionado por un clienteAWS KMS key. El control fallará si el almacén de datos de eventos no está cifrado con una clave de KMS administrada por el cliente. Puede especificar opcionalmente una lista de claves de KMS para que el control las incluya en la evaluación.

De forma predeterminada, AWS CloudTrail Lake cifra los almacenes de datos de eventos con claves administradas de Amazon S3 (SSE-S3) mediante un AES-256 algoritmo. Para tener un control adicional, puede configurar CloudTrail Lake para que cifre un almacén de datos de eventos con un archivo gestionado por el cliente AWS KMS key (SSE-KMS) en su lugar. Una clave KMS gestionada por el cliente es AWS KMS key aquella que usted crea, posee y administra en su Cuenta de AWS

propia cuenta. Ejerce control total sobre este tipo de clave de KMS. Esto incluye definir y mantener la política de claves, administrar concesiones, rotar el material criptográfico, asignar etiquetas, crear alias, y habilitar y deshabilitar la clave. Puede usar una clave KMS administrada por el cliente en operaciones criptográficas para sus CloudTrail datos y auditar el uso con CloudTrail registros.

Corrección

Para obtener información sobre cómo cifrar un banco de datos de eventos de AWS CloudTrail Lake con una AWS KMS key que usted especifique, consulte Actualizar un banco de datos de eventos en la Guía del AWS CloudTrailusuario. Después de asociar un almacén de datos de eventos a una clave de KMS, esta no se podrá eliminar ni cambiar.

Controles de CSPM de Security Hub para Amazon CloudWatch

Estos AWS Security Hub CSPM controles evalúan el CloudWatch servicio y los recursos de Amazon. Es posible que los controles no estén disponibles en todos los casos Regiones de AWS. Para obtener más información, consulte Disponibilidad de los controles por región.

[CloudWatch.1] Debe existir un registro, un filtro métrico y una alarma para el uso del usuario «raíz»

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2. 0/1.1, CIS AWS Foundations Benchmark v1.2. 0/3.3, CIS AWS Foundations Benchmark v1.4. 0/11.7, CIS AWS Foundations Benchmark v1.4. 0/44.3, NIST.800-171.r2 3.14.6, 3.14.7, PCI NIST.800-171.r2 DSS v3.2. 1/73.2.1

Categoría: Detectar - Servicios de detección

Gravedad: baja

Tipo de recurso: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config regla: Ninguna (regla CSPM personalizada de Security Hub)

Tipo de programa: Periódico

Parámetros: ninguno

Este usuario raíz tiene acceso a todos los recursos y los servicios no restringidos de Cuenta de AWS. Le recomendamos encarecidamente que evite utilizar el usuario raíz para las tareas diarias. Minimizar el uso del usuario raíz y adoptar el principio de privilegio mínimo para la administración del acceso reduce el riesgo de cambios accidentales y de la divulgación no intencionada de credenciales altamente privilegiadas.

Como práctica recomendada, utilice sus credenciales de usuario raíz solo cuando sea necesario para realizar tareas de administración de cuentas y servicios. Aplica las políticas AWS Identity and Access Management (IAM) directamente a los grupos y roles, pero no a los usuarios. Para ver un tutorial sobre cómo configurar un administrador para el uso diario, consulte Creación del primer grupo y usuario administrador de IAM en la Guía de usuario de IAM.

Para ejecutar esta comprobación, el CSPM de Security Hub utiliza una lógica personalizada para realizar exactamente los pasos de auditoría prescritos para el control 1.7 en la versión 1.4.0 de CIS AWS Foundations Benchmark. Este control produce un error si no se utilizan los filtros de métricas exactos prescritos por CIS. No se pueden añadir campos ni términos adicionales a los filtros de métricas.

> **Note**
>
> Cuando Security Hub CSPM comprueba este control, busca los CloudTrail rastros que utiliza la cuenta actual. Estas rutas pueden ser rutas de organizaciones que pertenecen a otra cuenta. Multi-Region Las rutas también pueden estar ubicadas en una región diferente. La comprobación arroja resultados de `FAILED` en los siguientes casos:
>
> - No hay ningún rastro configurado.
> - Las rutas disponibles que se encuentran en la Región actual y que son propiedad de una cuenta corriente no cumplen con los requisitos de control.
>
> La comprobación da como resultado un estado de control de `NO_DATA` en los siguientes casos:
>
> - Una ruta multirregional se basa en una Región diferente. Security Hub CSPM solo puede generar hallazgos en la región en la que se encuentra la ruta.
> - Una ruta multirregional pertenece a una cuenta diferente. El CSPM de Security Hub solo puede generar hallazgos para la cuenta propietaria de la ruta.
>
> Como práctica recomendada, utilice los registros de la organización para registrar los eventos de muchas cuentas de una organización. Los registros organizacionales son registros multirregionales de forma predeterminada y solo los puede administrar la cuenta AWS Organizations de administración o la cuenta de administrador CloudTrail delegado. El uso de un registro de la organización da como resultado un estado de control de `NO_DATA` de los controles evaluados en las cuentas de los miembros de la organización. En las cuentas de los miembros, Security Hub CSPM solo genera hallazgos para los

recursos que pertenecen a los miembros. Los resultados relacionados con los registros de la organización se generan en la cuenta del propietario del recurso. Puede ver estos resultados en su cuenta de administrador delegado de CSPM de Security Hub mediante la agregación entre regiones.

Para la alarma, la cuenta corriente debe ser propietaria del tema de Amazon SNS al que se hace referencia o debe obtener acceso al tema de Amazon SNS llamando a `ListSubscriptionsByTopic`. De lo contrario, Security Hub CSPM `WARNING` generará resultados para el control.

Corrección

Para pasar este control, siga estos pasos para crear un tema de Amazon SNS, una ruta de AWS CloudTrail , un filtro de métricas y una alarma para el filtro de métricas.

1. Crear un tema de Amazon SNS Para obtener instrucciones, consulte Introducción a Amazon SNS en la Guía para desarrolladores de Amazon Simple Notification Service. Cree un tema que reciba todas las alarmas del CIS y cree al menos una suscripción al tema.
2. Cree una CloudTrail ruta que se aplique a todos. Regiones de AWS Para obtener instrucciones, consulte Crear un registro de seguimiento en la Guía del usuario de AWS CloudTrail .

   Anote el nombre del grupo de CloudWatch registros que asocie a la CloudTrail ruta. En el siguiente paso, debe crear el filtro de métricas para ese grupo de registros.
3. Crear un filtro de métricas. Para obtener instrucciones, consulte Crear un filtro métrico para un grupo de registros en la Guía del CloudWatch usuario de Amazon. Use los siguientes valores:

Campo	Valor
Defina el patrón, el patrón de filtro	`{$.userIdentity.type="Root" && $.userIdentity.invokedBy NOT EXISTS && $.eventType !="AwsServiceEvent"}`
Espacio de nombres de métrica	**`LogMetrics`**
Valor de la métrica	**`1`**

Campo	Valor
Predeterminado	**0**

4. Crear una alarma basada en el filtro. Para obtener instrucciones, consulte Crear una CloudWatch alarma basada en un filtro métrico de grupos de registros en la Guía del CloudWatch usuario de Amazon. Use los siguientes valores:

Campo	Valor
Condiciones, tipo de umbral	Estático
Siempre que sea... *your-metric-name*	Greater/Equal
que…	**1**

[CloudWatch.2] Asegúrese de que existan un registro, un filtro métrico y una alarma para las llamadas a la API no autorizadas

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2. 0/3.1, NIST.800-171.r2 3.13.1, 3.14.6, NIST.800-171.r2 3.14.7 NIST.800-171.r2

Categoría: Detectar - Servicios de detección

Gravedad: baja

Tipo de recurso: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config regla: Ninguna (regla CSPM personalizada de Security Hub)

Tipo de programa: Periódico

Parámetros: ninguno

Para supervisar las llamadas a la API en tiempo real, dirija CloudTrail los CloudWatch registros a Logs y establezca las alarmas y los filtros métricos correspondientes.

CIS recomienda que cree un filtro de métricas y una alarma para llamadas a la API no autorizadas. La monitorización de las llamadas no autorizadas a la API ayuda a revelar errores de la aplicación y puede reducir el tiempo que se tarda en detectar actividades malintencionadas.

Para ejecutar esta comprobación, el CSPM de Security Hub utiliza una lógica personalizada para realizar los pasos de auditoría exactos prescritos para el control 3.1 en la versión 1.2 de CIS AWS Foundations Benchmark. Este control produce un error si no se utilizan los filtros de métricas exactos prescritos por CIS. No se pueden añadir campos ni términos adicionales a los filtros de métricas.

> **Note**
>
> Cuando Security Hub CSPM comprueba este control, busca los CloudTrail rastros que utiliza la cuenta actual. Estas rutas pueden ser rutas de organizaciones que pertenecen a otra cuenta. Multi-Region Las rutas también pueden estar ubicadas en una región diferente. La comprobación arroja resultados de `FAILED` en los siguientes casos:
>
> - No hay ningún rastro configurado.
> - Las rutas disponibles que se encuentran en la Región actual y que son propiedad de una cuenta corriente no cumplen con los requisitos de control.
>
> La comprobación da como resultado un estado de control de `NO_DATA` en los siguientes casos:
>
> - Una ruta multirregional se basa en una Región diferente. Security Hub CSPM solo puede generar hallazgos en la región en la que se encuentra la ruta.
> - Una ruta multirregional pertenece a una cuenta diferente. El CSPM de Security Hub solo puede generar hallazgos para la cuenta propietaria de la ruta.
>
> Como práctica recomendada, utilice los registros de la organización para registrar los eventos de muchas cuentas de una organización. Los registros organizacionales son registros multirregionales de forma predeterminada y solo los puede administrar la cuenta AWS Organizations de administración o la cuenta de administrador CloudTrail delegado. El uso de un registro de la organización da como resultado un estado de control de `NO_DATA` de los controles evaluados en las cuentas de los miembros de la organización. En las cuentas de los miembros, Security Hub CSPM solo genera hallazgos para los recursos que pertenecen a los miembros. Los resultados relacionados con los registros de la organización se generan en la cuenta del propietario del recurso. Puede ver estos resultados en su cuenta de administrador delegado de CSPM de Security Hub mediante la agregación entre regiones.

Para la alarma, la cuenta corriente debe ser propietaria del tema de Amazon SNS al que se hace referencia o debe obtener acceso al tema de Amazon SNS llamando a `ListSubscriptionsByTopic`. De lo contrario, Security Hub CSPM `WARNING` generará resultados para el control.

Corrección

Para pasar este control, siga estos pasos para crear un tema de Amazon SNS, una ruta de AWS CloudTrail , un filtro de métricas y una alarma para el filtro de métricas.

1. Crear un tema de Amazon SNS Para obtener instrucciones, consulte Introducción a Amazon SNS en la Guía para desarrolladores de Amazon Simple Notification Service. Cree un tema que reciba todas las alarmas del CIS y cree al menos una suscripción al tema.
2. Cree una CloudTrail ruta que se aplique a todos. Regiones de AWS Para obtener instrucciones, consulte Crear un registro de seguimiento en la Guía del usuario de AWS CloudTrail .

   Anote el nombre del grupo de CloudWatch registros que asocie a la CloudTrail ruta. En el siguiente paso, debe crear el filtro de métricas para ese grupo de registros.
3. Crear un filtro de métricas. Para obtener instrucciones, consulte Crear un filtro métrico para un grupo de registros en la Guía del CloudWatch usuario de Amazon. Use los siguientes valores:

Campo	Valor
Defina el patrón, el patrón de filtro	`{($.errorCode="*UnauthorizedOperation") \|\| ($.errorCode="AccessDenied*")}`
Espacio de nombres de métrica	**`LogMetrics`**
Valor de la métrica	**`1`**
Predeterminado	**`0`**

4. Crear una alarma basada en el filtro. Para obtener instrucciones, consulte Crear una CloudWatch alarma basada en un filtro métrico de grupos de registros en la Guía del CloudWatch usuario de Amazon. Use los siguientes valores:

Campo	Valor
Condiciones, tipo de umbral	Estático
Siempre que sea... *your-metric-name*	Greater/Equal
que…	**1**

[CloudWatch.3] Asegúrese de que haya un registro, un filtro métrico y una alarma para iniciar sesión en la consola de administración sin MFA

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2. 0/31.2

Categoría: Detectar - Servicios de detección

Gravedad: baja

Tipo de recurso: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config regla: Ninguna (regla CSPM personalizada de Security Hub)

Tipo de programa: Periódico

Parámetros: ninguno

Para supervisar las llamadas a la API en tiempo real, dirija CloudTrail los CloudWatch registros a Logs y establezca las alarmas y los filtros métricos correspondientes.

CIS recomienda que cree un filtro de métricas y alarma para los inicios de sesión en la consola que no estén protegidos por MFA. La monitorización de los inicios de sesión de la consola con un solo factor aumenta la visibilidad de las cuentas que no están protegidas por MFA.

Para ejecutar esta comprobación, el CSPM de Security Hub utiliza una lógica personalizada para realizar los pasos de auditoría exactos prescritos para el control 3.2 en la versión 1.2 de CIS AWS Foundations Benchmark. Este control produce un error si no se utilizan los filtros de métricas exactos prescritos por CIS. No se pueden añadir campos ni términos adicionales a los filtros de métricas.

> **Note**
>
> Cuando Security Hub CSPM comprueba este control, busca los CloudTrail rastros que utiliza la cuenta actual. Estas rutas pueden ser rutas de organizaciones que pertenecen a otra cuenta. Multi-Region Las rutas también pueden estar ubicadas en una región diferente. La comprobación arroja resultados de `FAILED` en los siguientes casos:
>
> - No hay ningún rastro configurado.
> - Las rutas disponibles que se encuentran en la Región actual y que son propiedad de una cuenta corriente no cumplen con los requisitos de control.
>
> La comprobación da como resultado un estado de control de `NO_DATA` en los siguientes casos:
>
> - Una ruta multirregional se basa en una Región diferente. Security Hub CSPM solo puede generar hallazgos en la región en la que se encuentra la ruta.
> - Una ruta multirregional pertenece a una cuenta diferente. El CSPM de Security Hub solo puede generar hallazgos para la cuenta propietaria de la ruta.
>
> Como práctica recomendada, utilice los registros de la organización para registrar los eventos de muchas cuentas de una organización. Los registros organizacionales son registros multirregionales de forma predeterminada y solo los puede administrar la cuenta AWS Organizations de administración o la cuenta de administrador CloudTrail delegado. El uso de un registro de la organización da como resultado un estado de control de `NO_DATA` de los controles evaluados en las cuentas de los miembros de la organización. En las cuentas de los miembros, Security Hub CSPM solo genera hallazgos para los recursos que pertenecen a los miembros. Los resultados relacionados con los registros de la organización se generan en la cuenta del propietario del recurso. Puede ver estos resultados en su cuenta de administrador delegado de CSPM de Security Hub mediante la agregación entre regiones.
>
> Para la alarma, la cuenta corriente debe ser propietaria del tema de Amazon SNS al que se hace referencia o debe obtener acceso al tema de Amazon SNS llamando a `ListSubscriptionsByTopic`. De lo contrario, Security Hub CSPM `WARNING` generará resultados para el control.

Corrección

Para pasar este control, siga estos pasos para crear un tema de Amazon SNS, una ruta de AWS CloudTrail , un filtro de métricas y una alarma para el filtro de métricas.

1. Crear un tema de Amazon SNS Para obtener instrucciones, consulte Introducción a Amazon SNS en la Guía para desarrolladores de Amazon Simple Notification Service. Cree un tema que reciba todas las alarmas del CIS y cree al menos una suscripción al tema.
2. Cree una CloudTrail ruta que se aplique a todos. Regiones de AWS Para obtener instrucciones, consulte Crear un registro de seguimiento en la Guía del usuario de AWS CloudTrail .

   Anote el nombre del grupo de CloudWatch registros que asocie a la CloudTrail ruta. En el siguiente paso, debe crear el filtro de métricas para ese grupo de registros.
3. Crear un filtro de métricas. Para obtener instrucciones, consulte Crear un filtro métrico para un grupo de registros en la Guía del CloudWatch usuario de Amazon. Use los siguientes valores:

Campo	Valor
Defina el patrón, el patrón de filtro	`{ ($.eventName = "ConsoleLogin") && ($.additionalEventData.MFAUsed != "Yes") && ($.userIdentity.type = "IAMUser") && ($.responseElements.ConsoleLogin = "Success") }`
Espacio de nombres de métrica	**`LogMetrics`**
Valor de la métrica	**`1`**
Predeterminado	**`0`**

4. Crear una alarma basada en el filtro. Para obtener instrucciones, consulte Crear una CloudWatch alarma basada en un filtro métrico de grupos de registros en la Guía del CloudWatch usuario de Amazon. Use los siguientes valores:

Campo	Valor
Condiciones, tipo de umbral	Estático
Siempre que sea... *your-metric-name*	Greater/Equal
que…	**1**

[CloudWatch.4] Asegúrese de que haya un registro, un filtro métrico y una alarma para los cambios en las políticas de IAM

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2. 0/31.4, CIS AWS Foundations Benchmark v1.4. 0/44.4, 3.14.6, 3.14.7 NIST.800-171.r2 NIST.800-171.r2

Categoría: Detectar - Servicios de detección

Gravedad: baja

Tipo de recurso: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config regla: Ninguna (regla CSPM personalizada de Security Hub)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si se supervisan las llamadas a la API en tiempo real redirigiendo CloudTrail los CloudWatch registros a Logs y estableciendo las alarmas y los filtros métricos correspondientes.

CIS recomienda que cree un filtro de métricas y alarma para los cambios realizados a las políticas de IAM. La monitorización de estos cambios ayuda a garantizar que los controles de autenticación y autorización permanezcan intactos.

> **Note**
>
> Cuando Security Hub CSPM comprueba este control, busca los CloudTrail rastros que utiliza la cuenta actual. Estas rutas pueden ser rutas de organizaciones que pertenecen a otra cuenta. Multi-Region Las rutas también pueden estar ubicadas en una región diferente.
> La comprobación arroja resultados de `FAILED` en los siguientes casos:

- No hay ningún rastro configurado.
- Las rutas disponibles que se encuentran en la Región actual y que son propiedad de una cuenta corriente no cumplen con los requisitos de control.

La comprobación da como resultado un estado de control de `NO_DATA` en los siguientes casos:

- Una ruta multirregional se basa en una Región diferente. Security Hub CSPM solo puede generar hallazgos en la región en la que se encuentra la ruta.
- Una ruta multirregional pertenece a una cuenta diferente. El CSPM de Security Hub solo puede generar hallazgos para la cuenta propietaria de la ruta.

  Como práctica recomendada, utilice los registros de la organización para registrar los eventos de muchas cuentas de una organización. Los registros organizacionales son registros multirregionales de forma predeterminada y solo los puede administrar la cuenta AWS Organizations de administración o la cuenta de administrador CloudTrail delegado. El uso de un registro de la organización da como resultado un estado de control de `NO_DATA` de los controles evaluados en las cuentas de los miembros de la organización. En las cuentas de los miembros, Security Hub CSPM solo genera hallazgos para los recursos que pertenecen a los miembros. Los resultados relacionados con los registros de la organización se generan en la cuenta del propietario del recurso. Puede ver estos resultados en su cuenta de administrador delegado de CSPM de Security Hub mediante la agregación entre regiones.

Para la alarma, la cuenta corriente debe ser propietaria del tema de Amazon SNS al que se hace referencia o debe obtener acceso al tema de Amazon SNS llamando a `ListSubscriptionsByTopic`. De lo contrario, Security Hub CSPM `WARNING` generará resultados para el control.

Corrección

> **Note**
>
> El patrón de filtro que recomendamos en estos pasos de corrección difiere del patrón de filtro de la guía del CIS. Nuestros filtros recomendados se dirigen únicamente a los eventos que provienen de las llamadas a la API de IAM.

Para pasar este control, siga estos pasos para crear un tema de Amazon SNS, una ruta de AWS CloudTrail , un filtro de métricas y una alarma para el filtro de métricas.

1. Crear un tema de Amazon SNS Para obtener instrucciones, consulte Introducción a Amazon SNS en la Guía para desarrolladores de Amazon Simple Notification Service. Cree un tema que reciba todas las alarmas del CIS y cree al menos una suscripción al tema.
2. Cree una CloudTrail ruta que se aplique a todos. Regiones de AWS Para obtener instrucciones, consulte Crear un registro de seguimiento en la Guía del usuario de AWS CloudTrail .

   Anote el nombre del grupo de CloudWatch registros que asocie a la CloudTrail ruta. En el siguiente paso, debe crear el filtro de métricas para ese grupo de registros.
3. Crear un filtro de métricas. Para obtener instrucciones, consulte Crear un filtro métrico para un grupo de registros en la Guía del CloudWatch usuario de Amazon. Use los siguientes valores:

Campo	Valor
Defina el patrón, el patrón de filtro	`{($.eventSource=iam.amazonaws.com) && (($.eventName=DeleteGroupPolicy) || ($.eventName=DeleteRolePolicy) \|\| ($.eventName=DeleteUserPolicy) || ($.eventName=PutGroupPolicy) \|\| ($.eventName=PutRolePolicy) || ($.eventName=PutUserPolicy) \|\| ($.eventName=CreatePolicy) || ($.eventName=DeletePolicy) \|\| ($.eventName=CreatePolicyVersion) || ($.eventN`

Campo	Valor
	`ame=DeletePolicyVersion) || ($.eventName=AttachRolePolicy) \|\| ($.eventName=DetachRolePolicy) || ($.eventName=AttachUserPolicy) \|\| ($.eventName=DetachUserPolicy) || ($.eventName=AttachGroupPolicy) \|\| ($.eventName=DetachGroupPolicy))}`
Espacio de nombres de métrica	**`LogMetrics`**
Valor de la métrica	**`1`**
Predeterminado	**`0`**

4. Crear una alarma basada en el filtro. Para obtener instrucciones, consulte Crear una CloudWatch alarma basada en un filtro métrico de grupos de registros en la Guía del CloudWatch usuario de Amazon. Use los siguientes valores:

Campo	Valor
Condiciones, tipo de umbral	Estático
Siempre que sea... *`your-metric-name`*	Greater/Equal
que…	**`1`**

[CloudWatch.5] Asegúrese de que existan un registro, un filtro métrico y una alarma para los cambios CloudTrail de configuración

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2. 0/3.5, CIS AWS Foundations Benchmark v1.4. 0/4.5, NIST.800-171.r2 3.3.8, 3.14.6, 3.14.7 NIST.800-171.r2 NIST.800-171.r2

Categoría: Detectar - Servicios de detección

Gravedad: baja

Tipo de recurso: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config regla: Ninguna (regla CSPM personalizada de Security Hub)

Tipo de programa: Periódico

Parámetros: ninguno

Para supervisar las llamadas a la API en tiempo real, dirija CloudTrail los CloudWatch registros a Logs y establezca las alarmas y los filtros métricos correspondientes.

CIS recomienda que cree un filtro de métricas y alarma para los cambios a los ajustes de la configuración de CloudTrail. La monitorización de estos cambios ayuda a garantizar la visibilidad continua de las actividades de la cuenta.

Para ejecutar esta comprobación, el CSPM de Security Hub utiliza una lógica personalizada para realizar los pasos de auditoría exactos prescritos para el control 4.5 en la versión 1.4.0 de CIS AWS Foundations Benchmark. Este control produce un error si no se utilizan los filtros de métricas exactos prescritos por CIS. No se pueden añadir campos ni términos adicionales a los filtros de métricas.

> **Note**
>
> Cuando Security Hub CSPM comprueba este control, busca los CloudTrail rastros que utiliza la cuenta actual. Estas rutas pueden ser rutas de organizaciones que pertenecen a otra cuenta. Multi-Region Las rutas también pueden estar ubicadas en una región diferente.
> La comprobación arroja resultados de `FAILED` en los siguientes casos:
>
> - No hay ningún rastro configurado.
> - Las rutas disponibles que se encuentran en la Región actual y que son propiedad de una cuenta corriente no cumplen con los requisitos de control.
>
> La comprobación da como resultado un estado de control de `NO_DATA` en los siguientes casos:
>
> - Una ruta multirregional se basa en una Región diferente. Security Hub CSPM solo puede generar hallazgos en la región en la que se encuentra la ruta.
> - Una ruta multirregional pertenece a una cuenta diferente. El CSPM de Security Hub solo puede generar hallazgos para la cuenta propietaria de la ruta.

Como práctica recomendada, utilice los registros de la organización para registrar los eventos de muchas cuentas de una organización. Los registros organizacionales son registros multirregionales de forma predeterminada y solo los puede administrar la cuenta AWS Organizations de administración o la cuenta de administrador CloudTrail delegado. El uso de un registro de la organización da como resultado un estado de control de `NO_DATA` de los controles evaluados en las cuentas de los miembros de la organización. En las cuentas de los miembros, Security Hub CSPM solo genera hallazgos para los recursos que pertenecen a los miembros. Los resultados relacionados con los registros de la organización se generan en la cuenta del propietario del recurso. Puede ver estos resultados en su cuenta de administrador delegado de CSPM de Security Hub mediante la agregación entre regiones.

Para la alarma, la cuenta corriente debe ser propietaria del tema de Amazon SNS al que se hace referencia o debe obtener acceso al tema de Amazon SNS llamando a `ListSubscriptionsByTopic`. De lo contrario, Security Hub CSPM `WARNING` generará resultados para el control.

Corrección

Para pasar este control, siga estos pasos para crear un tema de Amazon SNS, una ruta de AWS CloudTrail , un filtro de métricas y una alarma para el filtro de métricas.

1. Crear un tema de Amazon SNS Para obtener instrucciones, consulte Introducción a Amazon SNS en la Guía para desarrolladores de Amazon Simple Notification Service. Cree un tema que reciba todas las alarmas del CIS y cree al menos una suscripción al tema.
2. Cree una CloudTrail ruta que se aplique a todos. Regiones de AWS Para obtener instrucciones, consulte Crear un registro de seguimiento en la Guía del usuario de AWS CloudTrail .

   Anote el nombre del grupo de CloudWatch registros que asocie a la CloudTrail ruta. En el siguiente paso, debe crear el filtro de métricas para ese grupo de registros.
3. Crear un filtro de métricas. Para obtener instrucciones, consulte Crear un filtro métrico para un grupo de registros en la Guía del CloudWatch usuario de Amazon. Use los siguientes valores:

Campo	Valor
Defina el patrón, el patrón de filtro	`{($.eventName=CreateTrail) \|\| ($.eventName=UpdateTrail) || ($.eventName=DeleteTrail) \|\| ($.eventName=StartLogging) || ($.eventName=StopLogging)}`
Espacio de nombres de métrica	**`LogMetrics`**
Valor de la métrica	**`1`**
Predeterminado	**`0`**

4. Crear una alarma basada en el filtro. Para obtener instrucciones, consulte Crear una CloudWatch alarma basada en un filtro métrico de grupos de registros en la Guía del CloudWatch usuario de Amazon. Use los siguientes valores:

Campo	Valor
Condiciones, tipo de umbral	Estático
Siempre *`your-metric-name`* es...	Greater/Equal
que…	**`1`**

[CloudWatch.6] Asegúrese de que existan un registro métrico, un filtro y una alarma para Consola de administración de AWS errores de autenticación

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2. 0/31.6, CIS AWS Foundations Benchmark v1.4. 0/43.6, 3.14.6, NIST.800-171.r2 3.14.7 NIST.800-171.r2

Categoría: Detectar - Servicios de detección

Gravedad: baja

Tipo de recurso: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config regla: Ninguna (regla CSPM personalizada de Security Hub)

Tipo de programa: Periódico

Parámetros: ninguno

Para supervisar las llamadas a la API en tiempo real, dirija CloudTrail los CloudWatch registros a Logs y establezca las alarmas y los filtros métricos correspondientes.

CIS recomienda que cree un filtro de métrica y alarma para los intentos de autenticación de la consola que producen un error. La monitorización de los inicios de sesión con error en la consola podría disminuir el tiempo que se tarda en detectar un intento introducir credenciales por fuerza bruta, lo que podría proporcionar un indicador, como el IP de origen, que se puede utilizar en otras correlaciones de eventos.

Para ejecutar esta comprobación, el CSPM de Security Hub utiliza una lógica personalizada para realizar los pasos de auditoría exactos prescritos para el control 4.6 en la versión 1.4.0 de CIS AWS Foundations Benchmark. Este control produce un error si no se utilizan los filtros de métricas exactos prescritos por CIS. No se pueden añadir campos ni términos adicionales a los filtros de métricas.

> **Note**
>
> Cuando Security Hub CSPM comprueba este control, busca los CloudTrail rastros que utiliza la cuenta actual. Estas rutas pueden ser rutas de organizaciones que pertenecen a otra cuenta. Multi-Region Las rutas también pueden estar ubicadas en una región diferente.
> La comprobación arroja resultados de `FAILED` en los siguientes casos:
>
> - No hay ningún rastro configurado.
> - Las rutas disponibles que se encuentran en la Región actual y que son propiedad de una cuenta corriente no cumplen con los requisitos de control.
>
> La comprobación da como resultado un estado de control de `NO_DATA` en los siguientes casos:
>
> - Una ruta multirregional se basa en una Región diferente. Security Hub CSPM solo puede generar hallazgos en la región en la que se encuentra la ruta.
> - Una ruta multirregional pertenece a una cuenta diferente. El CSPM de Security Hub solo puede generar hallazgos para la cuenta propietaria de la ruta.

Como práctica recomendada, utilice los registros de la organización para registrar los eventos de muchas cuentas de una organización. Los registros organizacionales son registros multirregionales de forma predeterminada y solo los puede administrar la cuenta AWS Organizations de administración o la cuenta de administrador CloudTrail delegado. El uso de un registro de la organización da como resultado un estado de control de `NO_DATA` de los controles evaluados en las cuentas de los miembros de la organización. En las cuentas de los miembros, Security Hub CSPM solo genera hallazgos para los recursos que pertenecen a los miembros. Los resultados relacionados con los registros de la organización se generan en la cuenta del propietario del recurso. Puede ver estos resultados en su cuenta de administrador delegado de CSPM de Security Hub mediante la agregación entre regiones.

Para la alarma, la cuenta corriente debe ser propietaria del tema de Amazon SNS al que se hace referencia o debe obtener acceso al tema de Amazon SNS llamando a `ListSubscriptionsByTopic`. De lo contrario, Security Hub CSPM `WARNING` generará resultados para el control.

Corrección

Para pasar este control, siga estos pasos para crear un tema de Amazon SNS, una ruta de AWS CloudTrail , un filtro de métricas y una alarma para el filtro de métricas.

1. Crear un tema de Amazon SNS Para obtener instrucciones, consulte Introducción a Amazon SNS en la Guía para desarrolladores de Amazon Simple Notification Service. Cree un tema que reciba todas las alarmas del CIS y cree al menos una suscripción al tema.
2. Cree una CloudTrail ruta que se aplique a todos. Regiones de AWS Para obtener instrucciones, consulte Crear un registro de seguimiento en la Guía del usuario de AWS CloudTrail .

   Anote el nombre del grupo de CloudWatch registros que asocie a la CloudTrail ruta. En el siguiente paso, debe crear el filtro de métricas para ese grupo de registros.
3. Crear un filtro de métricas. Para obtener instrucciones, consulte Crear un filtro métrico para un grupo de registros en la Guía del CloudWatch usuario de Amazon. Use los siguientes valores:

Campo	Valor
Defina el patrón, el patrón de filtro	`{($.eventName=ConsoleLogin) && ($.errorMessage="Failed authentication")}`
Espacio de nombres de métrica	**`LogMetrics`**
Valor de la métrica	**`1`**
Predeterminado	**`0`**

4. Crear una alarma basada en el filtro. Para obtener instrucciones, consulte Crear una CloudWatch alarma basada en un filtro métrico de grupos de registros en la Guía del CloudWatch usuario de Amazon. Use los siguientes valores:

Campo	Valor
Condiciones, tipo de umbral	Estático
Siempre *`your-metric-name`* es...	Greater/Equal
que…	**`1`**

[CloudWatch.7] Asegúrese de que haya un registro, un filtro métrico y una alarma para deshabilitar o programar la eliminación de las claves administradas por el cliente

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2. 0/31.7, CIS AWS Foundations Benchmark v1.4. 0/4.7, NIST.800-171.r2 3.13.10, 3.13.16, 3.14.6, NIST.800-171.r2 3.14.7 NIST.800-171.r2 NIST.800-171.r2

Categoría: Detectar - Servicios de detección

Gravedad: baja

Tipo de recurso: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config regla: Ninguna (regla CSPM personalizada de Security Hub)

Tipo de programa: Periódico

Parámetros: ninguno

Para supervisar las llamadas a la API en tiempo real, dirija CloudTrail los CloudWatch registros a Logs y establezca las alarmas y los filtros métricos correspondientes.

CIS recomienda que cree un filtro de métricas y alarma para claves administradas por el cliente que hayan cambiado de estado a deshabilitada o eliminación programada. Los datos cifrados con claves deshabilitadas o eliminadas ya no son accesibles.

Para ejecutar esta comprobación, el CSPM de Security Hub utiliza una lógica personalizada para realizar los pasos de auditoría exactos prescritos para el control 4.7 en la versión 1.4.0 de CIS AWS Foundations Benchmark. Este control produce un error si no se utilizan los filtros de métricas exactos prescritos por CIS. No se pueden añadir campos ni términos adicionales a los filtros de métricas. El control también falla si `ExcludeManagementEventSources` contiene `kms.amazonaws.com`.

> **Note**
>
> Cuando Security Hub CSPM comprueba este control, busca los CloudTrail rastros que utiliza la cuenta actual. Estas rutas pueden ser rutas de organizaciones que pertenecen a otra cuenta. Multi-Region Las rutas también pueden estar ubicadas en una región diferente. La comprobación arroja resultados de `FAILED` en los siguientes casos:
>
> - No hay ningún rastro configurado.
> - Las rutas disponibles que se encuentran en la Región actual y que son propiedad de una cuenta corriente no cumplen con los requisitos de control.
>
> La comprobación da como resultado un estado de control de `NO_DATA` en los siguientes casos:
>
> - Una ruta multirregional se basa en una Región diferente. Security Hub CSPM solo puede generar hallazgos en la región en la que se encuentra la ruta.
> - Una ruta multirregional pertenece a una cuenta diferente. El CSPM de Security Hub solo puede generar hallazgos para la cuenta propietaria de la ruta.
>
> Como práctica recomendada, utilice los registros de la organización para registrar los eventos de muchas cuentas de una organización. Los registros organizacionales son

registros multirregionales de forma predeterminada y solo los puede administrar la cuenta AWS Organizations de administración o la cuenta de administrador CloudTrail delegado. El uso de un registro de la organización da como resultado un estado de control de `NO_DATA` de los controles evaluados en las cuentas de los miembros de la organización. En las cuentas de los miembros, Security Hub CSPM solo genera hallazgos para los recursos que pertenecen a los miembros. Los resultados relacionados con los registros de la organización se generan en la cuenta del propietario del recurso. Puede ver estos resultados en su cuenta de administrador delegado de CSPM de Security Hub mediante la agregación entre regiones.

Para la alarma, la cuenta corriente debe ser propietaria del tema de Amazon SNS al que se hace referencia o debe obtener acceso al tema de Amazon SNS llamando a `ListSubscriptionsByTopic`. De lo contrario, Security Hub CSPM `WARNING` generará resultados para el control.

Corrección

Para pasar este control, siga estos pasos para crear un tema de Amazon SNS, una ruta de AWS CloudTrail , un filtro de métricas y una alarma para el filtro de métricas.

1. Crear un tema de Amazon SNS Para obtener instrucciones, consulte Introducción a Amazon SNS en la Guía para desarrolladores de Amazon Simple Notification Service. Cree un tema que reciba todas las alarmas del CIS y cree al menos una suscripción al tema.
2. Cree una CloudTrail ruta que se aplique a todos. Regiones de AWS Para obtener instrucciones, consulte Crear un registro de seguimiento en la Guía del usuario de AWS CloudTrail .

   Anote el nombre del grupo de CloudWatch registros que asocie a la CloudTrail ruta. En el siguiente paso, debe crear el filtro de métricas para ese grupo de registros.
3. Crear un filtro de métricas. Para obtener instrucciones, consulte Crear un filtro métrico para un grupo de registros en la Guía del CloudWatch usuario de Amazon. Use los siguientes valores:

Campo	Valor
Defina el patrón, el patrón de filtro	`{($.eventSource=kms.amazonaws.com) && (($.eventName=Disa`

Campo	Valor
	`bleKey) || ($.eventName=Sched uleKeyDeletion))}`
Espacio de nombres de métrica	**`LogMetrics`**
Valor de la métrica	**`1`**
Predeterminado	**`0`**

4. Crear una alarma basada en el filtro. Para obtener instrucciones, consulte Crear una CloudWatch alarma basada en un filtro métrico de grupos de registros en la Guía del CloudWatch usuario de Amazon. Use los siguientes valores:

Campo	Valor
Condiciones, tipo de umbral	Estático
Siempre *`your-metric-name`* es...	Greater/Equal
que…	**`1`**

[CloudWatch.8] Asegúrese de que haya un registro, un filtro métrico y una alarma para los cambios en la política de buckets de S3

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2. 0/33.8, CIS AWS Foundations Benchmark v1.4. 0/43.8, 3.14.6, NIST.800-171.r2 3.14.7 NIST.800-171.r2

Categoría: Detectar - Servicios de detección

Gravedad: baja

Tipo de recurso: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config regla: Ninguna (regla CSPM personalizada de Security Hub)

Tipo de programa: Periódico

Parámetros: ninguno

Para supervisar las llamadas a la API en tiempo real, dirija CloudTrail los CloudWatch registros a Logs y establezca las alarmas y los filtros métricos correspondientes.

CIS recomienda que cree un filtro de métricas y alarma para los cambios realizados a las políticas de bucket S3. La monitorización de estos cambios puede reducir el tiempo que se tarda en detectar y corregir políticas permisivas sobre buckets de S3 confidenciales.

Para ejecutar esta comprobación, el CSPM de Security Hub utiliza una lógica personalizada para realizar los pasos de auditoría exactos prescritos para el control 4.8 en la versión 1.4.0 de CIS AWS Foundations Benchmark. Este control produce un error si no se utilizan los filtros de métricas exactos prescritos por CIS. No se pueden añadir campos ni términos adicionales a los filtros de métricas.

> **Note**
>
> Cuando Security Hub CSPM comprueba este control, busca los CloudTrail rastros que utiliza la cuenta actual. Estas rutas pueden ser rutas de organizaciones que pertenecen a otra cuenta. Multi-Region Las rutas también pueden estar ubicadas en una región diferente. La comprobación arroja resultados de `FAILED` en los siguientes casos:
>
> - No hay ningún rastro configurado.
> - Las rutas disponibles que se encuentran en la Región actual y que son propiedad de una cuenta corriente no cumplen con los requisitos de control.
>
> La comprobación da como resultado un estado de control de `NO_DATA` en los siguientes casos:
>
> - Una ruta multirregional se basa en una Región diferente. Security Hub CSPM solo puede generar hallazgos en la región en la que se encuentra la ruta.
> - Una ruta multirregional pertenece a una cuenta diferente. El CSPM de Security Hub solo puede generar hallazgos para la cuenta propietaria de la ruta.
>
> Como práctica recomendada, utilice los registros de la organización para registrar los eventos de muchas cuentas de una organización. Los registros organizacionales son registros multirregionales de forma predeterminada y solo los puede administrar la cuenta AWS Organizations de administración o la cuenta de administrador CloudTrail delegado. El uso de un registro de la organización da como resultado un estado de control de `NO_DATA` de los controles evaluados en las cuentas de los miembros de la organización.

En las cuentas de los miembros, Security Hub CSPM solo genera hallazgos para los recursos que pertenecen a los miembros. Los resultados relacionados con los registros de la organización se generan en la cuenta del propietario del recurso. Puede ver estos resultados en su cuenta de administrador delegado de CSPM de Security Hub mediante la agregación entre regiones.

Para la alarma, la cuenta corriente debe ser propietaria del tema de Amazon SNS al que se hace referencia o debe obtener acceso al tema de Amazon SNS llamando a `ListSubscriptionsByTopic`. De lo contrario, Security Hub CSPM `WARNING` generará resultados para el control.

Corrección

Para pasar este control, siga estos pasos para crear un tema de Amazon SNS, una ruta de AWS CloudTrail , un filtro de métricas y una alarma para el filtro de métricas.

1. Crear un tema de Amazon SNS Para obtener instrucciones, consulte Introducción a Amazon SNS en la Guía para desarrolladores de Amazon Simple Notification Service. Cree un tema que reciba todas las alarmas del CIS y cree al menos una suscripción al tema.
2. Cree una CloudTrail ruta que se aplique a todos. Regiones de AWS Para obtener instrucciones, consulte Crear un registro de seguimiento en la Guía del usuario de AWS CloudTrail .

   Anote el nombre del grupo de CloudWatch registros que asocie a la CloudTrail ruta. En el siguiente paso, debe crear el filtro de métricas para ese grupo de registros.
3. Crear un filtro de métricas. Para obtener instrucciones, consulte Crear un filtro métrico para un grupo de registros en la Guía del CloudWatch usuario de Amazon. Use los siguientes valores:

Campo	Valor
Defina el patrón, el patrón de filtro	`{($.eventSource=s3.amazonaws.com) && (($.eventName=PutBucketAcl) || ($.eventName=PutBucketPolicy) \|\| ($.eventName=PutBucketCors) || ($.eventName=PutBucketLifecycle) \|\| ($.eventName=PutBucketRepli`

Campo	Valor
	`cation) || ($.eventName=DeleteBucketPolicy) \|\| ($.eventName=DeleteBucketCors) || ($.eventName=DeleteBucketLifecycle) \|\| ($.eventName=DeleteBucketReplication))}`
Espacio de nombres de métrica	**`LogMetrics`**
Valor de la métrica	**`1`**
Predeterminado	**`0`**

4. Crear una alarma basada en el filtro. Para obtener instrucciones, consulte Crear una CloudWatch alarma basada en un filtro métrico de grupos de registros en la Guía del CloudWatch usuario de Amazon. Use los siguientes valores:

Campo	Valor
Condiciones, tipo de umbral	Estático
Siempre *`your-metric-name`* es...	Greater/Equal
que…	**`1`**

[CloudWatch.9] Asegúrese de que existan un registro métrico, un filtro y una alarma para AWS Config cambios de configuración

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2. 0/32.9, CIS AWS Foundations Benchmark v1.4. 0/49.9, NIST.800-171.r2 3.3.8, 3.14.6, 3.14.7 NIST.800-171.r2 NIST.800-171.r2

Categoría: Detectar - Servicios de detección

Gravedad: baja

Tipo de recurso: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config regla: Ninguna (regla CSPM personalizada de Security Hub)

Tipo de programa: Periódico

Parámetros: ninguno

Para supervisar las llamadas a la API en tiempo real, dirija CloudTrail los CloudWatch registros a Logs y establezca las alarmas y los filtros métricos correspondientes.

CIS recomienda que cree un filtro de métricas y alarma para los cambios a los ajustes de la configuración de AWS Config . La monitorización de estos cambios ayuda a garantizar la visibilidad continua de los elementos de configuración de la cuenta.

Para ejecutar esta comprobación, el CSPM de Security Hub utiliza una lógica personalizada para realizar los pasos de auditoría exactos prescritos para el control 4.9 en la versión 1.4.0 de CIS AWS Foundations Benchmark. Este control produce un error si no se utilizan los filtros de métricas exactos prescritos por CIS. No se pueden añadir campos ni términos adicionales a los filtros de métricas.

> **Note**
>
> Cuando Security Hub CSPM comprueba este control, busca los CloudTrail rastros que utiliza la cuenta actual. Estas rutas pueden ser rutas de organizaciones que pertenecen a otra cuenta. Multi-Region Las rutas también pueden estar ubicadas en una región diferente. La comprobación arroja resultados de `FAILED` en los siguientes casos:
>
> - No hay ningún rastro configurado.
> - Las rutas disponibles que se encuentran en la Región actual y que son propiedad de una cuenta corriente no cumplen con los requisitos de control.
>
> La comprobación da como resultado un estado de control de `NO_DATA` en los siguientes casos:
>
> - Una ruta multirregional se basa en una Región diferente. Security Hub CSPM solo puede generar hallazgos en la región en la que se encuentra la ruta.
> - Una ruta multirregional pertenece a una cuenta diferente. El CSPM de Security Hub solo puede generar hallazgos para la cuenta propietaria de la ruta.
>
> Como práctica recomendada, utilice los registros de la organización para registrar los eventos de muchas cuentas de una organización. Los registros organizacionales son

registros multirregionales de forma predeterminada y solo los puede administrar la cuenta AWS Organizations de administración o la cuenta de administrador CloudTrail delegado. El uso de un registro de la organización da como resultado un estado de control de `NO_DATA` de los controles evaluados en las cuentas de los miembros de la organización. En las cuentas de los miembros, Security Hub CSPM solo genera hallazgos para los recursos que pertenecen a los miembros. Los resultados relacionados con los registros de la organización se generan en la cuenta del propietario del recurso. Puede ver estos resultados en su cuenta de administrador delegado de CSPM de Security Hub mediante la agregación entre regiones.

Para la alarma, la cuenta corriente debe ser propietaria del tema de Amazon SNS al que se hace referencia o debe obtener acceso al tema de Amazon SNS llamando a `ListSubscriptionsByTopic`. De lo contrario, Security Hub CSPM `WARNING` generará resultados para el control.

Corrección

Para pasar este control, siga estos pasos para crear un tema de Amazon SNS, una ruta de AWS CloudTrail , un filtro de métricas y una alarma para el filtro de métricas.

1. Crear un tema de Amazon SNS Para obtener instrucciones, consulte Introducción a Amazon SNS en la Guía para desarrolladores de Amazon Simple Notification Service. Cree un tema que reciba todas las alarmas del CIS y cree al menos una suscripción al tema.
2. Cree una CloudTrail ruta que se aplique a todos. Regiones de AWS Para obtener instrucciones, consulte Crear un registro de seguimiento en la Guía del usuario de AWS CloudTrail .

   Anote el nombre del grupo de CloudWatch registros que asocie a la CloudTrail ruta. En el siguiente paso, debe crear el filtro de métricas para ese grupo de registros.
3. Crear un filtro de métricas. Para obtener instrucciones, consulte Crear un filtro métrico para un grupo de registros en la Guía del CloudWatch usuario de Amazon. Use los siguientes valores:

Campo	Valor
Defina el patrón, el patrón de filtro	`{($.eventSource=config.amazonaws.com) && ($.eventName=StopConfigurationRecor`

Campo	Valor
	`der) || ($.eventName=DeleteDeliveryChannel) \|\| ($.eventName=PutDeliveryChannel) || ($.eventName=PutConfigurationRecorder))}`
Espacio de nombres de métrica	**`LogMetrics`**
Valor de la métrica	**`1`**
Predeterminado	**`0`**

4. Crear una alarma basada en el filtro. Para obtener instrucciones, consulte Crear una CloudWatch alarma basada en un filtro métrico de grupos de registros en la Guía del CloudWatch usuario de Amazon. Use los siguientes valores:

Campo	Valor
Condiciones, tipo de umbral	Estático
Siempre *`your-metric-name`* es...	Greater/Equal
que…	**`1`**

[CloudWatch.10] Asegúrese de que haya un registro, un filtro métrico y una alarma para los cambios en los grupos de seguridad

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2. 0/31.0, CIS AWS Foundations Benchmark v1.4. 0/41.0, 3.14.6, 3.14.7 NIST.800-171.r2 NIST.800-171.r2

Categoría: Detectar - Servicios de detección

Gravedad: baja

Tipo de recurso: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config regla: Ninguna (regla CSPM personalizada de Security Hub)

Tipo de programa: Periódico

Parámetros: ninguno

Para supervisar las llamadas a la API en tiempo real, dirija CloudTrail los CloudWatch registros a Logs y establezca las alarmas y los filtros métricos correspondientes. Los grupos de seguridad son un filtro de paquetes con estado que controlan el tráfico de entrada y salida en una VPC.

CIS recomienda que cree un filtro de métricas y alarma para los cambios realizados a los grupos de seguridad. La monitorización de estos cambios ayuda a garantizar que los recursos y servicios no se expongan de forma involuntaria.

Para ejecutar esta comprobación, el CSPM de Security Hub utiliza una lógica personalizada para realizar los pasos de auditoría exactos prescritos para el control 4.10 en la versión 1.4.0 de CIS AWS Foundations Benchmark. Este control produce un error si no se utilizan los filtros de métricas exactos prescritos por CIS. No se pueden añadir campos ni términos adicionales a los filtros de métricas.

> **Note**
>
> Cuando Security Hub CSPM comprueba este control, busca los rastros que utiliza la cuenta actual. CloudTrail Estas rutas pueden ser rutas de organizaciones que pertenecen a otra cuenta. Multi-Region Las rutas también pueden estar ubicadas en una región diferente. La comprobación arroja resultados de `FAILED` en los siguientes casos:
>
> - No hay ningún rastro configurado.
> - Las rutas disponibles que se encuentran en la Región actual y que son propiedad de una cuenta corriente no cumplen con los requisitos de control.
>
> La comprobación da como resultado un estado de control de `NO_DATA` en los siguientes casos:
>
> - Una ruta multirregional se basa en una Región diferente. Security Hub CSPM solo puede generar hallazgos en la región en la que se encuentra la ruta.
> - Una ruta multirregional pertenece a una cuenta diferente. El CSPM de Security Hub solo puede generar hallazgos para la cuenta propietaria de la ruta.
>
> Como práctica recomendada, utilice los registros de la organización para registrar los eventos de muchas cuentas de una organización. Los registros organizacionales son

registros multirregionales de forma predeterminada y solo los puede administrar la cuenta AWS Organizations de administración o la cuenta de administrador CloudTrail delegado. El uso de un registro de la organización da como resultado un estado de control de `NO_DATA` de los controles evaluados en las cuentas de los miembros de la organización. En las cuentas de los miembros, Security Hub CSPM solo genera hallazgos para los recursos que pertenecen a los miembros. Los resultados relacionados con los registros de la organización se generan en la cuenta del propietario del recurso. Puede ver estos resultados en su cuenta de administrador delegado de CSPM de Security Hub mediante la agregación entre regiones.

Para la alarma, la cuenta corriente debe ser propietaria del tema de Amazon SNS al que se hace referencia o debe obtener acceso al tema de Amazon SNS llamando a `ListSubscriptionsByTopic`. De lo contrario, Security Hub CSPM `WARNING` generará resultados para el control.

Corrección

Para pasar este control, siga estos pasos para crear un tema de Amazon SNS, una ruta de AWS CloudTrail , un filtro de métricas y una alarma para el filtro de métricas.

1. Crear un tema de Amazon SNS Para obtener instrucciones, consulte Introducción a Amazon SNS en la Guía para desarrolladores de Amazon Simple Notification Service. Cree un tema que reciba todas las alarmas del CIS y cree al menos una suscripción al tema.
2. Cree una CloudTrail ruta que se aplique a todos. Regiones de AWS Para obtener instrucciones, consulte Crear un registro de seguimiento en la Guía del usuario de AWS CloudTrail .

   Anote el nombre del grupo de CloudWatch registros que asocie a la CloudTrail ruta. En el siguiente paso, debe crear el filtro de métricas para ese grupo de registros.
3. Crear un filtro de métricas. Para obtener instrucciones, consulte Crear un filtro métrico para un grupo de registros en la Guía del CloudWatch usuario de Amazon. Use los siguientes valores:

Campo	Valor
Defina el patrón, el patrón de filtro	`{($.eventName=AuthorizeSecurityGroupIngress) \|\| ($.eventName=AuthorizeSecurityGroupE`

Campo	Valor
	`gress) || ($.eventName=RevokeSecurityGroupIngress) \|\| ($.eventName=RevokeSecurityGroupEgress) || ($.eventName=CreateSecurityGroup) \|\| ($.eventName=DeleteSecurityGroup)}`
Espacio de nombres de métrica	**`LogMetrics`**
Valor de la métrica	**`1`**
Predeterminado	**`0`**

4. Crear una alarma basada en el filtro. Para obtener instrucciones, consulte Crear una CloudWatch alarma basada en un filtro métrico de grupos de registros en la Guía del CloudWatch usuario de Amazon. Use los siguientes valores:

Campo	Valor
Condiciones, tipo de umbral	Estático
Siempre *`your-metric-name`* es...	Greater/Equal
que…	**`1`**

[CloudWatch.11] Asegúrese de que existan un filtro métrico de registro y una alarma para los cambios en las listas de control de acceso a la red (NACL)

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2. 0/31.1, CIS AWS Foundations Benchmark v1.4. 0/41.1, 3.14.6, 3.14.7 NIST.800-171.r2 NIST.800-171.r2

Categoría: Detectar - Servicios de detección

Gravedad: baja

Tipo de recurso: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config regla: Ninguna (regla CSPM personalizada de Security Hub)

Tipo de programa: Periódico

Parámetros: ninguno

Para supervisar las llamadas a la API en tiempo real, dirija CloudTrail los CloudWatch registros a Logs y establezca las alarmas y los filtros métricos correspondientes. Las NACL se utilizan como un filtro de paquetes sin estado para controlar el tráfico de entrada y salida para las subredes en una VPC.

CIS recomienda que cree un filtro de métricas y alarma para los cambios realizados a las NACL. La supervisión de estos cambios ayuda a garantizar que AWS los recursos y los servicios no queden expuestos de forma involuntaria.

Para ejecutar esta comprobación, el CSPM de Security Hub utiliza una lógica personalizada para realizar exactamente los pasos de auditoría prescritos para el control 4.11 en la versión 1.4.0 de CIS AWS Foundations Benchmark. Este control produce un error si no se utilizan los filtros de métricas exactos prescritos por CIS. No se pueden añadir campos ni términos adicionales a los filtros de métricas.

> **Note**
>
> Cuando Security Hub CSPM comprueba este control, busca los rastros que utiliza la cuenta actual. CloudTrail Estas rutas pueden ser rutas de organizaciones que pertenecen a otra cuenta. Multi-Region Las rutas también pueden estar ubicadas en una región diferente.
> La comprobación arroja resultados de `FAILED` en los siguientes casos:
>
> - No hay ningún rastro configurado.
> - Las rutas disponibles que se encuentran en la Región actual y que son propiedad de una cuenta corriente no cumplen con los requisitos de control.
>
> La comprobación da como resultado un estado de control de `NO_DATA` en los siguientes casos:
>
> - Una ruta multirregional se basa en una Región diferente. Security Hub CSPM solo puede generar hallazgos en la región en la que se encuentra la ruta.
> - Una ruta multirregional pertenece a una cuenta diferente. El CSPM de Security Hub solo puede generar hallazgos para la cuenta propietaria de la ruta.

Como práctica recomendada, utilice los registros de la organización para registrar los eventos de muchas cuentas de una organización. Los registros organizacionales son registros multirregionales de forma predeterminada y solo los puede administrar la cuenta AWS Organizations de administración o la cuenta de administrador CloudTrail delegado. El uso de un registro de la organización da como resultado un estado de control de `NO_DATA` de los controles evaluados en las cuentas de los miembros de la organización. En las cuentas de los miembros, Security Hub CSPM solo genera hallazgos para los recursos que pertenecen a los miembros. Los resultados relacionados con los registros de la organización se generan en la cuenta del propietario del recurso. Puede ver estos resultados en su cuenta de administrador delegado de CSPM de Security Hub mediante la agregación entre regiones.

Para la alarma, la cuenta corriente debe ser propietaria del tema de Amazon SNS al que se hace referencia o debe obtener acceso al tema de Amazon SNS llamando a `ListSubscriptionsByTopic`. De lo contrario, Security Hub CSPM `WARNING` generará resultados para el control.

Corrección

Para pasar este control, siga estos pasos para crear un tema de Amazon SNS, una ruta de AWS CloudTrail , un filtro de métricas y una alarma para el filtro de métricas.

1. Crear un tema de Amazon SNS Para obtener instrucciones, consulte Introducción a Amazon SNS en la Guía para desarrolladores de Amazon Simple Notification Service. Cree un tema que reciba todas las alarmas del CIS y cree al menos una suscripción al tema.
2. Cree una CloudTrail ruta que se aplique a todos. Regiones de AWS Para obtener instrucciones, consulte Crear un registro de seguimiento en la Guía del usuario de AWS CloudTrail .

   Anote el nombre del grupo de CloudWatch registros que asocie a la CloudTrail ruta. En el siguiente paso, debe crear el filtro de métricas para ese grupo de registros.
3. Crear un filtro de métricas. Para obtener instrucciones, consulte Crear un filtro métrico para un grupo de registros en la Guía del CloudWatch usuario de Amazon. Use los siguientes valores:

Campo	Valor
Defina el patrón, el patrón de filtro	`{($.eventName=CreateNetworkAcl) \|\| ($.eventName=CreateNetworkAclEntry) || ($.eventName=DeleteNetworkAcl) \|\| ($.eventName=DeleteNetworkAclEntry) || ($.eventName=ReplaceNetworkAclEntry) \|\| ($.eventName=ReplaceNetworkAclAssociation)}`
Espacio de nombres de métrica	**`LogMetrics`**
Valor de la métrica	**`1`**
Predeterminado	**`0`**

4. Crear una alarma basada en el filtro. Para obtener instrucciones, consulte Crear una CloudWatch alarma basada en un filtro métrico de grupos de registros en la Guía del CloudWatch usuario de Amazon. Use los siguientes valores:

Campo	Valor
Condiciones, tipo de umbral	Estático
Siempre que sea... *`your-metric-name`*	Greater/Equal
que…	**`1`**

[CloudWatch.12] Asegúrese de que haya un registro, un filtro métrico y una alarma para detectar los cambios en las pasarelas de red

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2. 0/31.2, CIS AWS Foundations Benchmark v1.4. 0/41.2, 3.3.1, 3.13.1 NIST.800-171.r2 NIST.800-171.r2

Categoría: Detectar - Servicios de detección

Gravedad: baja

Tipo de recurso: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config regla: Ninguna (regla CSPM personalizada de Security Hub)

Tipo de programa: Periódico

Parámetros: ninguno

Para supervisar las llamadas a la API en tiempo real, dirija CloudTrail los CloudWatch registros a Logs y establezca las alarmas y los filtros métricos correspondientes. Las gateways de red son necesarias para enviar y recibir tráfico a un destino fuera de una VPC.

CIS recomienda que cree un filtro de métricas y alarma para los cambios realizados a las puertas de enlace de red. La monitorización de estos cambios ayuda a garantizar que todo el tráfico de entrada y salida atraviesa la frontera de la VPC a través de una ruta controlada.

Para ejecutar esta comprobación, el CSPM de Security Hub utiliza una lógica personalizada para realizar los pasos de auditoría exactos prescritos para el control 4.12 en la versión 1.2 de CIS AWS Foundations Benchmark. Este control produce un error si no se utilizan los filtros de métricas exactos prescritos por CIS. No se pueden añadir campos ni términos adicionales a los filtros de métricas.

> **Note**
>
> Cuando Security Hub CSPM comprueba este control, busca los CloudTrail rastros que utiliza la cuenta actual. Estas rutas pueden ser rutas de organizaciones que pertenecen a otra cuenta. Multi-Region Las rutas también pueden estar ubicadas en una región diferente. La comprobación arroja resultados de `FAILED` en los siguientes casos:
>
> - No hay ningún rastro configurado.
> - Las rutas disponibles que se encuentran en la Región actual y que son propiedad de una cuenta corriente no cumplen con los requisitos de control.
>
> La comprobación da como resultado un estado de control de `NO_DATA` en los siguientes casos:

- Una ruta multirregional se basa en una Región diferente. Security Hub CSPM solo puede generar hallazgos en la región en la que se encuentra la ruta.
- Una ruta multirregional pertenece a una cuenta diferente. El CSPM de Security Hub solo puede generar hallazgos para la cuenta propietaria de la ruta.

  Como práctica recomendada, utilice los registros de la organización para registrar los eventos de muchas cuentas de una organización. Los registros organizacionales son registros multirregionales de forma predeterminada y solo los puede administrar la cuenta AWS Organizations de administración o la cuenta de administrador CloudTrail delegado. El uso de un registro de la organización da como resultado un estado de control de `NO_DATA` de los controles evaluados en las cuentas de los miembros de la organización. En las cuentas de los miembros, Security Hub CSPM solo genera hallazgos para los recursos que pertenecen a los miembros. Los resultados relacionados con los registros de la organización se generan en la cuenta del propietario del recurso. Puede ver estos resultados en su cuenta de administrador delegado de CSPM de Security Hub mediante la agregación entre regiones.

Para la alarma, la cuenta corriente debe ser propietaria del tema de Amazon SNS al que se hace referencia o debe obtener acceso al tema de Amazon SNS llamando a `ListSubscriptionsByTopic`. De lo contrario, Security Hub CSPM `WARNING` generará resultados para el control.

Corrección

Para pasar este control, siga estos pasos para crear un tema de Amazon SNS, una ruta de AWS CloudTrail , un filtro de métricas y una alarma para el filtro de métricas.

1. Crear un tema de Amazon SNS Para obtener instrucciones, consulte Introducción a Amazon SNS en la Guía para desarrolladores de Amazon Simple Notification Service. Cree un tema que reciba todas las alarmas del CIS y cree al menos una suscripción al tema.
2. Cree una CloudTrail ruta que se aplique a todos. Regiones de AWS Para obtener instrucciones, consulte Crear un registro de seguimiento en la Guía del usuario de AWS CloudTrail .

   Anote el nombre del grupo de CloudWatch registros que asocie a la CloudTrail ruta. En el siguiente paso, debe crear el filtro de métricas para ese grupo de registros.

3. Crear un filtro de métricas. Para obtener instrucciones, consulte Crear un filtro métrico para un grupo de registros en la Guía del CloudWatch usuario de Amazon. Use los siguientes valores:

Campo	Valor
Defina el patrón, el patrón de filtro	`{($.eventName=CreateCustomerGateway) \|\| ($.eventName=DeleteCustomerGateway) || ($.eventName=AttachInternetGateway) \|\| ($.eventName=CreateInternetGateway) || ($.eventName=DeleteInternetGateway) \|\| ($.eventName=DetachInternetGateway)}`
Espacio de nombres de métrica	**`LogMetrics`**
Valor de la métrica	**`1`**
Predeterminado	**`0`**

4. Crear una alarma basada en el filtro. Para obtener instrucciones, consulte Crear una CloudWatch alarma basada en un filtro métrico de grupos de registros en la Guía del CloudWatch usuario de Amazon. Use los siguientes valores:

Campo	Valor
Condiciones, tipo de umbral	Estático
Siempre que sea... *`your-metric-name`*	Greater/Equal
que…	**`1`**

[CloudWatch.13] Asegúrese de que haya un registro, un filtro métrico y una alarma para los cambios en la tabla de rutas

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2. 0/31.3, CIS AWS Foundations Benchmark v1.4. 0/41.3, NIST.800-171.r2 3.3.1, 3.13.1, 3.14.6, NIST.800-171.r2 3.14.7 NIST.800-171.r2 NIST.800-171.r2

Categoría: Detectar - Servicios de detección

Gravedad: baja

Tipo de recurso: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config regla: Ninguna (regla CSPM personalizada de Security Hub)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si se supervisan las llamadas a la API en tiempo real. Para ello, redirige CloudTrail los CloudWatch registros a Logs y establece las alarmas y los filtros métricos correspondientes. Las tablas de enrutamiento dirigen el tráfico de red entre subredes y a gateways de red.

CIS recomienda que cree un filtro de métricas y alarma para los cambios realizados a las tablas de enrutamiento. La monitorización de estos cambios ayuda a garantizar que todo el tráfico de la VPC vaya a través de una ruta esperada.

> **Note**
>
> Cuando Security Hub CSPM comprueba este control, busca los CloudTrail rastros que utiliza la cuenta actual. Estas rutas pueden ser rutas de organizaciones que pertenecen a otra cuenta. Multi-Region Las rutas también pueden estar ubicadas en una región diferente. La comprobación arroja resultados de `FAILED` en los siguientes casos:
>
> - No hay ningún rastro configurado.
> - Las rutas disponibles que se encuentran en la Región actual y que son propiedad de una cuenta corriente no cumplen con los requisitos de control.
>
> La comprobación da como resultado un estado de control de `NO_DATA` en los siguientes casos:
>
> - Una ruta multirregional se basa en una Región diferente. Security Hub CSPM solo puede generar hallazgos en la región en la que se encuentra la ruta.
> - Una ruta multirregional pertenece a una cuenta diferente. El CSPM de Security Hub solo puede generar hallazgos para la cuenta propietaria de la ruta.

Como práctica recomendada, utilice los registros de la organización para registrar los eventos de muchas cuentas de una organización. Los registros organizacionales son registros multirregionales de forma predeterminada y solo los puede administrar la cuenta AWS Organizations de administración o la cuenta de administrador CloudTrail delegado. El uso de un registro de la organización da como resultado un estado de control de `NO_DATA` de los controles evaluados en las cuentas de los miembros de la organización. En las cuentas de los miembros, Security Hub CSPM solo genera hallazgos para los recursos que pertenecen a los miembros. Los resultados relacionados con los registros de la organización se generan en la cuenta del propietario del recurso. Puede ver estos resultados en su cuenta de administrador delegado de CSPM de Security Hub mediante la agregación entre regiones.

Para la alarma, la cuenta corriente debe ser propietaria del tema de Amazon SNS al que se hace referencia o debe obtener acceso al tema de Amazon SNS llamando a `ListSubscriptionsByTopic`. De lo contrario, Security Hub CSPM `WARNING` generará resultados para el control.

Corrección

> **Note**
>
> El patrón de filtro que recomendamos en estos pasos de corrección difiere del patrón de filtro de la guía del CIS. Nuestros filtros recomendados se centran únicamente en eventos procedentes de llamadas a la API de Amazon Elastic Compute Cloud (EC2).

Para pasar este control, siga estos pasos para crear un tema de Amazon SNS, una ruta de AWS CloudTrail , un filtro de métricas y una alarma para el filtro de métricas.

1. Crear un tema de Amazon SNS Para obtener instrucciones, consulte Introducción a Amazon SNS en la Guía para desarrolladores de Amazon Simple Notification Service. Cree un tema que reciba todas las alarmas del CIS y cree al menos una suscripción al tema.
2. Cree una CloudTrail ruta que se aplique a todos. Regiones de AWS Para obtener instrucciones, consulte Crear un registro de seguimiento en la Guía del usuario de AWS CloudTrail .

Anote el nombre del grupo de CloudWatch registros que asocie a la CloudTrail ruta. En el siguiente paso, debe crear el filtro de métricas para ese grupo de registros.

3. Crear un filtro de métricas. Para obtener instrucciones, consulte Crear un filtro métrico para un grupo de registros en la Guía del CloudWatch usuario de Amazon. Use los siguientes valores:

Campo	Valor
Defina el patrón, el patrón de filtro	`{($.eventSource=ec2.amazonaws.com) && (($.eventName=CreateRoute) || ($.eventName=CreateRouteTable) \|\| ($.eventName=ReplaceRoute) || ($.eventName=ReplaceRouteTableAssociation) \|\| ($.eventName=DeleteRouteTable) || ($.eventName=DeleteRoute) \|\| ($.eventName=DisassociateRouteTable))}`
Espacio de nombres de métrica	**`LogMetrics`**
Valor de la métrica	**`1`**
Predeterminado	**`0`**

4. Crear una alarma basada en el filtro. Para obtener instrucciones, consulte Crear una CloudWatch alarma basada en un filtro métrico de grupos de registros en la Guía del CloudWatch usuario de Amazon. Use los siguientes valores:

Campo	Valor
Condiciones, tipo de umbral	Estático
Siempre que sea... *`your-metric-name`*	Greater/Equal
que…	**`1`**

[CloudWatch.14] Asegúrese de que haya un registro, un filtro métrico y una alarma para los cambios en la VPC

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2. 0/31.4, CIS AWS Foundations Benchmark v1.4. 0/41.4, NIST.800-171.r2 3.3.1, 3.13.1, 3.14.6, NIST.800-171.r2 3.14.7 NIST.800-171.r2 NIST.800-171.r2

Categoría: Detectar - Servicios de detección

Gravedad: baja

Tipo de recurso: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config regla: Ninguna (regla CSPM personalizada de Security Hub)

Tipo de programa: Periódico

Parámetros: ninguno

Para supervisar las llamadas a la API en tiempo real, dirija CloudTrail los CloudWatch registros a Logs y establezca las alarmas y los filtros métricos correspondientes. Puede tener más de un VPC en una cuenta, y puede crear una interconexión entre dos VPC, lo que permite dirigir el tráfico de red entre VPC.

CIS recomienda que cree un filtro de métricas y alarma para los cambios realizados a las VPC. La monitorización de estos cambios ayuda a garantizar que los controles de autenticación y autorización permanezcan intactos.

Para ejecutar esta comprobación, el CSPM de Security Hub utiliza una lógica personalizada para realizar los pasos de auditoría exactos prescritos para el control 4.14 en la versión 1.4.0 de CIS AWS Foundations Benchmark. Este control produce un error si no se utilizan los filtros de métricas exactos prescritos por CIS. No se pueden añadir campos ni términos adicionales a los filtros de métricas.

> **Note**
>
> Cuando Security Hub CSPM comprueba este control, busca los rastros que utiliza la cuenta actual. CloudTrail Estas rutas pueden ser rutas de organizaciones que pertenecen a otra cuenta. Multi-Region Las rutas también pueden estar ubicadas en una región diferente.

La comprobación arroja resultados de `FAILED` en los siguientes casos:

- No hay ningún rastro configurado.
- Las rutas disponibles que se encuentran en la Región actual y que son propiedad de una cuenta corriente no cumplen con los requisitos de control.

La comprobación da como resultado un estado de control de `NO_DATA` en los siguientes casos:

- Una ruta multirregional se basa en una Región diferente. Security Hub CSPM solo puede generar hallazgos en la región en la que se encuentra la ruta.
- Una ruta multirregional pertenece a una cuenta diferente. El CSPM de Security Hub solo puede generar hallazgos para la cuenta propietaria de la ruta.

  Como práctica recomendada, utilice los registros de la organización para registrar los eventos de muchas cuentas de una organización. Los registros organizacionales son registros multirregionales de forma predeterminada y solo los puede administrar la cuenta AWS Organizations de administración o la cuenta de administrador CloudTrail delegado. El uso de un registro de la organización da como resultado un estado de control de `NO_DATA` de los controles evaluados en las cuentas de los miembros de la organización. En las cuentas de los miembros, Security Hub CSPM solo genera hallazgos para los recursos que pertenecen a los miembros. Los resultados relacionados con los registros de la organización se generan en la cuenta del propietario del recurso. Puede ver estos resultados en su cuenta de administrador delegado de CSPM de Security Hub mediante la agregación entre regiones.

Para la alarma, la cuenta corriente debe ser propietaria del tema de Amazon SNS al que se hace referencia o debe obtener acceso al tema de Amazon SNS llamando a `ListSubscriptionsByTopic`. De lo contrario, Security Hub CSPM `WARNING` generará resultados para el control.

Corrección

Para pasar este control, siga estos pasos para crear un tema de Amazon SNS, una ruta de AWS CloudTrail , un filtro de métricas y una alarma para el filtro de métricas.

1. Crear un tema de Amazon SNS Para obtener instrucciones, consulte Introducción a Amazon SNS en la Guía para desarrolladores de Amazon Simple Notification Service. Cree un tema que reciba todas las alarmas del CIS y cree al menos una suscripción al tema.
2. Cree una CloudTrail ruta que se aplique a todos. Regiones de AWS Para obtener instrucciones, consulte Crear un registro de seguimiento en la Guía del usuario de AWS CloudTrail .

   Anote el nombre del grupo de CloudWatch registros que asocie a la CloudTrail ruta. En el siguiente paso, debe crear el filtro de métricas para ese grupo de registros.
3. Crear un filtro de métricas. Para obtener instrucciones, consulte Crear un filtro métrico para un grupo de registros en la Guía del CloudWatch usuario de Amazon. Use los siguientes valores:

Campo	Valor
Defina el patrón, el patrón de filtro	`{($.eventName=CreateVpc) \|\| ($.eventName=DeleteVpc) || ($.eventName=ModifyVpcAttribute) \|\| ($.eventName=AcceptVpcPeeringConnection) || ($.eventName=CreateVpcPeeringConnection) \|\| ($.eventName=DeleteVpcPeeringConnection) || ($.eventName=RejectVpcPeeringConnection) \|\| ($.eventName=AttachClassicLinkVpc) || ($.eventName=DetachClassicLinkVpc) \|\| ($.eventName=DisableVpcClassicLink) || ($.eventName=EnableVpcClassicLink)}`
Espacio de nombres de métrica	**`LogMetrics`**
Valor de la métrica	**`1`**
Predeterminado	**`0`**

4. Crear una alarma basada en el filtro. Para obtener instrucciones, consulte Crear una CloudWatch alarma basada en un filtro métrico de grupos de registros en la Guía del CloudWatch usuario de Amazon. Use los siguientes valores:

Campo	Valor
Condiciones, tipo de umbral	Estático
Siempre que sea... *your-metric-name*	Greater/Equal
que…	**1**

[CloudWatch.15] CloudWatch las alarmas deben tener configuradas acciones específicas

Requisitos relacionados: NIST.800-53.r5 AU-6 (1), NIST.800-53.r5 AU-6 (5) NIST.800-53.r5 CA-7, NIST.800-53.r5 IR-4 (1), NIST.800-53.r5 IR-4 (5),, NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-4 (12) NIST.800-53.r5 SI-20, NIST.800-53.r5 SI-4 (5), NIST.800-171.r2 3.3.4, NIST.800-171.r2 3.14.6

Categoría: Detectar - Servicios de detección

Gravedad: alta

Tipo de recurso: `AWS::CloudWatch::Alarm`

AWS Config regla: `cloudwatch-alarm-action-check`

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub CSPM
`alarmActionRequired`	El control genera un resultado `PASSED` si el parámetro está establecido en `true` y	Booleano	No personalizable	`true`

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub CSPM
	la alarma tiene una acción cuando el estado de la alarma cambia a `ALARM`.			
`insufficientDataActionRequired`	El control genera un resultado `PASSED` si el parámetro está establecido en `true` y la alarma tiene una acción cuando el estado de la alarma cambia a `INSUFFICIENT_DATA` .	Booleano	`true` o `false`	`false`
`okActionRequired`	El control genera un resultado `PASSED` si el parámetro está establecido en `true` y la alarma tiene una acción cuando el estado de la alarma cambia a `OK`.	Booleano	`true` o `false`	`false`

Este control comprueba si una CloudWatch alarma de Amazon tiene al menos una acción configurada para ese estado. `ALARM` Se produce un error en el control si la alarma no tiene ninguna acción configurada para el estado `ALARM`. De manera opcional, puede incluir valores personalizados de parámetros para requerir también acciones de alarma para los estados `INSUFFICIENT_DATA` o `OK`.

> **Note**
>
> El CSPM de Security Hub evalúa este control en CloudWatch función de las alarmas métricas. Las alarmas de métricas pueden formar parte de alarmas compuestas que tienen configuradas las acciones especificadas. El control arroja resultados `FAILED` en los siguientes casos:

- Las acciones especificadas no están configuradas para una alarma de métrica.
- La alarma de métrica forma parte de una alarma compuesta que tiene configuradas las acciones especificadas.

Este control se centra en si una CloudWatch alarma tiene una acción de alarma configurada, mientras que CloudWatch.17 se centra en el estado de activación de una CloudWatch acción de alarma.

Recomendamos que las acciones de CloudWatch alarma le avisen automáticamente cuando una métrica supervisada supere el umbral definido. Las alarmas de supervisión ayudan a identificar actividades inusuales y a responder rápidamente a los problemas operativos y de seguridad cuando una alarma pasa a un estado específico. El tipo más común de acción de alarma es notificar a uno o más usuarios mediante el envío de un mensaje a un tema de Amazon Simple Notification Service (Amazon SNS).

Corrección

Para obtener información sobre las acciones que admiten las CloudWatch alarmas, consulte las acciones de alarma en la Guía del CloudWatch usuario de Amazon.

[CloudWatch.16] los grupos de CloudWatch registros deben conservarse durante un período de tiempo específico

Categoría: Identificar - Registro

Requisitos relacionados: NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-11, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4) NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-12

Gravedad: media

Tipo de recurso: `AWS::Logs::LogGroup`

AWS Config regla: `cw-loggroup-retention-period-check`

Tipo de programa: Periódico

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub CSPM	
`minRetentionTime`	Período mínimo de retención en días para los grupos de registros CloudWatch	Enum	`365`, `400`, `545`, `731`, `1827`, `3653`	`365`	

Este control comprueba si un grupo de CloudWatch registros de Amazon tiene un período de retención de al menos el número de días especificado. Se produce un error en el control si el periodo de retención es inferior a la cantidad especificada. A menos que proporciones un valor de parámetro personalizado para el período de retención, Security Hub CSPM utiliza un valor predeterminado de 365 días.

CloudWatch Los registros centralizan los registros de todos sus sistemas y aplicaciones Servicios de AWS en un único servicio altamente escalable. Puede usar CloudWatch los registros para supervisar, almacenar y acceder a sus archivos de registro desde las instancias de Amazon Elastic Compute Cloud (EC2) AWS CloudTrail, Amazon Route 53 y otras fuentes. Conservar los registros durante al menos un año puede ayudarle a cumplir con los estándares de retención de registros.

Corrección

Para configurar los ajustes de retención de registros, consulte Cambiar la retención de datos de registro en CloudWatch Logs en la Guía del CloudWatch usuario de Amazon.

[CloudWatch.17] las acciones CloudWatch de alarma deben estar activadas

Categoría: Detectar - Servicios de detección

Requisitos relacionados: NIST.800-53.r5 AU-6 (1), NIST.800-53.r5 AU-6 (5), NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-4 (12)

Gravedad: alta

Tipo de recurso: `AWS::CloudWatch::Alarm`

AWS Config regla: `cloudwatch-alarm-action-enabled-check`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si las acciones de CloudWatch alarma están activadas (`ActionEnabled`deben establecerse como verdaderas). El control falla si la acción de alarma de una CloudWatch alarma está desactivada.

> **Note**
>
> Security Hub CSPM evalúa este control en CloudWatch función de las alarmas métricas. Las alarmas de métricas pueden formar parte de alarmas compuestas que tienen activadas las acciones de alarma. El control arroja resultados `FAILED` en los siguientes casos:
>
> - Las acciones especificadas no están configuradas para una alarma de métrica.
> - La alarma de métrica forma parte de una alarma compuesta que tiene activadas las acciones de alarma.

Este control se centra en el estado de activación de una acción de CloudWatch alarma, mientras que CloudWatch.15 se centra en si alguna `ALARM` acción está configurada en una alarma. CloudWatch

Las acciones de alarma le avisan automáticamente cuando una métrica monitorizada está fuera del umbral definido. Si la acción de alarma está desactivada, no se ejecuta ninguna acción cuando la alarma cambia de estado y no se le avisará de los cambios en las métricas monitorizadas. Recomendamos activar las acciones de CloudWatch alarma para ayudarle a responder rápidamente a los problemas operativos y de seguridad.

Corrección

Para activar una acción CloudWatch de alarma (consola)

1. Abra la CloudWatch consola en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, elija Alarmas y, luego, Todas las alarmas.
3. Seleccione la alarma para la que desea activar las acciones.

4. En Acciones, selecciona Acciones de alarma (nuevas) y, a continuación, selecciona Habilitar.

Para obtener más información sobre la activación de las acciones de CloudWatch alarma, consulte las acciones de alarma en la Guía del CloudWatch usuario de Amazon.

Controles CSPM de Security Hub para CodeArtifact

Estos controles CSPM de Security Hub evalúan el AWS CodeArtifact servicio y los recursos.

Es posible que estos controles no estén disponibles en todos. Regiones de AWS Para obtener más información, consulte Disponibilidad de los controles por región.

[CodeArtifact.1] CodeArtifact los repositorios deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::CodeArtifact::Repository`

AWS Configregla: `tagged-codeartifact-repository` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si un AWS CodeArtifact repositorio tiene etiquetas con las claves específicas definidas en el parámetro`requiredTagKeys`. El control lanza error si el repositorio no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si el repositorio no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, incluidasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte Etiquetar sus AWS recursos en el. Referencia general de AWS

Corrección

Para añadir etiquetas a un CodeArtifact repositorio, consulte Etiquetar un repositorio CodeArtifact en la Guía del AWS CodeArtifactusuario.

Controles CSPM de Security Hub para CodeBuild

Estos controles CSPM de Security Hub evalúan el AWS CodeBuild servicio y los recursos.

Es posible que estos controles no estén disponibles en todos. Regiones de AWS Para obtener más información, consulte Disponibilidad de los controles por región.

[CodeBuild.1] Las URL del repositorio fuente de CodeBuild Bitbucket no deben contener credenciales confidenciales

Requisitos relacionados: PCI NIST.800-53.r5 SA-3 DSS v3.2. 1/82.2.1, PCI DSS v4.0. 1/8.3.2

Categoría: Proteger - Desarrollo seguro

Gravedad: crítica

Tipo de recurso: `AWS::CodeBuild::Project`

Regla de AWS Config: `codebuild-project-source-repo-url-check`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si la URL del repositorio fuente de Bitbucket de un AWS CodeBuild proyecto contiene tokens de acceso personales o un nombre de usuario y una contraseña. El control falla si la URL del repositorio de origen de Bitbucket contiene tókenes de acceso personal o un nombre de usuario y una contraseña.

> **Note**
>
> Este control evalúa tanto la fuente principal como las fuentes secundarias de un proyecto de CodeBuild compilación. Para obtener más información acerca de los orígenes del proyecto, consulte Multiple input sources and output artifacts sample en la Guía del usuario de AWS CodeBuild.

Sign-in las credenciales no deben almacenarse ni transmitirse en texto sin cifrar ni aparecer en la URL del repositorio de origen. En lugar de utilizar fichas de acceso personales o credenciales de inicio de sesión, debes acceder a tu proveedor de origen y cambiar la URL del repositorio de origen para que contenga solo la ruta a la ubicación del repositorio de Bitbucket. CodeBuild El uso de tókenes de acceso personal o de credenciales de inicio de sesión podría dar lugar a la exposición involuntaria de datos o al acceso no autorizado.

Corrección

Puedes actualizar tu CodeBuild proyecto para usar OAuth.

Para eliminar el token de autenticación básica/(GitHub) de acceso personal de la fuente del proyecto CodeBuild

1. Abra la CodeBuild consola en https://console.aws.amazon.com/codebuild/.
2. Elija el proyecto de compilación que contiene tokens de acceso personales o un nombre de usuario y una contraseña.
3. En Edit (Editar), elija Source (Origen).
4. Selecciona Desconectar de GitHub /Bitbucket.
5. Elige Conectar mediante OAuth y, a continuación, selecciona Conectar a GitHub /Bitbucket.
6. Cuando se le solicite, elija authorize as appropriate (autorizar según corresponda).
7. Vuelva a configurar la URL de repositorio y los ajustes de la configuración adicional, según sea necesario.
8. Elija Update source (Actualizar origen).

Para obtener más información, consulta los ejemplos basados en casos de CodeBuild uso en la Guía del usuario. AWS CodeBuild

[CodeBuild.2] las variables de entorno CodeBuild del proyecto no deben contener credenciales de texto claro

Requisitos relacionados: NIST.800-53.r5 IA-5 (7) NIST.800-53.r5 SA-3, PCI DSS v3.2. 1/82.2.1, PCI DSS v4.0. 1/8.3.2

Categoría: Proteger - Desarrollo seguro

Gravedad: crítica

Tipo de recurso: `AWS::CodeBuild::Project`

Regla de AWS Config: `codebuild-project-envvar-awscred-check`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si el proyecto contiene las variables de entorno `AWS_ACCESS_KEY_ID` y `AWS_SECRET_ACCESS_KEY`.

Las credenciales de autenticación `AWS_ACCESS_KEY_ID` y `AWS_SECRET_ACCESS_KEY` no deben almacenarse nunca en texto sin cifrar, ya que esto podría conducir a una exposición no intencionada de los datos y a un acceso no autorizado.

Corrección

Para eliminar las variables de entorno de un CodeBuild proyecto, consulte Cambiar la configuración de un proyecto de compilación AWS CodeBuild en la Guía del AWS CodeBuild usuario. Asegúrese de que no haya nada seleccionado para las Variables de entorno.

Puede almacenar variables de entorno con valores sensibles en el almacén de AWS Systems Manager parámetros oAWS Secrets Manager, a continuación, recuperarlas de las especificaciones de compilación. Para obtener instrucciones, consulte el cuadro denominado Importante en la sección Medio ambiente de la Guía del usuario de AWS CodeBuild.

[CodeBuild.3] Los registros de CodeBuild S3 deben estar cifrados

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28 (1) NIST.800-53.r5 SC-28, NIST.800-53.r5 SI-7 (6), PCI DSS v4.0. 1/103.3.2

Categoría: Proteger > Protección de datos > Cifrado de datos en reposo

Gravedad: baja

Tipo de recurso: `AWS::CodeBuild::Project`

Regla de AWS Config: `codebuild-project-s3-logs-encrypted`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si los registros de Amazon S3 de un AWS CodeBuild proyecto están cifrados. El control falla si se desactiva el cifrado de los registros de S3 de un CodeBuild proyecto.

El cifrado de los datos en reposo es una práctica recomendada para añadir una capa de gestión del acceso a los datos. El cifrado de los registros inactivos reduce el riesgo de que un usuario no autenticado acceda AWS a los datos almacenados en el disco. Añade otro conjunto de controles de acceso para limitar la capacidad de los usuarios no autorizados de acceder a los datos.

Corrección

Para cambiar la configuración de cifrado de los registros CodeBuild del proyecto S3, consulte Cambiar la configuración de un proyecto de compilación AWS CodeBuild en la Guía del AWS CodeBuildusuario.

[CodeBuild.4] los entornos de CodeBuild proyectos deben tener un registroAWS ConfigDuración

Requisitos relacionados: NIST.800-53.r5 AC-2 (12), NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 AU-9 (7) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-3 (8) NIST.800-53.r5 SI-4, NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8)

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: `AWS::CodeBuild::Project`

Regla de AWS Config: `codebuild-project-logging-enabled`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si el entorno de un CodeBuild proyecto tiene al menos una opción de registro, ya sea para S3 o para CloudWatch registros habilitados. Este control falla si un entorno de CodeBuild proyecto no tiene habilitada al menos una opción de registro.

Desde una perspectiva de seguridad, el registro es una característica importante para permitir futuros esfuerzos forenses en caso de cualquier incidente de seguridad. La correlación de las anomalías en los CodeBuild proyectos con las detecciones de amenazas puede aumentar la confianza en la precisión de esas detecciones de amenazas.

Corrección

Para obtener más información sobre cómo configurar los ajustes CodeBuild del registro del proyecto, consulte Crear un proyecto de compilación (consola) en la Guía del usuario. CodeBuild

[CodeBuild.5] los entornos de CodeBuild proyectos no deberían tener habilitado el modo privilegiado

> **Important**
>
> Security Hub CSPM retiró este control en abril de 2024. Para obtener más información, consulte Registro de cambios de los controles del CSPM de Security Hub.

Requisitos relacionados: NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-5, NIST.800-53.r5 AC-6 (10) NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6 (2)

Categoría: Proteger > Administración de acceso seguro

Gravedad: alta

Tipo de recurso: `AWS::CodeBuild::Project`

Regla de AWS Config: `codebuild-project-environment-privileged-check`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si el entorno de un AWS CodeBuild proyecto tiene el modo privilegiado activado o desactivado. El control falla si el entorno de un CodeBuild proyecto tiene habilitado el modo privilegiado.

De forma predeterminada, los contenedores Docker no permiten el acceso a ningún dispositivo. El modo privilegiado otorga acceso al contenedor Docker de un proyecto de compilación a todos los dispositivos. La configuración `privilegedMode` con un valor `true` permite que el daemon de Docker se ejecute dentro de un contenedor de Docker. El daemon de Docker escucha las solicitudes de la API de Docker y administra los objetos de Docker, como imágenes, contenedores, redes y volúmenes. Este parámetro solo debe establecerse en true si el proyecto de compilación se utiliza para compilar imágenes de Docker. De lo contrario, esta configuración debe estar deshabilitada para evitar el acceso no deseado a las API de Docker y al hardware subyacente del contenedor. Esta configuración de `privilegedMode` como `false` a proteger los recursos críticos contra la manipulación y la eliminación.

Corrección

Para configurar los ajustes CodeBuild del entorno del proyecto, consulte Crear un proyecto de compilación (consola) en la Guía del CodeBuild usuario. En la sección Entorno, no seleccione la configuración Privilegiada.

[CodeBuild.7] las exportaciones de grupos de CodeBuild informes deben cifrarse en reposo

Categoría: Proteger > Protección de datos > Cifrado de datos en reposo

Gravedad: media

Tipo de recurso: `AWS::CodeBuild::ReportGroup`

Regla de AWS Config: `codebuild-report-group-encrypted-at-rest`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si los resultados de las pruebas de un grupo de AWS CodeBuild informes que se exportan a un bucket de Amazon Simple Storage Service (Amazon S3) están cifrados en reposo. El control falla si la exportación del grupo de informes no está cifrada en reposo.

Los datos en reposo hacen referencia a los datos que se almacenan en un almacenamiento persistente y no volátil durante cualquier periodo de tiempo. El cifrado de datos en reposo permite proteger la confidencialidad de los datos, lo que reduce el riesgo de que un usuario no autorizado pueda acceder a ellos.

Corrección

Para cifrar la exportación del grupo de informes a S3, consulte Update a report group en la Guía del usuario de AWS CodeBuild.

Controles CSPM de Security Hub para Amazon Profiler CodeGuru

Estos controles CSPM de Security Hub evalúan el servicio y los recursos de Amazon CodeGuru Profiler.

Es posible que estos controles no estén disponibles en todos. Regiones de AWS Para obtener más información, consulte Disponibilidad de los controles por región.

[CodeGuruProfiler.1] Los grupos CodeGuru de creación de perfiles de Profiler deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::CodeGuruProfiler::ProfilingGroup`

Regla de AWS Config: `codeguruprofiler-profiling-group-tagged`

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredKeyTags`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si un grupo de CodeGuru perfiles de Amazon Profiler tiene etiquetas con las claves específicas definidas en el parámetro. `requiredKeyTags` El control falla si el grupo de generación de perfiles no tiene ninguna clave de etiqueta, o si no tiene todas las claves especificadas en el parámetro `requiredKeyTags`. Si no se proporcionan valores para el parámetro `requiredKeyTags`, el control solo comprueba la existencia de una clave de etiqueta y falla si el grupo de generación de perfiles no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno

u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte Definición de permisos basados en atributos con autorización ABAC en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte las mejores prácticas y estrategias en los AWSrecursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para añadir etiquetas a un grupo de creación de CodeGuru perfiles, consulte Etiquetado de grupos de creación de perfiles en la Guía del usuario de Amazon CodeGuru Profiler.

Controles de CSPM de Security Hub para Amazon Reviewer CodeGuru

Estos controles CSPM de Security Hub evalúan el servicio y los recursos de Amazon CodeGuru Reviewer.

Es posible que estos controles no estén disponibles en todos. Regiones de AWS Para obtener más información, consulte Disponibilidad de los controles por región.

[CodeGuruReviewer.1] Las asociaciones de repositorios de CodeGuru Reviewer deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::CodeGuruReviewer::RepositoryAssociation`

Regla de AWS Config: `codegururevieweer-repository-association-tagged`

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredKeyTags`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si una asociación de repositorios de Amazon CodeGuru Reviewer tiene etiquetas con las claves específicas definidas en el parámetro`requiredKeyTags`. El control falla si la asociación de repositorio no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredKeyTags`. Si no proporciona valores para el parámetro `requiredKeyTags`, el control solo verifica la existencia de una clave de etiqueta y falla si la asociación de repositorio no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para

sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte Definición de permisos basados en atributos con autorización ABAC en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte las mejores prácticas y estrategias en los AWSrecursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para añadir etiquetas a una asociación de repositorios de CodeGuru Reviewer, consulte Etiquetar una asociación de repositorios en la Guía del usuario de Amazon CodeGuru Reviewer.

Controles de CSPM de Security Hub para Amazon Cognito

Estos AWS Security Hub CSPM controles evalúan el servicio y los recursos de Amazon Cognito. Es posible que los controles no estén disponibles en todos los Regiones de AWS casos. Para obtener más información, consulte Disponibilidad de los controles por región.

[Cognito.1] Los grupos de usuarios de Cognito deben tener activada la protección contra amenazas y el modo de aplicación con todas las funciones para la autenticación estándar

Categoría: Proteger - Administración de acceso seguro

Gravedad: media

Tipo de recurso: `AWS::Cognito::UserPool`

Regla de AWS Config : cognito-user-pool-advanced-security-enabled

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub CSPM
`SecurityMode`	El modo de aplicación obligatoria de la protección contra amenazas que el control revisa.	Cadena	`AUDIT`, `ENFORCED`	`ENFORCED`

Este control verifica si un grupo de usuarios de Amazon Cognito tiene la protección contra amenazas activada con el modo de aplicación obligatoria configurado en función completa para la autenticación estándar. El control falla si el grupo de usuarios tiene la protección contra amenazas desactivada o si el modo de aplicación obligatoria no está configurado en función completa para la autenticación estándar. A menos que proporcione valores de parámetros personalizados, el CSPM de Security Hub utiliza el valor predeterminado de `ENFORCED` para el modo de cumplimiento establecido en función completa para la autenticación estándar.

Después de crear un grupo de usuarios de Amazon Cognito, puede activar la protección contra amenazas y personalizar las acciones que se realizan en respuesta a distintos riesgos. O puede usar el modo de auditoría para recopilar métricas sobre riesgos detectados sin aplicar ninguna mitigación de seguridad. En el modo auditoría, la protección contra amenazas publica las métricas en Amazon. CloudWatch Puede ver las métricas después de que Amazon Cognito genere su primer evento.

Corrección

Para obtener información sobre cómo activar la protección contra amenazas para un grupo de usuarios de Amazon Cognito, consulte Seguridad avanzada con protección contra amenazas en la Guía del desarrollador de Amazon Cognito.

[Cognito.2] Los grupos de identidades de Cognito no deben permitir identidades no autenticadas

Categoría: Proteger > Gestión del acceso seguro > Autenticación sin contraseña

Gravedad: media

Tipo de recurso: `AWS::Cognito::IdentityPool`

Regla de AWS Config : cognito-identity-pool-unauth-access-check

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control verifica si un grupo de identidades de Amazon Cognito está configurado para permitir identidades no autenticadas. El control falla si el acceso de invitado está activado (el parámetro `AllowUnauthenticatedIdentities` está configurado en `true`) para el grupo de identidades.

Si un grupo de identidades de Amazon Cognito permite identidades no autenticadas, el grupo de identidades proporciona AWS credenciales temporales a los usuarios que no se han autenticado a través de un proveedor de identidades (invitados). Esto crea riesgos de seguridad porque permite el acceso anónimo a los recursos. AWS Si desactivas el acceso como invitado, puedes garantizar que solo los usuarios debidamente autenticados puedan acceder a tus AWS recursos, lo que reduce el riesgo de acceso no autorizado y de posibles infracciones de seguridad. Como práctica recomendada, un grupo de identidades debe requerir autenticación a través de proveedores de identidades compatibles. Si el acceso no autenticado es necesario, es importante restringir cuidadosamente los permisos para las identidades no autenticadas y revisar y supervisar regularmente su uso.

Corrección

Para obtener información sobre cómo desactivar el acceso de invitado para un grupo de identidades de Amazon Cognito, consulte Activación o desactivación del acceso de invitado en la Guía del desarrollador de Amazon Cognito.

[Cognito.3] Las políticas de contraseñas para los grupos de usuarios de Cognito deben tener configuraciones sólidas

Categoría: Proteger - Administración de acceso seguro

Gravedad: media

Tipo de recurso: `AWS::Cognito::UserPool`

Regla de AWS Config : cognito-user-pool-password-policy-check

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub CSPM
`minLength`	El número mínimo de caracteres que debe contener una contraseña.	Entero	De 8 a 99	8
`requireLowercase`	Requerir al menos un carácter en minúscula en una contraseña.	Booleano	`True`, `False`	`True`
`requireUppercase`	Requerir al menos un carácter en mayúscula en una contraseña.	Booleano	`True`, `False`	`True`
`requireNumbers`	Requerir al menos un número en una contraseña.	Booleano	`True`, `False`	`True`
`requireSymbols`	Requerir al menos un símbolo en una contraseña.	Booleano	`True`, `False`	`True`
`temporaryPasswordValidity`	El número máximo de días que una contraseña puede existir antes de que expire.	Entero	De 1 a 365	7

Este control verifica si la política de contraseñas de un grupo de usuarios de Amazon Cognito requiere el uso de contraseñas sólidas, basadas en configuraciones recomendadas para políticas de contraseñas. El control falla si la política de contraseñas del grupo de usuarios no exige contraseñas sólidas. Puede especificar opcionalmente valores personalizados para los ajustes de la política que el control verifica.

Las contraseñas sólidas son una práctica recomendada de seguridad para los grupos de usuarios de Amazon Cognito. Las contraseñas débiles pueden exponer las credenciales de los usuarios a sistemas que adivinan contraseñas y tratan de acceder a datos. Este es especialmente el caso de

aplicaciones que están abiertas a Internet. Las políticas de contraseñas son un elemento central de la seguridad de los directorios de usuarios. Al usar una política de contraseñas, puede configurar un grupo de usuarios para exigir complejidad de contraseñas y otros ajustes que cumplan con los estándares y requisitos de seguridad.

Corrección

Para obtener información sobre cómo crear o actualizar la política de contraseñas para un grupo de usuarios de Amazon Cognito, consulte Cómo agregar requisitos de contraseña para grupos de usuarios en la Guía del desarrollador de Amazon Cognito.

[Cognito.4] Los grupos de usuarios de Cognito deben tener activada la protección contra amenazas y el modo de aplicación con todas las funciones para la autenticación personalizada

Categoría: Proteger - Administración de acceso seguro

Gravedad: media

Tipo de recurso: `AWS::Cognito::UserPool`

Regla de AWS Config : cognito-userpool-cust-auth-threat-full-check

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un grupo de usuarios de Amazon Cognito tiene activada la protección contra amenazas con el modo de aplicación configurado como plenamente funcional para la autenticación personalizada. El control falla si el grupo de usuarios tiene deshabilitada la protección contra amenazas o si el modo de aplicación no está configurado para funcionar a pleno rendimiento para la autenticación personalizada.

La protección contra amenazas, anteriormente conocida como características avanzadas de seguridad, consiste en un conjunto de herramientas de supervisión de la actividad no deseada en el grupo de usuarios y las herramientas de configuración para detener automáticamente cualquier actividad potencialmente maliciosa. Tras crear un grupo de usuarios de Amazon Cognito, puede activar la protección contra amenazas con el modo de cumplimiento con todas las funciones para personalizar la autenticación y personalizar las acciones que se toman en respuesta a los diferentes riesgos. Full-function el modo incluye un conjunto de reacciones automáticas para detectar actividades no deseadas y contraseñas comprometidas.

Corrección

Para obtener información sobre cómo activar la protección contra amenazas para un grupo de usuarios de Amazon Cognito, consulte Seguridad avanzada con protección contra amenazas en la Guía del desarrollador de Amazon Cognito.

[Cognito.5] La MFA debe estar habilitada para los grupos de usuarios de Cognito

Categoría: Proteger > Gestión de acceso seguro > autenticación Multi-factor

Gravedad: media

Tipo de recurso: `AWS::Cognito::UserPool`

Regla de AWS Config : cognito-user-pool-mfa-enabled

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un grupo de usuarios de Amazon Cognito configurado con una política de inicio de sesión solo con contraseña tiene habilitada la autenticación multifactor (MFA). El control falla si el grupo de usuarios configurado con una política de inicio de sesión solo con contraseña no tiene habilitada la MFA.

Multi-factor La autenticación (MFA) añade un factor de autenticación «algo que tienes» al factor «algo que sabes» (normalmente un nombre de usuario y una contraseña). En el caso de los usuarios federados, Amazon Cognito delega la autenticación en el proveedor de identidad (IdP) y no ofrece factores de autenticación adicionales. Sin embargo, si tiene usuarios locales con autenticación con contraseña, configurar la MFA para el grupo de usuarios aumenta su seguridad.

> **Note**
>
> Este control no se aplica a los usuarios federados ni a los usuarios que inician sesión con factores sin contraseña.

Corrección

Para obtener información sobre cómo configurar la MFA para un grupo de usuarios de Amazon Cognito, consulte Añadir MFA a un grupo de usuarios en la Guía para desarrolladores de Amazon Cognito.

[Cognito.6] Los grupos de usuarios de Cognito deben tener habilitada la protección contra la eliminación

Categoría: Proteger > Protección de datos > Protección contra la eliminación de datos

Gravedad: media

Tipo de recurso: `AWS::Cognito::UserPool`

Regla de AWS Config : cognito-user-pool-deletion-protection-enabled

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un grupo de usuarios de Amazon Cognito tiene habilitada la protección contra la eliminación. El control falla si la protección contra la eliminación está deshabilitada para el grupo de usuarios.

La protección contra la eliminación ayuda a garantizar que su grupo de usuarios no se elimine accidentalmente. Al configurar un grupo de usuarios con protección contra la eliminación, ningún usuario puede eliminar el grupo. La protección contra la eliminación le impide solicitar la eliminación de un grupo de usuarios a menos que primero modifique el grupo y desactive la protección contra la eliminación.

Corrección

Para configurar la protección contra la eliminación de un grupo de usuarios de Amazon Cognito, consulte la sección Protección contra la eliminación de un grupo de usuarios en la Guía para desarrolladores de Amazon Cognito.

Controles CSPM de Security Hub para AWS Config

Estos controles de CSPM de Security Hub evalúan el AWS Config servicio y los recursos.

Es posible que estos controles no estén disponibles en todos los casos. Regiones de AWS Para obtener más información, consulte Disponibilidad de los controles por región.

[Config.1] AWS Config deben estar habilitados y usar la función vinculada al servicio para el registro de recursos

> **Note**
>
> Cuando Security Hub CSPM y Security Hub estén habilitados, la Config.1 regla siempre tendrá el estado de APROBADA. Esto se debe a que el CSPM de Security Hub tiene acceso directo a los elementos de configuración a través de un grabador de configuración vinculado a un servicio. El parámetro de este control no es aplicable, ya que el grabador de configuración vinculado a un servicio interno se crea automáticamente con la función vinculada a un servicio. AWS Config Para obtener más información, consulte Uso del grabador de configuración vinculado a un servicio.
>
> Los controles multinube (como los controles de Azure) y su registro de recursos asociado no se tienen en cuenta en las evaluaciones. Config.1 Los estándares multinube siempre utilizan un grabador de configuración interno vinculado a un servicio que el conector multinube de CSPM configura automáticamente, independientemente del estado de activación de Security Hub. Dado que la grabación multinube está totalmente gestionada por el conector, esto no afecta al estado de cumplimiento. Config.1 Config.1 evalúa solo la configuración de grabación AWS de recursos.

Requisitos relacionados: CIS AWS Foundations Benchmark v5.0. 0/3.3, CIS AWS Foundations Benchmark v1.2. 0/2.5, CIS AWS Foundations Benchmark v1.4. 0/3.5, CIS AWS Foundations Benchmark v3.0. 0/3.3 NIST.800-53.r5 CM-3, NIST.800-53.r5 CM-6 (1), NIST.800-53.r5 CM-8 (2) NIST.800-53.r5 CM-8, PCI DSS v3.2. 1/101.5.2, PCI DSS v3.2. 1/115.

Categoría: Identificar - Inventario

Gravedad: crítica

Tipo de recurso: `AWS::::Account`

AWS Config regla: Ninguna (regla CSPM personalizada de Security Hub)

Tipo de programa: Periódico

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`includeConfigServiceLinkedRoleCheck`	El control no evalúa si AWS Config utiliza la función vinculada al servicio si el parámetro está establecido en. `false`	Booleano	`true` o `false`	`true`

Este control comprueba si AWS Config está habilitado en su cuenta en la actualidad Región de AWS, registra todos los recursos que corresponden a los controles que están habilitados en la región actual y utiliza el rol vinculado al servicio AWS Config . El nombre del rol vinculado al servicio es. AWSServiceRoleForConfig Si no usas el rol vinculado a un servicio y no configuras el `includeConfigServiceLinkedRoleCheck` parámetro en`false`, el control fallará porque es posible que otros roles no tengan los permisos necesarios AWS Config para registrar tus recursos con precisión.

El AWS Config servicio gestiona la configuración de AWS los recursos admitidos en tu cuenta y te entrega los archivos de registro. La información registrada incluye el elemento de configuración (AWS recurso), las relaciones entre los elementos de configuración y cualquier cambio de configuración en los recursos. Los recursos globales son recursos que están disponibles en cualquier región.

El control se evalúa de la siguiente manera:

- Si la región actual se establece como su región de agregación, el control solo produce `PASSED` resultados si se registran los recursos globales AWS Identity and Access Management (de IAM) (si ha habilitado los controles que los requieren).
- Si la región actual está configurada como una región vinculada, el control no evalúa si se registran recursos globales de IAM.
- Si la región actual no está en su agregador o si la agregación entre regiones no está configurada en la cuenta, el control solo produce resultados `PASSED` si se registran los recursos globales de IAM (si ha habilitado los controles que los requieren).

Los resultados del control no se ven afectados por el registro diario o continuo de los cambios en el estado de los recursos en AWS Config. Sin embargo, los resultados de este control pueden cambiar cuando se lanzan controles nuevos si se ha configurado la habilitación automática de los nuevos controles o si se cuenta con una política de configuración centralizada que habilita automáticamente los controles nuevos. En estos casos, si no registra todos los recursos, debe configurar el registro de los recursos asociados a los nuevos controles para recibir un resultado `PASSED`.

Las comprobaciones de seguridad del CSPM de Security Hub funcionan según lo previsto solo si habilitas el registro de recursos AWS Config en todas las regiones y configuras el registro de recursos para los controles que lo requieren.

> **Note**
>
> Config.1 requiere que AWS Config esté habilitada en todas las regiones en las que utilice Security Hub CSPM.
> Dado que el CSPM de Security Hub es un servicio regional, la comprobación que se realiza para este control evalúa solo la región actual de la cuenta.
> Para admitir los controles de seguridad en recursos globales de IAM de una región, debe registrar los recursos globales de IAM en esa región. Las regiones en las que no se hayan registrado los recursos globales de IAM recibirán un resultado `PASSED` predeterminado por los controles que comprueban los recursos globales de IAM. Dado que los recursos globales de IAM son idénticos en todos los países Regiones de AWS, le recomendamos que registre los recursos globales de IAM únicamente en la región de origen (si la agregación interregional está habilitada en su cuenta). Los recursos de IAM solo se registrarán en la región en la que esté activado el registro de recursos globales.
> Los tipos de recursos de IAM registrados a nivel mundial que AWS Config admite son los usuarios, los grupos, las funciones y las políticas gestionadas por los clientes de IAM. Puedes considerar la posibilidad de deshabilitar los controles de CSPM de Security Hub que comprueban estos tipos de recursos en las regiones en las que el registro global de recursos esté desactivado. Para obtener más información, consulte Controles sugeridos para desactivar en el CSPM de Security Hub.

Corrección

En la región de origen y en las regiones que no forman parte de un agregador, registre todos los recursos necesarios para los controles que están habilitados en la región actual, incluidos los recursos globales de IAM si ha habilitado los controles que requieren recursos globales de IAM.

En las regiones vinculadas, puede usar cualquier modo de AWS Config grabación, siempre y cuando registre todos los recursos que corresponden a los controles que están habilitados en la región actual. En las regiones vinculadas, si tiene habilitados controles que requieren el registro de recursos globales de IAM, no recibirá un resultado `FAILED` (el registro de otros recursos es suficiente).

El campo `StatusReasons` en el objeto `Compliance` del resultado puede ayudarle a determinar por qué tiene un resultado fallido para este control. Para obtener más información, consulte Detalles de cumplimiento para los resultados de control.

Para obtener una lista de los recursos que deben registrarse para cada control, consulte ObligatorioAWS Configrecursos para hallazgos de control. Para obtener información general sobre cómo habilitar AWS Config y configurar el registro de recursos, consulteActivación y configuración AWS Config para Security Hub CSPM.

Controles CSPM de Security Hub para Amazon Connect

Estos controles CSPM de Security Hub evalúan el servicio y los recursos de Amazon Connect.

Es posible que estos controles no estén disponibles en todos. Regiones de AWS Para obtener más información, consulte Disponibilidad de los controles por región.

[Connect.1] Los tipos de objetos de los perfiles de clientes de Amazon Connect deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::CustomerProfiles::ObjectType`

Regla de AWS Config: `customerprofiles-object-type-tagged`

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredKeyTags`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si un tipo de objeto de Perfiles de clientes de Amazon Connect tiene etiquetas con las claves específicas definidas en el parámetro `requiredKeyTags`. El control falla si el tipo de objeto no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredKeyTags`. Si no se proporciona el parámetro `requiredKeyTags`, el control solo comprueba la existencia de una clave de etiqueta y falla si el tipo de objeto no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte Definición de permisos basados en atributos con autorización ABAC en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte las mejores prácticas y estrategias en los AWSrecursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para añadir etiquetas a un tipo de objeto de perfiles de clientes, consulte Añadir etiquetas a los recursos de Amazon Connect Customer en la Guía del administrador de clientes de Connect.

[Connect.2] Las instancias de Connect Customer deben tener el CloudWatch registro habilitado

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: `AWS::Connect::Instance`

AWS Configregla: función de registro de instancias de conexión habilitada

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una instancia de Connect Customer está configurada para generar y almacenar registros de flujo en un grupo de CloudWatch registros de Amazon. El control falla si la instancia de Connect Customer no está configurada para generar y almacenar registros de flujo en un grupo de CloudWatch registros.

Los registros de flujo de clientes de Amazon Connect proporcionan detalles en tiempo real sobre los eventos de los flujos de clientes de Amazon Connect. Un flujo define la experiencia del cliente con un centro de atención al cliente de Amazon Connect de principio a fin. De forma predeterminada, al crear una nueva instancia de Amazon Connect Customer, se crea automáticamente un grupo de CloudWatch registros de Amazon para almacenar los registros de flujo de la instancia. Los registros de flujo pueden ayudar a analizar flujos, encontrar errores y supervisar métricas operativas. También puede configurar alertas para eventos específicos que pueden ocurrir en un flujo.

Corrección

Para obtener información sobre cómo habilitar los registros de flujo para una instancia de Amazon Connect Customer, consulte Habilitar los registros de flujo de Amazon Connect Customer en un grupo de registros de Amazon CloudWatch en la Guía del administrador de Amazon Connect Customer.

Controles CSPM de Security Hub para Amazon Data Firehose

Estos controles CSPM de Security Hub evalúan el servicio y los recursos de Amazon Data Firehose.

Es posible que estos controles no estén disponibles en todos. Regiones de AWS Para obtener más información, consulte Disponibilidad de los controles por región.

[DataFirehose.1] Los flujos de entrega de Firehose deben cifrarse en reposo

Requisitos relacionados: NIST.800-53.r5 AC-3, NIST.800-53.r5 AU-3, NIST.800-53.r5 SC-12, NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-28

Categoría: Proteger > Protección de datos > Cifrado de datos en reposo

Gravedad: media

Tipo de recurso: `AWS::KinesisFirehose::DeliveryStream`

Regla de AWS Config: `kinesis-firehose-delivery-stream-encrypted`

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si un flujo de entrega de Amazon Data Firehose está cifrado en reposo con el cifrado del servidor. Este control falla si un flujo de entrega de Firehose no se cifra en reposo con el cifrado del servidor.

Server-side el cifrado es una función de las transmisiones de entrega de Amazon Data Firehose que cifra automáticamente los datos antes de que estén en reposo mediante una clave creada en AWS Key Management Service (). AWS KMS Los datos se cifran antes de transmitirlos a la capa de almacenamiento del flujo de Data Firehose, y se descifran después de recuperarlos del almacenamiento. Esto permite cumplir con los requisitos normativos estrictos y mejorar la seguridad de sus datos.

Corrección

Para habilitar el cifrado del servidor en los flujos de entrega de Firehose, consulte Protección de datos en Amazon Data Firehose en la Guía para desarrolladores de Amazon Data Firehose.

Controles CSPM de Security Hub paraAWS Database Migration Service

Estos AWS Security Hub CSPM controles evalúan los AWS Database Migration Service (AWS DMS) y AWS DMS los recursos. Es posible que los controles no estén disponibles en todosRegiones de AWS. Para obtener más información, consulte Disponibilidad de los controles por región.

[DMS.1] Las instancias de replicación de Database Migration Service no deben ser públicas

Requisitos relacionados: NIST.800-53.r5 AC-21 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), (21) NIST.800-53.r5 AC-4,, NIST.800-53.r5 AC-4 (11) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9), PCI DSS v3.2. 1/1.2.1, PCI DSS v3.2. 1/1.3.1, PCI DSS v3.2. 1/1.3.4, PCI DSS v3.2. 1/1.3.2, PCI DSS v3.2. 1/1.3.6, PCI DSS v4.0. 1/1.4.4

Categoría: Proteger - Configuración de red segura

Gravedad: crítica

Tipo de recurso: `AWS::DMS::ReplicationInstance`

Regla de AWS Config: dms-replication-not-public

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si las instancias de AWS DMS replicación son públicas. Para ello, examina el valor del campo `PubliclyAccessible`.

Una instancia de replicación privada tiene una dirección IP privada a la que no puede obtener acceso desde fuera de la red de replicación. Una instancia de replicación debe tener una dirección IP privada cuando las bases de datos de origen y destino estén en la misma red. La red también debe estar conectada a la VPC de la instancia de replicación mediante una VPN o un emparejamiento Direct Connect de VPC. Para obtener más información sobre las instancias de replicación públicas y

privadas, consulte las instancias de Replicación públicas y privadas en la Guía del usuario de AWS Database Migration Service.

También debes asegurarte de que el acceso a la configuración de tu AWS DMS instancia esté limitado únicamente a los usuarios autorizados. Para ello, restrinja los permisos de IAM de los usuarios para modificar la AWS DMS configuración y los recursos.

Corrección

No puede cambiar la configuración de acceso público de una instancia de replicación del DMS después de crearla. Para cambiar la configuración de acceso público, elimine la instancia actual y, a continuación, vuelva a crearla. No seleccione la opción de Acceso público.

[DMS.2] Los certificados DMS deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::DMS::Certificate`

AWS Configregla: `tagged-dms-certificate` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	`No default value`

Este control comprueba si un AWS DMS certificado tiene etiquetas con las claves específicas definidas en el parámetro`requiredTagKeys`. El control falla si el certificado no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y falla si el certificado no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte Etiquetar sus AWS recursos en el. Referencia general de AWS

Corrección

Para agregar etiquetas a un certificado DMS, consulte Etiquetado de recursos en AWS Database Migration Service en la Guía del usuario de AWS Database Migration Service.

[DMS.3] Las suscripciones a eventos de DMS deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::DMS::EventSubscription`

AWS Configregla: `tagged-dms-eventsubscription` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	`No default value`

Este control comprueba si la suscripción a un AWS DMS evento tiene etiquetas con las claves específicas definidas en el parámetro`requiredTagKeys`. El control falla si la suscripción a un evento no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y falla si la suscripción a un evento no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan

operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte Etiquetar sus AWS recursos en el. Referencia general de AWS

Corrección

Para agregar etiquetas a una inscripción a un evento, consulte Etiquetado de recursos en AWS Database Migration Service en la Guía del usuario de AWS Database Migration Service.

[DMS.4] Las instancias de replicación de DMS deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::DMS::ReplicationInstance`

AWS Configregla: `tagged-dms-replicationinstance` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que	`No default value`

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
	recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.		cumplan los requisitos de AWS.	

Este control comprueba si una instancia de AWS DMS replicación tiene etiquetas con las claves específicas definidas en el parámetro`requiredTagKeys`. El control falla si la instancia de replicación no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y falla si la instancia de replicación no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte Etiquetar sus AWS recursos en el. Referencia general de AWS

Corrección

Para agregar etiquetas a una instancia de replicación, consulte Etiquetado de recursos en AWS Database Migration Service en la Guía del usuario de AWS Database Migration Service.

[DMS.5] Los grupos de subredes de replicación del DMS deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::DMS::ReplicationSubnetGroup`

AWS Configregla: `tagged-dms-replicationsubnetgroup` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	`No default value`

Este control comprueba si un grupo de subredes de AWS DMS replicación tiene etiquetas con las claves específicas definidas en el parámetro`requiredTagKeys`. El control falla si el grupo de subredes de replicación no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y falla si el

grupo de subredes de replicación no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte Etiquetar sus AWS recursos en el. Referencia general de AWS

Corrección

Para agregar etiquetas a un grupo de subredes de replicación, consulte Etiquetado de recursos en AWS Database Migration Service en la Guía del usuario de AWS Database Migration Service.

[DMS.6] Las instancias de replicación de DMS deben tener habilitada la actualización automática de las versiones secundarias

Requisitos relacionados: NIST.800-53.r5 SI-2 NIST.800-53.r5 SI-2 (2), (4), NIST.800-53.r5 SI-2 NIST.800-53.r5 SI-2 (5), PCI DSS v4.0. 1/63.3.3

Categoría: Identificar > Administración de vulnerabilidades, parches y versiones

Gravedad: media

Tipo de recurso: `AWS::DMS::ReplicationInstance`

Regla de AWS Config: dms-auto-minor-version-upgrade-check

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si la actualización automática de la versión secundaria está habilitada para una instancia de AWS DMS replicación. El control falla si la actualización automática de la versión secundaria no está habilitada para una instancia de replicación del DMS.

El DMS proporciona una actualización automática de las versiones secundarias de cada motor de replicación compatible para que pueda mantener la instancia de replicación actualizada. Las versiones secundarias pueden introducir nuevas funciones de software, correcciones de errores, parches de seguridad y mejoras de rendimiento. Al habilitar la actualización automática de las versiones secundarias en las instancias de replicación del DMS, las actualizaciones menores se aplican automáticamente durante el período de mantenimiento o inmediatamente si se selecciona la opción Aplicar los cambios inmediatamente.

Corrección

Para habilitar la actualización automática de la versión secundaria en las instancias de replicación del DMS, consulte Modificación de una instancia de replicación en la Guía del usuario de AWS Database Migration Service.

[DMS.7] Las tareas de replicación del DMS para la base de datos de destino deben tener el registro habilitado

Requisitos relacionados: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9),, NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12 NIST.800-53.r5 AU-2 NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), (9) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (8), NIST.800-53.r5 SI-3 (20), NIST.800-53.r5 SI-4 NIST.800-53.r5 SI-7 (8), PCI DSS v4.0. 1/104.4.2

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: `AWS::DMS::ReplicationTask`

Regla de AWS Config: dms-replication-task-targetdb-logging

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si el registro está habilitado con el nivel de gravedad mínimo `LOGGER_SEVERITY_DEFAULT` para las tareas de replicación del DMS `TARGET_APPLY` y `TARGET_LOAD`. El control falla si el registro no está habilitado para estas tareas o si el nivel de gravedad mínimo es inferior a `LOGGER_SEVERITY_DEFAULT`.

DMS utiliza Amazon CloudWatch para registrar la información durante el proceso de migración. Con la configuración de tareas de registro, puede especificar qué actividades de componentes se registran y qué cantidad de información se registra. Debe especificar el registro para las siguientes tareas:

- `TARGET_APPLY`: los datos e instrucciones de lenguaje de definición de datos (DDL) se aplican a la base de datos de destino.
- `TARGET_LOAD`: Los datos se cargan en la base de datos destino.

El registro desempeña un papel fundamental en las tareas de replicación del DMS, ya que permite la supervisión, la solución de problemas, la auditoría, el análisis del rendimiento, la detección de errores y la recuperación, así como el análisis histórico y la elaboración de informes. Ayuda a garantizar la replicación exitosa de los datos entre bases de datos y, al mismo tiempo, a mantener la integridad de los datos y el cumplimiento de los requisitos reglamentarios. Los niveles de registro que no estén fijados como `DEFAULT` suelen ser necesarios para estos componentes durante la resolución de problemas. Recomendamos mantener el nivel de registro igual que `DEFAULT` para estos componentes, a menos que se solicite específicamente cambiarloSoporte. Un nivel de registro mínimo como `DEFAULT` garantiza que los mensajes informativos, las advertencias y los mensajes de error se escriban en los registros. Este control comprueba si el nivel de registro es al menos uno de los siguientes para las tareas de replicación anteriores: `LOGGER_SEVERITY_DEFAULT`, `LOGGER_SEVERITY_DEBUG` o `LOGGER_SEVERITY_DETAILED_DEBUG`.

Corrección

Para habilitar el registro de las tareas de replicación del DMS de la base de datos de destino, consulte Visualización y administración de los registros de AWS DMS tareas en la Guía del AWS Database Migration Serviceusuario.

[DMS.8] Las tareas de replicación del DMS para la base de datos de origen deben tener el registro activado

Requisitos relacionados: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9),, NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12 NIST.800-53.r5 AU-2 NIST.800-53.r5 AU-3,

NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), (9) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (8), NIST.800-53.r5 SI-3 (20), NIST.800-53.r5 SI-4 NIST.800-53.r5 SI-7 (8), PCI DSS v4.0. 1/104.4.2

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: `AWS::DMS::ReplicationTask`

Regla de AWS Config: dms-replication-task-sourcedb-logging

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si el registro está habilitado con el nivel de gravedad mínimo `LOGGER_SEVERITY_DEFAULT` para las tareas de replicación del DMS `SOURCE_CAPTURE` y `SOURCE_UNLOAD`. El control falla si el registro no está habilitado para estas tareas o si el nivel de gravedad mínimo es inferior a `LOGGER_SEVERITY_DEFAULT`.

DMS utiliza Amazon CloudWatch para registrar la información durante el proceso de migración. Con la configuración de tareas de registro, puede especificar qué actividades de componentes se registran y qué cantidad de información se registra. Debe especificar el registro para las siguientes tareas:

- `SOURCE_CAPTURE`: Los datos de replicación continua o captura de datos modificados (CDC) se capturan de la base de datos o el servicio de origen y se transfieren al componente de servicio de `SORTER`.
- `SOURCE_UNLOAD`: Los datos se descargan de la base de datos o del servicio de origen durante la carga completa.

El registro desempeña un papel fundamental en las tareas de replicación del DMS, ya que permite la supervisión, la solución de problemas, la auditoría, el análisis del rendimiento, la detección de errores y la recuperación, así como el análisis histórico y la elaboración de informes. Ayuda a garantizar la replicación exitosa de los datos entre bases de datos y, al mismo tiempo, a mantener la integridad de los datos y el cumplimiento de los requisitos reglamentarios. Los niveles de registro que no estén fijados como `DEFAULT` suelen ser necesarios para estos componentes durante la resolución de problemas. Recomendamos mantener el nivel de registro igual que `DEFAULT` para estos componentes, a menos que se solicite específicamente cambiarloSoporte. Un nivel de registro mínimo como `DEFAULT` garantiza que los mensajes informativos, las advertencias y los mensajes

de error se escriban en los registros. Este control comprueba si el nivel de registro es al menos uno de los siguientes para las tareas de replicación anteriores: `LOGGER_SEVERITY_DEFAULT`, `LOGGER_SEVERITY_DEBUG` o `LOGGER_SEVERITY_DETAILED_DEBUG`.

Corrección

Para habilitar el registro de las tareas de replicación del DMS de la base de datos fuente, consulte Visualización y administración de los registros de AWS DMS tareas en la Guía del AWS Database Migration Serviceusuario.

[DMS.9] Los puntos finales del DMS deben usar SSL

Requisitos relacionados: NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (3), (4), NIST.800-53.r5 SC-7 (1) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 NIST.800-53.r5 SC-8 (2), PCI DSS v4.0. 1/42.2.1

Categoría: Proteger > Protección de datos > Cifrado de datos en tránsito

Gravedad: media

Tipo de recurso: `AWS::DMS::Endpoint`

Regla de AWS Config: dms-endpoint-ssl-configured

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un AWS DMS punto final utiliza una conexión SSL. El control falla si el punto de conexión no usa SSL.

SSL/TLS las conexiones proporcionan un nivel de seguridad al cifrar las conexiones entre las instancias de replicación del DMS y la base de datos. El uso de certificados brinda una capa extra de seguridad al validar que la conexión se realice en una base de datos esperada. Se hace al verificar que el certificado de servidor se instale automáticamente en todas las instancias de base de datos que usted aprovisiona. Al habilitar la conexión SSL en los puntos de conexión del DMS, se protege la confidencialidad de los datos durante la migración.

Corrección

Para añadir una conexión SSL a un punto de conexión de DMS nuevo o existente, consulte Uso de SSL de AWS Database Migration Service en la Guía del usuario de AWS Database Migration Service.

[DMS.10] Los puntos finales de DMS para las bases de datos de Neptune deben tener habilitada la autorización de IAM

Requisitos relacionados: NIST.800-53.r5 AC-2,,, NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-6 NIST.800-53.r5 AC-17, PCI DSS NIST.800-53.r5 IA-2 v4.0 NIST.800-53.r5 IA-5. 1/73.3.1

Categoría: Proteger > Gestión del acceso seguro > Autenticación sin contraseña

Gravedad: media

Tipo de recurso: `AWS::DMS::Endpoint`

Regla de AWS Config: dms-neptune-iam-authorization-enabled

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un AWS DMS punto final de una base de datos de Amazon Neptune está configurado con autorización de IAM. El control falla si el punto de conexión de DMS no tiene habilitada la autorización de IAM.

AWS Identity and Access Management(IAM) proporciona un control de acceso detallado en todas partes. AWS Con IAM, puede especificar quién puede acceder a qué servicios y recursos y en qué condiciones. Con las políticas de IAM, puede administrar los permisos del personal y sus sistemas para garantizar los permisos con privilegio mínimo. Al habilitar la autorización de IAM en AWS DMS los puntos finales de las bases de datos de Neptune, puede conceder privilegios de autorización a los usuarios de IAM mediante un rol de servicio especificado en el parámetro. `ServiceAccessRoleARN`

Corrección

Para habilitar la autorización de IAM en los puntos de conexión de DMS para las bases de datos de Neptune, consulte Uso de Amazon Neptune como destino para AWS Database Migration Service en la Guía del usuario de AWS Database Migration Service.

[DMS.11] Los puntos finales de DMS para MongoDB deben tener un mecanismo de autenticación habilitado

Requisitos relacionados: NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-6, PCI DSS NIST.800-53.r5 IA-2 v4.0 NIST.800-53.r5 IA-5. 1/73.3.1

Categoría: Proteger > Gestión del acceso seguro > Autenticación sin contraseña

Gravedad: media

Tipo de recurso: `AWS::DMS::Endpoint`

Regla de AWS Config: dms-mongo-db-authentication-enabled

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un AWS DMS punto final para MongoDB está configurado con un mecanismo de autenticación. El control falla si no se estableció un tipo de autenticación para el punto de conexión.

AWS Database Migration Serviceadmite dos métodos de autenticación para MongoDB MONGODB-CR: para MongoDB versión 2.x y para MongoDB versión 3.x SCRAM-SHA-1o posterior. Estos métodos de autenticación se utilizan para autenticar y cifrar las contraseñas de MongoDB si los usuarios desean utilizarlas para acceder a las bases de datos. La autenticación en los AWS DMS puntos finales garantiza que solo los usuarios autorizados puedan acceder a los datos que se migran entre bases de datos y modificarlos. Sin la autenticación adecuada, los usuarios no autorizados pueden acceder a datos confidenciales durante el proceso de migración. Esto puede provocar filtraciones de datos, pérdida de datos u otros incidentes de seguridad.

Corrección

Para habilitar un mecanismo de autenticación en los puntos de conexión de DMS para MongoDB, consulte Uso de MongoDB como origen en AWS DMS en la Guía del usuario de AWS Database Migration Service.

[DMS.12] Los puntos finales de DMS para Redis OSS deben tener el TLS habilitado

Requisitos relacionados: PCI DSS NIST.800-53.r5 SC-8 v4.0 NIST.800-53.r5 SC-13. 1/42.2.1

Categoría: Proteger > Protección de datos > Cifrado de datos en tránsito

Gravedad: media

Tipo de recurso: `AWS::DMS::Endpoint`

Regla de AWS Config: dms-redis-tls-enabled

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un AWS DMS punto final para Redis OSS está configurado con una conexión TLS. El control falla si el punto de conexión no tiene habilitado el TLS.

El TLS proporciona una seguridad integral cuando los datos se envían entre aplicaciones o bases de datos a través de Internet. Al configurar el cifrado SSL para su punto de conexión de DMS, permite la comunicación cifrada entre las bases de datos de origen y destino durante el proceso de migración. Esto ayuda a evitar el espionaje y la interceptación de datos confidenciales por parte de actores malintencionados. Sin el cifrado SSL, se puede acceder a los datos confidenciales, lo que provoca filtraciones de datos, pérdida de datos u otros incidentes de seguridad.

Corrección

Para habilitar una conexión TLS en los puntos de conexión de DMS para Redis, consulte Uso de Redis como destino para AWS Database Migration Service en la Guía del usuario de AWS Database Migration Service.

[DMS.13] Las instancias de replicación de DMS deben configurarse para usar varias zonas de disponibilidad

Categoría: Recuperación > Resiliencia > Alta disponibilidad

Gravedad: media

Tipo de recurso: `AWS::DMS::ReplicationInstance`

Regla de AWS Config: dms-replication-instance-multi-az-enabled

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una instancia de replicación AWS Database Migration Service (AWS DMS) está configurada para usar varias zonas de disponibilidad (Multi-AZ implementación). El control falla si la instancia de AWS DMS replicación no está configurada para usar una Multi-AZ implementación.

En una Multi-AZ implementación, aprovisiona y mantiene AWS DMS automáticamente una réplica en espera de una instancia de replicación en una zona de disponibilidad (AZ) diferente. La instancia de replicación principal se replica luego de manera sincronizada en la réplica en espera. Si la instancia de replicación principal falla o no responde, la instancia en espera reanuda cualquier tarea en

ejecución con una interrupción mínima. Para obtener más información, consulte Uso de una instancia de replicación en la Guía del usuario de AWS Database Migration Service.

Corrección

Tras crear una instancia de AWS DMS replicación, puede cambiar la configuración de Multi-AZ implementación de la misma. Para obtener información sobre cómo cambiar esta y otras configuraciones de una instancia de replicación existente, consulte Modificación de una instancia de replicación en la Guía del usuario de AWS Database Migration Service.

Controles CSPM de Security Hub paraAWS DataSync

Estos controles CSPM de Security Hub evalúan el AWS DataSync servicio y los recursos. Es posible que los controles no estén disponibles en todos. Regiones de AWS Para obtener más información, consulte Disponibilidad de los controles por región.

[DataSync.1] DataSync las tareas deberían tener el registro activado

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: `AWS::DataSync::Task`

Regla de AWS Config: datasync-task-logging-enabled

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una AWS DataSync tarea tiene activado el registro. El control falla si la tarea no tiene habilitado el registro.

Los registros de auditoría rastrean y supervisan las actividades del sistema. Proporcionan un registro de los eventos que puede ayudarlo a detectar brechas de seguridad, investigar incidentes y cumplir con las normativas. Los registros de auditoría también mejoran la responsabilidad y la transparencia generales de su organización.

Corrección

Para obtener información sobre cómo configurar el registro para AWS DataSync las tareas, consulte Supervisión de las transferencias de datos con Amazon CloudWatch Logs en la Guía del AWS DataSync usuario.

[DataSync.2] DataSync las tareas deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::DataSync::Task`

Regla de AWS Config: datasync-task-tagged

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredKeyTags`	Una lista de claves de etiqueta que no son del sistema y que se deben asignar a un recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si una AWS DataSync tarea tiene las claves de etiqueta especificadas por el `requiredKeyTags` parámetro. El control falla si la tarea no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas por el parámetro `requiredKeyTags`. Si no especifica ningún valor para el parámetro `requiredKeyTags`, el control solo verifica la existencia de una clave de etiqueta y falla si la tarea no tiene ninguna clave de etiqueta. El control ignora las etiquetas del sistema, que se aplican automáticamente y tienen el prefijo `aws:`.

Una etiqueta es una etiqueta que se crea y se asigna a un AWS recurso. Cada etiqueta consta de una clave de etiqueta necesaria y un valor de etiqueta opcional. Utilice etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. También pueden ayudar a identificar, organizar, buscar y filtrar recursos. También pueden ayudar a rastrear propietarios de recursos

para acciones y notificaciones. También puede usar etiquetas para implementar control de acceso basado en atributos (ABAC) como estrategia de autorización. Para obtener más información sobre estrategias ABAC, consulte Definición de permisos basados en atributos con autorización ABAC en la Guía del usuario de IAM. Para obtener más información sobre las etiquetas, consulte los AWSrecursos de etiquetado y la Guía del usuario del editor de etiquetas.

> **Note**
>
> No almacene información de identificación personal (PII) ni otra información confidencial en las etiquetas. Se puede acceder a las etiquetas desde muchos Servicios de AWS sitios. No están destinadas a usarse para datos privados o información confidencial.

Corrección

Para obtener información sobre cómo añadir etiquetas a una AWS DataSync tarea, consulte Etiquetar AWS DataSync las tareas en la Guía del AWS DataSync usuario.

Controles CSPM de Security Hub para Amazon Detective

Este AWS Security Hub CSPM control evalúa el servicio y los recursos de Amazon Detective. Es posible que el control no esté disponible en todas las Regiones de AWS. Para obtener más información, consulte Disponibilidad de los controles por región.

[Detective.1] Los gráficos de comportamiento de los detectives deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::Detective::Graph`

AWS Configregla: `tagged-detective-graph` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	`No default value`

Este control comprueba si un gráfico de comportamiento de Amazon Detective tiene etiquetas con las claves específicas definidas en el parámetro`requiredTagKeys`. El control falla si el gráfico de comportamiento no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y falla si el gráfico de comportamiento no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte Etiquetar sus AWS recursos en el. Referencia general de AWS

Corrección

Para agregar etiquetas a un gráfico de comportamiento de Detective, consulte Agregar etiquetas a un gráfico de comportamiento en la Guía de administración de Amazon Detective.

Controles de CSPM de Security Hub para Amazon DocumentDB

Estos AWS Security Hub CSPM controles evalúan el servicio y los recursos de Amazon DocumentDB (compatible con MongoDB). Es posible que los controles no estén disponibles en todos. Regiones de AWS Para obtener más información, consulte Disponibilidad de los controles por región.

[DocumentDB.1] Los clústeres de Amazon DocumentDB deben cifrarse en reposo

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6)

Categoría: Proteger > Protección de datos > Cifrado de datos en reposo

Gravedad: media

Tipo de recurso: `AWS::RDS::DBCluster`

Regla de AWS Config: docdb-cluster-encrypted

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un clúster de Amazon DocumentDB está cifrado en reposo. El control falla si un clúster de Amazon DocumentDB no está cifrado en reposo.

Los datos en reposo se refieren a cualquier dato que se almacene en un almacenamiento persistente y no volátil durante cualquier período de tiempo. El cifrado le ayuda a proteger la confidencialidad

de dichos datos, reduciendo el riesgo de que un usuario no autorizado acceda a ellos. Los datos de los clústeres de Amazon DocumentDB deben cifrarse en reposo para ofrecer un nivel de seguridad adicional. Amazon DocumentDB utiliza el estándar de cifrado avanzado de 256 bits (AES-256) para cifrar los datos mediante claves de cifrado almacenadas en (). AWS Key Management Service AWS KMS

Corrección

Puede habilitar el cifrado en reposo al crear un clúster de Amazon DocumentDB. No se puede cambiar la configuración de cifrado después de crear un clúster. Para obtener más información, consulte Habilitar el cifrado en reposo para un clúster de Amazon DocumentDB en la Guía para desarrolladores de Amazon DocumentDB.

[DocumentDB.2] Los clústeres de Amazon DocumentDB deben tener un período de retención de copias de seguridad adecuado

Requisitos relacionados: NIST.800-53.r5 SI-12 PCI DSS v4.0. 1/32.2.1

Categoría: Recuperación > Resiliencia > Respaldos habilitados

Gravedad: media

Tipo de recurso: `AWS::RDS::DBCluster`

Regla de AWS Config: docdb-cluster-backup-retention-check

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`minimumBackupRetentionPeriod`	El periodo mínimo de retención de copias de seguridad en días	Entero	De 7 a 35	7

Este control comprueba si un clúster de Amazon DocumentDB tiene un periodo de retención de copias de seguridad superior o igual al periodo especificado. Se produce un error en el control si el periodo de retención de copia de seguridad es inferior al periodo especificado. A menos que proporcione un valor de parámetro personalizado para el período de retención de la copia de seguridad, Security Hub CSPM utiliza un valor predeterminado de 7 días.

Las copias de seguridad le ayudan a recuperarse más rápidamente de un incidente de seguridad y a reforzar la resiliencia de sus sistemas. Al automatizar las copias de seguridad de los clústeres de Amazon DocumentDB, podrá restaurar los sistemas en un momento determinado y minimizar el tiempo de inactividad y la pérdida de datos. En Amazon DocumentDB, los clústeres tienen un periodo predeterminado de retención de copia de seguridad de 1 día. Debe aumentarse a un valor de entre 7 y 35 días para superar este control.

Corrección

Para cambiar el período de retención de copias de seguridad de sus clústeres de Amazon DocumentDB, consulte Modificación de un clúster de Amazon DocumentDB en la Guía para desarrolladores de Amazon DocumentDB. En Copia de seguridad, elija el periodo de retención de copia de seguridad.

[DocumentDB.3] Las instantáneas de clústeres manuales de Amazon DocumentDB no deben ser públicas

Requisitos relacionados: NIST.800-53.r5 AC-21 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 AC-4,, (11) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), PCI DSS v4.0.1/14.4.4

Categoría: Proteger - Configuración de red segura

Gravedad: crítica

Tipo de recurso: `AWS::RDS::DBClusterSnapshot`

Regla de AWS Config: docdb-cluster-snapshot-public-prohibited

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una instantánea de clúster manual de Amazon DocumentDB es pública. El control falla si la instantánea manual del clúster es pública.

Una instantánea manual de un clúster de Amazon DocumentDB no debe ser pública a menos que se pretenda. Si comparte una instantánea manual sin cifrar públicamente, la instantánea estará disponible para todo Cuentas de AWS. Las instantáneas públicas pueden provocar una exposición no intencionada de los datos.

> **Note**
>
> Este control evalúa las instantáneas de clúster manuales. No se pueden compartir instantáneas automatizadas de un clúster de Amazon DocumentDB. Sin embargo, puede crear una instantánea manual copiando la instantánea automatizada y compartiéndola después.

Corrección

Para eliminar el acceso público a las instantáneas de clústeres manuales de Amazon DocumentDB, consulte Compartir una instantánea en la Guía para desarrolladores de Amazon DocumentDB. Mediante programación, puede utilizar la operación Amazon DocumentDB de `modify-db-snapshot-attribute`. Establecer `attribute-name` en `restore` y `values-to-remove` en `all`.

[DocumentDB.4] Los clústeres de Amazon DocumentDB deben publicar los registros de auditoría en Logs CloudWatch

Requisitos relacionados: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9),, NIST.800-53.r5 AU-10 NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-6 (3) NIST.800-53.r5 AU-2 NIST.800-53.r5 AU-3, (4), NIST.800-53.r5 AU-6 (9) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), (8), NIST.800-53.r5 SI-3 (20), NIST.800-53.r5 SI-4 NIST.800-53.r5 SI-7 (8), PCI DSS v4.0. 1/103.3.3

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: `AWS::RDS::DBCluster`

Regla de AWS Config: docdb-cluster-audit-logging-enabled

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un clúster de Amazon DocumentDB publica registros de auditoría en Amazon CloudWatch Logs. El control falla si el clúster no publica los registros de auditoría en CloudWatch Logs.

Amazon DocumentDB (con compatibilidad con MongoDB) le permite auditar eventos que se realizaron en su clúster. Los intentos de autenticación correctos e incorrectos, la eliminación de una colección en una base de datos o la creación de un índice son algunos ejemplos de eventos registrados. De forma predeterminada, la auditoría está deshabilitada en Amazon DocumentDB y requiere que tome medidas para habilitarla.

Corrección

Para publicar los registros de auditoría de Amazon DocumentDB en Logs, consulte Habilitar la auditoría en la Guía para CloudWatch desarrolladores de Amazon DocumentDB.

[DocumentDB.5] Los clústeres de Amazon DocumentDB deben tener habilitada la protección contra eliminaciones

Requisitos relacionados: NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2) NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2)

Categoría: Proteger > Protección de datos > Protección contra la eliminación de datos

Gravedad: media

Tipo de recurso: `AWS::RDS::DBCluster`

Regla de AWS Config: docdb-cluster-deletion-protection-enabled

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un clúster de Amazon DocumentDB tiene habilitada la protección contra eliminación. El control falla si el clúster no tiene habilitada la protección contra eliminación.

La activación de la protección contra la eliminación de clústeres ofrece un nivel adicional de protección contra la eliminación accidental de la base de datos o la eliminación por parte de un usuario no autorizado. No se puede eliminar un clúster de Amazon DocumentDB mientras esté habilitada la protección contra eliminación. Primero debe deshabilitar la protección contra la

eliminación para que la solicitud de eliminación se pueda realizar correctamente. La protección contra eliminación se habilita de forma predeterminada cuando crea un clúster mediante la consola de Amazon DocumentDB.

Corrección

Para habilitar la protección contra la eliminación de un clúster de Amazon DocumentDB existente, consulte Modificación de un clúster de Amazon DocumentDB en la Guía para desarrolladores de Amazon DocumentDB. En la sección Modificar el clúster, seleccione Habilitar la Protección contra la eliminación.

[DocumentDB.6] Los clústeres de Amazon DocumentDB deben cifrarse en tránsito

Categoría: Proteger > Protección de datos > Cifrado de datos en tránsito

Gravedad: media

Tipo de recurso: `AWS::RDS::DBCluster`

Regla de AWS Config: docdb-cluster-encrypted-in-transit

Tipo de programa: Periódico

Parámetros: `excludeTlsParameters`: `disabled`, `enabled` (no personalizables)

Este control comprueba si un clúster de Amazon DocumentDB requiere TLS para las conexiones al clúster. El control falla si el grupo de parámetros del clúster asociado con el clúster no está sincronizado, o si el parámetro TLS del clúster está configurado en `disabled` o `enabled`.

Puede usar TLS para cifrar la conexión entre una aplicación y un clúster de Amazon DocumentDB. El uso de TLS puede ayudar a proteger los datos de ser interceptados mientras están en tránsito entre una aplicación y un clúster de Amazon DocumentDB. El cifrado en tránsito para un clúster de Amazon DocumentDB se administra mediante el parámetro TLS en el grupo de parámetros del clúster asociado al clúster. Cuando se habilita el cifrado en tránsito, se requieren conexiones seguras con TLS para conectarse al clúster. Recomendamos usar los siguientes parámetros TLS: `tls1.2+`, `tls1.3+` y `fips-140-3`.

Corrección

Para obtener información sobre cómo cambiar la configuración de TLS para un clúster de Amazon DocumentDB, consulte Cifrado de datos en tránsito en la Guía del desarrollador de Amazon DocumentDB.

Controles CSPM de Security Hub para DynamoDB

Estos AWS Security Hub CSPM controles evalúan el servicio y los recursos de Amazon DynamoDB. Es posible que los controles no estén disponibles en todos. Regiones de AWS Para obtener más información, consulte Disponibilidad de los controles por región.

[DynamoDB.1] Las tablas de DynamoDB deberían escalar automáticamente la capacidad en función de la demanda

Requisitos relacionados: NIST.800-53.r5 CP-10 NIST.800-53.r5 CP-2 (2), NIST.800-53.r5 CP-6 (2) NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoría: Recuperación > Resiliencia > Alta disponibilidad

Gravedad: media

Tipo de recurso: `AWS::DynamoDB::Table`

Regla de AWS Config: `dynamodb-autoscaling-enabled`

Tipo de programa: Periódico

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados válidos	Valor predeterminado de CSPM de Security Hub
`minProvisionedReadCapacity`	Número mínimo de unidades de capacidad de lectura aprovisionadas para el escalado automático de DynamoDB	Entero	De `1` a `40000`	Sin valor predeterminado
`targetReadUtilization`	Porcentaje de uso objetivo de capacidad de lectura	Entero	De `20` a `90`	Sin valor predeterminado

Parámetro	Descripción	Tipo	Valores personalizados válidos	Valor predeterminado de CSPM de Security Hub
`minProvisionedWriteCapacity`	Número mínimo de unidades de capacidad de escritura aprovisionadas para el escalado automático de DynamoDB	Entero	De `1` a `40000`	Sin valor predeterminado
`targetWriteUtilization`	Porcentaje de uso objetivo de capacidad de escritura	Entero	De `20` a `90`	Sin valor predeterminado

Este control comprueba si una tabla de Amazon DynamoDB puede escalar su capacidad de lectura y escritura según sea necesario. Se produce un error en el control si la tabla utiliza el modo de capacidad bajo demanda o el modo aprovisionado con el escalado automático configurado. De manera predeterminada, este control solo requiere que se configure uno de estos modos, independientemente de los niveles específicos de la capacidad de lectura o escritura. De manera opcional, puede proporcionar valores personalizados de parámetros para requerir niveles específicos de la capacidad de lectura y escritura o de utilización objetivo.

Escalar la capacidad en función de la demanda evita limitar las excepciones, lo que ayuda a mantener la disponibilidad de las aplicaciones. Las tablas de DynamoDB que usan el modo de capacidad bajo demanda solo están limitadas por las cuotas predeterminadas de rendimiento de las tablas de DynamoDB. Para aumentar estas cuotas, puede presentar una solicitud de asistencia en. Soporte Las tablas de DynamoDB que usan el modo aprovisionado con escalado automático ajustan la capacidad de rendimiento aprovisionada de forma dinámica de acuerdo con los patrones de tráfico. Para obtener más información acerca de la limitación de solicitudes de DynamoDB, consulte Limitación controlada de solicitudes y capacidad de ampliación en la Guía para desarrolladores de Amazon DynamoDB.

Corrección

Para habilitar el escalado automático de DynamoDB en tablas existentes en el modo de capacidad, consulte Habilitación de la función Auto Scaling de DynamoDB en tablas existentes en la Guía para desarrolladores de Amazon DynamoDB.

[DynamoDB.2] Las tablas de DynamoDB deben tener habilitada la recuperación puntual

Requisitos relacionados: NIST.800-53.r5 CP-10 NIST.800-53.r5 CP-6 (2), (2) NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (5) NIST.800-53.r5 SI-12 NIST.800-53.r5 SI-13

Categoría: Recuperación > Resiliencia > Respaldos habilitados

Gravedad: media

Tipo de recurso: `AWS::DynamoDB::Table`

Regla de AWS Config: `dynamodb-pitr-enabled`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si la recuperación en un momento dado (PITR) está habilitada para una tabla de Amazon DynamoDB.

Las copias de seguridad le ayudan a recuperarse más rápidamente de un incidente de seguridad. También refuerzan la resiliencia de sus sistemas. La recuperación a un momento dado en DynamoDB automatiza las copias de seguridad de las tablas de DynamoDB. Reduce el tiempo de recuperación tras operaciones de borrado o escritura accidentales. Las tablas de DynamoDB que tienen PITR habilitada se pueden restaurar a cualquier momento de los últimos 35 días.

Corrección

Para restaurar una tabla de DynamoDB a un punto en el tiempo, consulte Restauración de una tabla de DynamoDB a un punto en el tiempo en la Guía para desarrolladores de Amazon DynamoDB.

[DynamoDB.3] Los clústeres de DynamoDB Accelerator (DAX) deben cifrarse en reposo

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28 (1) NIST.800-53.r5 SC-28, (10), NIST.800-53.r5 SC-7 (6) NIST.800-53.r5 SI-7

Categoría: Proteger > Protección de datos > Cifrado de datos en reposo

Gravedad: media

Tipo de recurso: `AWS::DAX::Cluster`

Regla de AWS Config: `dax-encryption-enabled`

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si un clúster de Acelerador de Amazon DynamoDB (DAX) está cifrado en reposo. El control lanza un error si un clúster de DAX no está cifrado en reposo.

El cifrado de los datos en reposo reduce el riesgo de que un usuario no autenticado acceda a los datos almacenados en el disco. AWS El cifrado añade otro conjunto de controles de acceso para limitar la capacidad de los usuarios no autorizados de acceder a los datos. Por ejemplo, se requieren permisos de API para descifrar los datos antes de que puedan leerse.

Corrección

No puede habilitar o deshabilitar el cifrado en reposo después de haber creado un clúster. Debe volver a crear el clúster para habilitar el cifrado en reposo. Para obtener instrucciones detalladas sobre cómo crear un clúster de DAX con el cifrado en reposo activado, consulte Habilitar el cifrado en reposo mediante la Consola de administración de AWS en la Guía para desarrolladores de Amazon DynamoDB.

[DynamoDB.4] Las tablas de DynamoDB deben estar presentes en un plan de respaldo

Requisitos relacionados: NIST.800-53.r5 CP-10 NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6 (1), NIST.800-53.r5 CP-6 (2) NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2) NIST.800-53.r5 SI-12, NIST.800-53.r5 SI-13 (5)

Categoría: Recuperación > Resiliencia > Respaldos habilitados

Gravedad: media

Tipo de recurso: `AWS::DynamoDB::Table`

AWS Configregla: **`dynamodb-resources-protected-by-backup-plan`**

Tipo de programa: Periódico

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`backupVaultLockCheck`	El control determina si el parámetro está establecido en AWS Backup Vault Lock `true` y el recurso lo utiliza. `PASSED`	Booleano	`true` o `false`	Sin valor predeterminado

Este control evalúa si una tabla de Amazon DynamoDB en estado `ACTIVE` está cubierta por un plan de copias de seguridad. Se produce un error en el control si la tabla de DynamoDB no está cubierta por un plan de copias de seguridad. Si establece el `backupVaultLockCheck` parámetro en un valor igual `atrue`, el control solo pasa si la tabla de DynamoDB está guardada en AWS Backup un almacén cerrado.

AWS Backupes un servicio de copias de seguridad totalmente gestionado que le ayuda a centralizar y automatizar las copias de seguridad de todos los datos. Servicios de AWS Con AWS Backup él, puede crear planes de respaldo que definan sus requisitos de respaldo, como la frecuencia con la que debe realizar copias de seguridad de sus datos y cuánto tiempo debe conservarlas. La inclusión de tablas de DynamoDB en sus planes de copia de seguridad le ayuda a proteger sus datos de pérdidas o eliminaciones involuntarias.

Corrección

Para agregar una tabla de DynamoDB a AWS Backup un plan de respaldo, consulte Asignación de recursos a un plan de respaldo en la Guía para desarrolladores. AWS Backup

[DynamoDB.5] Las tablas de DynamoDB deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::DynamoDB::Table`

AWS Configregla: `tagged-dynamodb-table` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	`No default value`

Este control comprueba si una tabla de Amazon DynamoDB tiene etiquetas con claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza un error si la tabla no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si la tabla no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte Etiquetar sus AWS recursos en el. Referencia general de AWS

Corrección

Para agregar etiquetas a una tabla de DynamoDB, consulte Etiquetado de recursos en DynamoDB en la Guía para desarrolladores de Amazon DynamoDB.

[DynamoDB.6] Las tablas de DynamoDB deben tener habilitada la protección de eliminación

Requisitos relacionados: NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2) NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2)

Categoría: Proteger > Protección de datos > Protección contra la eliminación de datos

Gravedad: media

Tipo de recurso: `AWS::DynamoDB::Table`

AWS Configregla: **`dynamodb-table-deletion-protection-enabled`**

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una tabla de Amazon DynamoDB tiene habilitada la protección contra eliminación. Se produce un error en el control si una tabla DynamoDB no tiene habilitada la protección contra eliminación.

Puede proteger una tabla de DynamoDB contra la eliminación accidental con la propiedad de protección contra la eliminación. Habilitar esta propiedad para las tablas ayuda a garantizar que los administradores no eliminen las tablas accidentalmente durante las operaciones habituales de administración. De este modo, evita que se interrumpan las operaciones comerciales normales.

Corrección

Para habilitar la protección contra eliminación de una tabla de DynamoDB, consulte Uso de la protección contra eliminación en la Guía para desarrolladores de Amazon DynamoDB.

[DynamoDB.7] Los clústeres de DynamoDB Accelerator deben cifrarse en tránsito

Requisitos relacionados: NIST.800-53.r5 AC-17,, NIST.800-53.r5 SC-8 NIST.800-53.r5 SC-13, PCI DSS NIST.800-53.r5 SC-23 v4.0. 1/42.2.1

Categoría: Proteger > Protección de datos > Cifrado de datos en tránsito

Gravedad: media

Tipo de recurso: `AWS::DAX::Cluster`

Regla de AWS Config: `dax-tls-endpoint-encryption`

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si un clúster de Acelerador de Amazon DynamoDB (DAX) está cifrado en tránsito, con el tipo de cifrado de punto de conexión establecido en TLS. El control lanza un error si el clúster de DAX no está cifrado en tránsito.

Puede utilizar HTTPS (TLS) para ayudarle a evitar posibles ataques de tipo “intermediario”, de espionaje o de manipulación del tráfico de red. Solo debe permitir que conexiones cifradas pasen por TLS para acceder a los clústeres de DAX. Sin embargo, el cifrado de los datos en tránsito puede afectar el rendimiento. Debe probar su aplicación con cifrado para comprender el perfil de rendimiento y el impacto de TLS.

Corrección

No se puede cambiar la configuración de cifrado de TLS después de crear un clúster de DAX. Para cifrar un clúster de DAX existente, cree un nuevo clúster con el cifrado en tránsito habilitado, traslade el tráfico de la aplicación hacia él y, a continuación, elimine el clúster anterior. Para obtener más información, consulte Uso de la protección contra eliminación en la Guía para desarrolladores de Amazon DynamoDB.

Controles CSPM de Security Hub para Amazon EC2

Estos AWS Security Hub CSPM controles evalúan el servicio y los recursos de Amazon Elastic Compute Cloud (Amazon EC2). Es posible que los controles no estén disponibles en todos Regiones de AWS. Para obtener más información, consulte Disponibilidad de los controles por región.

[EC2.1] Las instantáneas de Amazon EBS no deben configurarse para que se puedan restaurar públicamente

Requisitos relacionados: PCI DSS v3.2. 1/12.2.1, PCI DSS v3.2. 1/1.3.1, PCI DSS v3.2. 1/1.3.4, PCI DSS v3.2. 1/7.2.1, NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21),, (11) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9) NIST.800-53.r5 SC-7

Categoría: Proteger - Configuración de red segura

Gravedad: crítica

Tipo de recurso: `AWS::::Account`

Regla de AWS Config : `ebs-snapshot-public-restorable-check`

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si las instantáneas de Amazon Elastic Block Store están configuradas para poder restaurarse públicamente. El control falla si las instantáneas de Amazon EBS están configuradas para que todos puedan restaurarlas.

Las instantáneas de EBS se utilizan para hacer una copia de seguridad de los datos de sus volúmenes de EBS en Amazon S3 en un momento específico. Puede utilizar las instantáneas para restaurar estados anteriores de volúmenes de EBS. Rara vez es aceptable compartir una instantánea con el público. Por lo general, la decisión de compartir una instantánea públicamente se toma por error o sin una comprensión completa de las consecuencias. Esta comprobación ayuda a garantizar que todos esos intercambios se planificaron y son intencionados.

Corrección

Para hacer privada una instantánea de EBS pública, consulte Compartir una instantánea en la Guía del usuario de Amazon EC2. En Acciones, Modificar permisos, seleccione Privado.

[EC2.2] Los grupos de seguridad predeterminados de VPC no deben permitir el tráfico entrante o saliente

Requisitos relacionados: CIS AWS Foundations Benchmark v5.0. 0/53.5, PCI DSS v3.2. 1/1.2.1, PCI DSS v3.2. 1/1.3.4, PCI DSS v3.2. 1/2.1, Punto de referencia sobre AWS los fundamentos de la CEI v1.2. 0/4.3, Punto de referencia sobre AWS los fundamentos de la CEI v1.4. 0/5.3,

Criterio de referencia sobre AWS los fundamentos de la CEI v3.0. 0/5.4 NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (5)

Categoría: Proteger - Configuración de red segura

Gravedad: alta

Tipo de recurso: `AWS::EC2::SecurityGroup`

Regla de AWS Config : `vpc-default-security-group-closed`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba que el grupo de seguridad predeterminado de una VPC permita el tráfico entrante o saliente. El control falla si el grupo de seguridad permite el tráfico entrante o saliente.

Las reglas del grupo de seguridad predeterminado permiten todo el tráfico saliente y entrante de las interfaces de red (y de sus instancias asociadas) asignadas al mismo grupo de seguridad. Le recomendamos que no utilice el grupo de seguridad predeterminado. Dado que el grupo de seguridad predeterminado no se puede eliminar, debería cambiar la configuración de reglas de grupo de seguridad predeterminada para restringir el tráfico entrante y saliente. Esto evita el tráfico no deseado si el grupo de seguridad predeterminado se configura accidentalmente para recursos como instancias EC2.

Corrección

Para solucionar este problema, comience por crear nuevos grupos de seguridad con privilegios mínimos. Para obtener instrucciones, consulte Crear un grupo de seguridad en la Guía del usuario de Amazon VPC. A continuación, asigne los nuevos grupos de seguridad a sus instancias de EC2. Para conocer las instrucciones, consulte Cambiar un grupo de seguridad de una instancia en la Guía del usuario de Amazon EC2.

Tras asignar los nuevos grupos de seguridad a sus recursos, elimine todas las reglas de entrada y salida de los grupos de seguridad predeterminados. Para conocer las instrucciones, consulte Configuración de las reglas de un grupo de seguridad en la Guía del usuario de Amazon VPC.

[EC2.3] Los volúmenes adjuntos de Amazon EBS deben cifrarse en reposo

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6)

Categoría: Proteger > Protección de datos > Cifrado de datos en reposo

Gravedad: media

Tipo de recurso: `AWS::EC2::Volume`

Regla de AWS Config : `encrypted-volumes`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si los volúmenes de EBS asociados están cifrados. Para superar esta comprobación, los volúmenes de EBS deben tener el estado de uso y estar cifrados. Si el volumen de EBS no está asociado, entonces no estará en el alcance de esta comprobación.

Para obtener una capa adicional de seguridad de la información confidencial en volúmenes de EBS, debe habilitar el cifrado de EBS en reposo. Amazon EBS ofrece una solución de cifrado sencilla para los recursos de EBS que no precisa que cree, mantenga y proteja su propia infraestructura de administración de claves. Utiliza claves CMK al crear volúmenes cifrados e instantáneas.

Para obtener más información acerca del cifrado de Amazon EBS, consulte Cifrado de Amazon EBS en la Guía del usuario de Amazon EC2.

Corrección

No existe una forma directa para cifrar un volumen o una instantánea sin cifrar existente. Solo puede cifrar un nuevo volumen o instantánea al crearlo.

Si ha habilitado el cifrado de forma predeterminada, Amazon EBS cifra el nuevo volumen o la instantánea resultante utilizando la clave predeterminada para el cifrado de Amazon EBS. Aunque no haya habilitado el cifrado de forma predeterminada, puede habilitarlo al crear un volumen o una instantánea individuales. En ambos casos, puede anular la clave predeterminada para el cifrado de Amazon EBS y elegir una clave administrada por el cliente simétrica.

Para obtener más información, consulte Creación de un volumen de Amazon EBS y Copia de una instantánea de Amazon EBS en la Guía del usuario de Amazon EC2.

[EC2.4] Las instancias EC2 detenidas deben eliminarse después de un período de tiempo específico

Requisitos relacionados: NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoría: Identificar - Inventario

Gravedad: media

Tipo de recurso: `AWS::EC2::Instance`

AWS Config regla: `ec2-stopped-instance-days-check` (regla CSPM de Security Hub personalizada)

Tipo de programa: Periódico

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`AllowedDays`	Cantidad de días que se permite que la instancia de EC2 permanezca detenida antes de generar un resultado con errores.	Entero	De `1` a `365`	`30`

Este control comprueba si una instancia de Amazon EC2 ha estado detenida durante más días de lo permitido. Se produce un error en el control si una instancia de EC2 se detiene durante más tiempo que el máximo permitido. A menos que proporcione un valor de parámetro personalizado para el período de tiempo máximo permitido, el CSPM de Security Hub utiliza un valor predeterminado de 30 días.

Cuando una instancia de EC2 no se ha ejecutado durante un periodo significativo, se crea un riesgo de seguridad porque la instancia no se mantiene de manera activa (se analiza, se le aplican parches o se actualiza). Si se lanza más adelante, la falta de un mantenimiento adecuado podría provocar problemas inesperados en su AWS entorno. Para mantener segura una instancia de EC2 a lo largo del tiempo en un estado inactivo, iníciela de manera periódica para hacer tareas de mantenimiento y deténgala después del mantenimiento. Lo ideal es que se tratara de un proceso automatizado.

> **Note**
>
> Este control evalúa el número de días que una instancia de EC2 ha estado detenida utilizando la marca de tiempo de `StateTransitionReason` la instancia. Cuando `StateTransitionReason` no incluye una marca de tiempo (por ejemplo, cuando una instancia se detiene debido a un error interno), el control utiliza en su lugar la hora de lanzamiento de la instancia. En este caso, si la hora de lanzamiento es anterior al período de tiempo máximo permitido, el control genera un error.

Corrección

Para terminar una instancia de EC2 inactiva, consulte Terminación de una instancia en la Guía del usuario de Amazon EC2.

[EC2.6] El registro de flujo de VPC debe estar habilitado en todas las VPC

Requisitos relacionados: CIS AWS Foundations Benchmark v5.0. 0/3.7, Criterio de referencia sobre los AWS fundamentos de la CEI v1.2. 0/2.9, Punto de referencia sobre los AWS fundamentos de la CEI v1.4. 0/3.9, Criterio de referencia sobre los AWS fundamentos de la CEI v3.0. 0/3.7, NIST.800-53.r5 AC-4 (26),,, NIST.800-53.r5 AU-12 NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-6 (3) NIST.800-53.r5 AU-3, (4), NIST.800-53.r5 AU-6 NIST.800-53.r5 SI-7 (8), NIST.800-171.r2 3.1.20 NIST.800-53.r5 CA-7, NIST.800-171.r2 3.3.1, 3.13.1, NIST.800-171.r2 PCI DSS v3.2. 1/10.3.3, PCI DSS v3.2. 1/10.3.4, PCI DSS v3.2. 1/10.3.5, PCI DSS v3.2. 1/10.3.6

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: `AWS::EC2::VPC`

Regla de AWS Config : `vpc-flow-logs-enabled`

Tipo de programa: Periódico

Parámetros:

- `trafficType`: `REJECT` (no personalizable)

Este control comprueba si se encuentran los registros de flujo de Amazon VPC y si están habilitados para VPC. El tipo de tráfico se ha establecido como `Reject`. El control lanza error si los registros de flujo de VPC no están habilitados para las VPC de su cuenta.

> **Note**
>
> Este control no comprueba si los registros de flujo de Amazon VPC están habilitados a través de Amazon Security Lake para la Cuenta de AWS.

Con la característica de VPC Flow Logs, puede utilizar los registros de flujo de la VPC para capturar información sobre el tráfico de direcciones IP entrante y saliente de las interfaces de red de su VPC. Tras crear un registro de flujo, puede ver y recuperar sus datos en los CloudWatch registros. Para reducir los costos, también puede enviar los registros de flujo a Amazon S3.

Security Hub (CSPM) recomienda habilitar el registro de flujo para los paquetes rechazados en las VPC. Los registros de flujo proporcionan visibilidad del tráfico de red que atraviesa la VPC y pueden detectar tráfico anómalo o brindar información durante los flujos de trabajo de seguridad.

De forma predeterminada, el registro incluye valores para los distintos componentes del flujo de dirección IP, incluido el origen, el destino y el protocolo. Para obtener más información y descripciones de los campos de registro, consulte Registros de flujo de VPC en la Guía del usuario de Amazon VPC.

Corrección

Para crear un registro de flujo de VPC, consulte Crear un registro de flujo en la Guía del usuario de Amazon VPC. Tras abrir la consola de Amazon VPC, elija Sus VPC. En Filtro, elija Rechazar o Todos.

[EC2.7] El cifrado predeterminado de EBS debe estar habilitado

Requisitos relacionados: CIS AWS Foundations Benchmark v5.0. 0/5.1.1, Punto de referencia sobre los AWS fundamentos de la CEI v1.4. 0/2.2.1, Criterio de referencia sobre los AWS fundamentos de la CEI v3.0. 0/2.2.1, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28 (1) NIST.800-53.r5 SC-28, (10), NIST.800-53.r5 SC-7 (6) NIST.800-53.r5 SI-7

Categoría: Proteger > Protección de datos > Cifrado de datos en reposo

Gravedad: media

Tipo de recurso: `AWS::::Account`

Regla de AWS Config : `ec2-ebs-encryption-by-default`

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si el cifrado a nivel de cuenta está habilitado de forma predeterminada para los volúmenes de Amazon Elastic Block Store (Amazon EBS). El control falla si el cifrado a nivel de cuenta no está habilitado para los volúmenes de EBS.

Cuando el cifrado está activado en su cuenta, los volúmenes de Amazon EBS y las copias instantáneas se cifran en reposo. Esto agrega una capa adicional de protección para sus datos. Para obtener más información, consulte Cifrado de forma predeterminada en la Guía del usuario de Amazon EC2.

Corrección

Para configurar el cifrado predeterminado para los volúmenes de Amazon EBS, consulte Cifrado predeterminado en la Guía del usuario de Amazon EC2.

[EC2.8] Las instancias EC2 deben utilizar la versión 2 del servicio de metadatos de instancia (IMDSv2)

Requisitos relacionados: CIS AWS Foundations Benchmark v5.0. 0/5.7, Criterio de referencia sobre los AWS fundamentos de la CEI v3.0. 0/5.6, NIST.800-53.r5 AC-3 (15) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-6, PCI DSS v4.0. 1/2.2.6

Categoría: Proteger > Seguridad de red

Gravedad: alta

Tipo de recurso: `AWS::EC2::Instance`

Regla de AWS Config : `ec2-imdsv2-check`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si la versión de metadatos de la instancia de EC2 está configurada con la versión 2 del servicio de metadatos de la instancia (IMDSv2). El control aprueba si `HttpTokens` está configurado como obligatorio para IMDSv2. El control tiene errores si `HttpTokens` está configurado como `optional`,

Utiliza metadatos de instancia para configurar o administrar la instancia en ejecución. El IMDS proporciona acceso a credenciales temporales que se rotan con frecuencia. Estas credenciales eliminan la necesidad de codificar o distribuir credenciales confidenciales a las instancias de forma manual o programática. El IMDS se conecta localmente a todas las instancias de EC2. Se ejecuta en una dirección IP de «enlace local» de 169.254.169.254. Solo el software que se ejecuta en la instancia puede acceder a esta dirección IP.

La versión 2 del IMDS añade nuevas protecciones para los siguientes tipos de vulnerabilidades. Estas vulnerabilidades podrían utilizarse para intentar acceder al IMDS.

- Abra firewalls de aplicaciones de sitios web
- Abra proxies inversos
- Server-side vulnerabilidades de solicitud de falsificación (SSRF)
- Firewalls de capa 3 abiertos y traducción de direcciones de red (NAT)

Security Hub (CSPM) recomienda configurar las instancias EC2 con IMDSv2.

Corrección

Para configurar instancias de EC2 con IMDSv2, consulte Ruta recomendada para solicitar IMDSv2 en la Guía del usuario de Amazon EC2.

[EC2.9] Las instancias de Amazon EC2 no deben tener una dirección IPv4 pública

Requisitos relacionados: NIST.800-53.r5 AC-21 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7 (11) NIST.800-53.r5 SC-7, (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9)

Categoría: Proteger > Configuración de red segura > Recursos no accesibles públicamente

Gravedad: alta

Tipo de recurso: `AWS::EC2::Instance`

Regla de AWS Config : `ec2-instance-no-public-ip`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si las instancias EC2 tienen una dirección IP pública. El control falla si el campo `publicIp` está presente en el elemento de configuración de instancia EC2. Este control se aplica únicamente a las direcciones IPv4.

Una dirección IPv4 pública es una dirección IP a la que se puede tener acceso desde Internet. Si lanza la instancia con una dirección IP pública, se puede obtener acceso a la instancia de EC2 desde Internet. Una dirección IPv4 privada es una dirección IP a la que no se puede obtener acceso desde Internet. Puede utilizar direcciones IPv4 privadas para la comunicación entre las instancias EC2 de una misma VPC o en su red privada conectada.

Las direcciones IPv6 son únicas de forma global y, por lo tanto, están disponibles a través de Internet. De forma predeterminada, todas las subredes tienen el atributo de direcciones IPv6 configurado como falso. Para obtener más información sobre IPv6, consulte Direcciones IP en su VPC en la Guía del usuario de Amazon VPC.

Si tiene un caso de uso legítimo para mantener las instancias de EC2 con direcciones IP públicas, puede ocultar los resultados de este control. Para obtener más información sobre las opciones de arquitectura front-end, consulte el blog de AWS arquitectura o la serie de AWS vídeos This Is My Architecture.

Corrección

Utilice una VPC no predeterminada para que no se le asigne a su instancia una dirección IP pública de forma predeterminada.

Cuando se lanza una instancia EC2 en una VPC predeterminada, se le asigna una dirección IP pública. Al lanzar una instancia EC2 en una VPC no predeterminada, la configuración de subred determina si recibe una dirección IP pública. La subred tiene un atributo para determinar si las instancias de EC2 nuevas de la subred reciben una dirección IP pública del grupo de direcciones IPv4 públicas.

Puede desvincular una dirección IP pública asignada de manera automática de su instancia de EC2. Para obtener más información, consulte Direcciones IPv4 públicas y nombres de host DNS externos en la Guía del usuario de Amazon EC2.

[EC2.10] Amazon EC2 debe configurarse para utilizar los puntos de enlace de VPC que se crean para el servicio Amazon EC2

Requisitos relacionados: NIST.800-53.r5 AC-21 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), (21) NIST.800-53.r5 AC-4,,, NIST.800-53.r5 AC-4 (11) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (4), 3.1.3, 3.13.1 NIST.800-171.r2 NIST.800-171.r2

Categoría: Proteger > Configuración de red segura > Acceso privado a la API

Gravedad: media

Tipo de recurso: `AWS::EC2::VPC`

Regla de AWS Config : vpc-endpoint-enabled

Tipo de programa: Periódico

Parámetros:

- `serviceNames`: `ec2` (no personalizable)

Este control comprueba si se ha creado un punto de conexión de servicio para Amazon EC2 para cada VPC. El control falla si una VPC no tiene un punto de conexión de VPC creado para el servicio Amazon EC2.

Este control evalúa los recursos en una sola cuenta. No puede describir los recursos que están fuera de la cuenta. Como el CSPM AWS Config y Security Hub no realizan comprobaciones entre cuentas, verá los `FAILED` resultados de las VPC que se comparten entre cuentas. Security Hub CSPM recomienda suprimir estos `FAILED` hallazgos.

Para mejorar la posición de seguridad de su VPC, puede configurar Amazon EC2 para que utilice un punto de conexión de VPC de interfaz. Los puntos de enlace de la interfaz funcionan con una tecnología que le permite acceder a las operaciones de la API de Amazon EC2 de forma privada. AWS PrivateLink Restringe todo el tráfico de red entre su VPC y Amazon EC2 a la red de Amazon. Dado que los puntos de conexión solo se admiten dentro de la misma región, no se puede crear un punto de conexión entre una VPC y un servicio de otra región. Esto evita las llamadas no deseadas a la API de Amazon EC2 a otras regiones.

Para obtener más información acerca de cómo crear puntos de conexión de VPC para Amazon EC2, consulte Amazon EC2 y puntos de conexión de VPC de interfaz en la Guía del usuario de Amazon EC2.

Corrección

Para crear un punto de conexión de interfaz para Amazon EC2 desde la consola de Amazon VPC, consulte Crear un punto de conexión de VPC en la Guía de AWS PrivateLink . En Nombre del servicio, elija com.amazonaws. ***region***.ec2.

También puede crear y asociar una política de punto de conexión a su punto de conexión de VPC para controlar el acceso a la API de Amazon EC2. Para obtener instrucciones sobre cómo crear una política de punto de conexión de VPC, consulte Creación de una política de punto de conexión en la Guía del usuario de Amazon EC2.

[EC2.12] Deben eliminarse las EIP de Amazon EC2 no utilizadas

Requisitos relacionados: PCI DSS v3.2. 1/24., (1) NIST.800-53.r5 CM-8

Categoría: Proteger - Configuración de red segura

Gravedad: baja

Tipo de recurso: `AWS::EC2::EIP`

Regla de AWS Config : `eip-attached`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si las direcciones IP elásticas (EIP) que están asignadas a una VPC están asociadas a instancias EC2 o a interfaces de red elásticas (ENI) en uso.

Un error en el resultado indica que puede tener EIP de EC2 sin utilizar.

Esto le ayudará a mantener un inventario de activos de EIP preciso en su entorno de datos del titular (CDE).

Corrección

Para lanzar una EIP que no está en uso, consulte Lanzamiento de una dirección IP elástica en la Guía del usuario de Amazon EC2.

[EC2.13] Los grupos de seguridad no deberían permitir la entrada desde la versión 0.0.0. 0/0 o: :/0 al puerto 22

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2. 0/4.1 NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21),, NIST.800-53.r5 SC-7 (11) NIST.800-53.r5 CM-7 NIST.800-53.r5 SC-7, (16), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (5), NIST.800-171.r2 3.1.3, NIST.800-171.r2 3.13.1, PCI DSS v3.2. 1/12.2.1, PCI DSS v3.2. 1/1.3.1, PCI DSS v3.2. 1/2.2.2, PCI DSS v4.0. 1/1.3.1

Categoría: Proteger - Configuración de red segura

Gravedad: alta

Tipo de recurso: `AWS::EC2::SecurityGroup`

Regla de AWS Config : `restricted-ssh`

Tipo de programa: activado por cambios y periódico

Parámetros: ninguno

Este control comprueba si un grupo de seguridad de Amazon EC2 permite la entrada desde 0.0.0. 0/0 o: :/0 al puerto 22. El control falla si el grupo de seguridad permite la entrada desde la versión 0.0.0. 0/0o: :/0 al puerto 22.

Los grupos de seguridad proporcionan filtrado con estado del tráfico de red de entrada y salida a los recursos de AWS . Recomendamos que ningún grupo de seguridad permita el acceso de entrada ilimitado al puerto 22. La eliminación de la conectividad libre a los servicios de la consola a distancia, como SSH, reduce la exposición al riesgo del servidor.

Corrección

Para prohibir la entrada al puerto 22, elimine la regla que permite dicho acceso a cada grupo de seguridad asociado a una VPC. Para obtener instrucciones, consulte Actualización de las reglas de un grupo de seguridad en la Guía del usuario de Amazon EC2. Después de seleccionar un grupo de seguridad en la consola de Amazon EC2, elija Acciones y editar reglas de entrada. Elimine la regla que permite el acceso al puerto 22.

[EC2.14] Los grupos de seguridad no deberían permitir la entrada desde la versión 0.0.0. 0/0 o: :/0 al puerto 3389

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2. 0/44.2, PCI DSS v4.0. 1/13.3.1

Categoría: Proteger - Configuración de red segura

Gravedad: alta

Tipo de recurso: `AWS::EC2::SecurityGroup`

AWS Config regla: **`restricted-common-ports`**(la regla creada es`restricted-rdp`)

Tipo de programa: activado por cambios y periódico

Parámetros: ninguno

Este control comprueba si un grupo de seguridad de Amazon EC2 permite la entrada desde 0.0.0. 0/0 o: :/0 al puerto 3389. El control falla si el grupo de seguridad permite la entrada desde la versión 0.0.0. 0/0o: :/0 al puerto 3389.

Los grupos de seguridad proporcionan filtrado con estado del tráfico de red de entrada y salida a los recursos de AWS . Recomendamos que ningún grupo de seguridad permita el acceso de entrada ilimitado al puerto 3389. La eliminación de la conectividad libre a los servicios de la consola a distancia, como RDP, reduce la exposición al riesgo del servidor.

Corrección

Para prohibir la entrada al puerto 3389, elimine la regla que permite dicho acceso a cada grupo de seguridad asociado a una VPC. Para obtener instrucciones, consulte Actualizar reglas del grupo de seguridad en la Guía del usuario de Amazon VPC. Tras seleccionar un grupo de seguridad en la consola de Amazon VPC, elija Acciones y editar reglas de entrada. Elimine la regla que permite el acceso al puerto 3389.

[EC2.15] Las subredes de Amazon EC2 no deben asignar automáticamente direcciones IP públicas

Requisitos relacionados: NIST.800-53.r5 AC-21 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 AC-4,, (11) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), PCI DSS v4.0. 1/14.4.4

Categoría: Proteger > Seguridad de red

Gravedad: media

Tipo de recurso: `AWS::EC2::Subnet`

Regla de AWS Config : `subnet-auto-assign-public-ip-disabled`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una subred de Amazon Virtual Private Cloud (Amazon VPC) está configurada para asignar automáticamente direcciones IP públicas. El control falla si la subred está configurada para asignar automáticamente direcciones IPv4 o IPv6 públicas.

Las subredes tienen atributos que determinan si las interfaces de red reciben automáticamente las direcciones IPv4 e IPv6 públicas. En el caso de IPv4, este atributo se establece en las subredes predeterminadas y `FALSE` en las subredes no predeterminadas (con la excepción de las subredes no predeterminadas creadas mediante el asistente de lanzamiento de instancias de EC2, donde se establece en). `TRUE` `TRUE` En el caso de IPv6, este atributo se establece en para todas las subredes de forma predeterminada. `FALSE` Cuando estos atributos están habilitados, las instancias lanzadas en la subred reciben automáticamente las direcciones IP correspondientes (IPv4 o IPv6) en su interfaz de red principal.

Corrección

Para configurar una subred para que no asigne direcciones IP públicas, consulte Modificación de los atributos de direccionamiento IP de la subred en la Guía del usuario de Amazon VPC.

[EC2.16] Se deben eliminar las listas de control de acceso a la red no utilizadas

Requisitos relacionados: NIST.800-53.r5 CM-8 (1), NIST.800-171.r2 3.4.7, PCI DSS v4.0. 1/12.2.7

Categoría: Proteger > Seguridad de red

Gravedad: baja

Tipo de recurso: `AWS::EC2::NetworkAcl`

Regla de AWS Config : `vpc-network-acl-unused-check`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si hay alguna lista de control de acceso de la red (ACL de la red) sin utilizar en su nube privada virtual (VPC). El control lanza error si la ACL de la red no está asociada a una subred. El control no genera resultados para una ACL de red predeterminada que no está en uso.

El control comprueba la configuración de elementos del recurso de `AWS::EC2::NetworkAcl` y determina las relaciones de la ACL de la red.

Si la única relación es la VPC de la ACL de la red, el control lanza error.

Si se enumeran otras relaciones, el control pasa.

Corrección

Para obtener instrucciones sobre cómo eliminar una ACL de red no utilizada, consulte Eliminar una ACL de red en la Guía del usuario de Amazon VPC. No puede eliminar la ACL de red predeterminada ni una ACL asociada a subredes.

[EC2.17] Las instancias de Amazon EC2 no deben usar varios ENI

Requisitos relacionados: NIST.800-53.r5 AC-4 (21)

Categoría: Proteger > Seguridad de red

Gravedad: baja

Tipo de recurso: `AWS::EC2::Instance`

Regla de AWS Config : `ec2-instance-multiple-eni-check`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una instancia EC2 utiliza varias interfaces de red elásticas (ENI) o adaptadores de estructura elástica (EFA). Este control se ejecuta si se utiliza un único adaptador de red. El control incluye una lista de parámetros opcional para identificar los ENI permitidos. Este control también falla si una instancia EC2 que pertenece a un clúster de Amazon EKS utiliza más de un ENI. Si sus instancias EC2 necesitan tener varios ENI como parte de un clúster de Amazon EKS, puede suprimir esos resultados de control.

Si hay varios ENI, se pueden crear instancias de doble host, es decir, instancias que tienen varias subredes. Esto puede añadir complejidad a la seguridad de la red e introducir rutas y accesos a la red no deseados.

Corrección

Para desvincular una interfaz de red de una instancia de EC2, consulte Desvinculación de una interfaz de red de una instancia en la Guía del usuario de Amazon EC2.

[EC2.18] Los grupos de seguridad solo deben permitir el tráfico entrante sin restricciones en los puertos autorizados

Requisitos relacionados: NIST.800-53.r5 AC-4 NIST.800-53.r5 AC-4 (21), (11) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (5), NIST.800-171.r2 3.1.3, 3.1.20, NIST.800-171.r2 3.13.1 NIST.800-171.r2

Categoría: Proteger > Configuración de red segura > Configuración de grupos de seguridad

Gravedad: alta

Tipo de recurso: `AWS::EC2::SecurityGroup`

Regla de AWS Config : `vpc-sg-open-only-to-authorized-ports`

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`authorizedTcpPorts`	Lista de puertos TCP autorizados	IntegerList (mínimo de 1 elemento y máximo de 32 elementos)	De 1 a 65535	`[80,443]`
`authorizedUdpPorts`	Lista de puertos UDP autorizados	IntegerList (mínimo de 1 artículo y máximo de 32 artículos)	De 1 a 65535	Sin valor predeterminado

Este control comprueba si un grupo de seguridad de Amazon EC2 permite el tráfico entrante sin restricciones de puertos no autorizados. El estado de control se determina de la siguiente manera:

- Si se utiliza el valor predeterminado para `authorizedTcpPorts`, se producirá un error en el control si el grupo de seguridad permite el tráfico entrante sin restricciones de cualquier puerto que no sea el 80 ni el 443.
- Si proporciona valores personalizados para `authorizedTcpPorts` o `authorizedUdpPorts`, se producirá un error en el control si el grupo de seguridad permite el tráfico entrante sin restricciones de cualquier puerto que no figure en la lista.

Los grupos de seguridad proporcionan filtrado con estado del tráfico de red de entrada y salida a AWS. Las reglas de los grupos de seguridad deben seguir el principio del acceso con menos privilegios. El acceso sin restricciones (dirección IP con sufijo /0) aumenta la posibilidad de actividades maliciosas, como piratería, ataques de denegación de servicio y pérdida de datos. A menos que se permita específicamente un puerto, dicho puerto debería denegar el acceso sin restricciones.

Corrección

Para modificar un grupo de seguridad, consulte Trabajo con grupos de seguridad en la Guía del usuario de Amazon VPC.

[EC2.19] Los grupos de seguridad no deben permitir el acceso irrestricto a los puertos de alto riesgo

Requisitos relacionados: NIST.800-53.r5 AC-4 NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 CA-9 (1), (2) NIST.800-53.r5 CM-2,, NIST.800-53.r5 CM-2 (11) NIST.800-53.r5 CM-7 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (5), NIST.800-171.r2 3.1.3, 3.1.20, NIST.800-171.r2 3.13.1 NIST.800-171.r2

Categoría: Proteger > Acceso restringido a la red

Gravedad: crítica

Tipo de recurso: `AWS::EC2::SecurityGroup`

AWS Config regla: **`restricted-common-ports`**(la regla creada es) `vpc-sg-restricted-common-ports`

Tipo de programa: activado por cambios y periódico

Parámetros: `"blockedPorts": "20,21,22,23,25,110,135,143,445,1433,1434,3000,3306,3389,4333,5000,5432,5500,560` (no personalizables)

Este control comprueba si el tráfico entrante sin restricciones de un grupo de seguridad de Amazon EC2 es accesible para los puertos especificados que se consideran de mayor riesgo. Este control falla si alguna de las reglas de un grupo de seguridad permite la entrada de tráfico desde la versión 0.0.0. 0/0' o ': :/0' a esos puertos.

Los grupos de seguridad proporcionan filtrado con estado del tráfico de red de entrada y salida a los recursos de AWS . Acceso sin restricciones (0.0.0. 0/0) aumenta las posibilidades de que se produzcan actividades maliciosas, como la piratería informática, los ataques de denegación de servicio y la pérdida de datos. Ningún grupo de seguridad debe permitir el acceso de entrada sin restricciones a los siguientes puertos:

- 20, 21 (FTP)
- 22 (SSH)
- 23 (Telnet)
- 25 (SMTP)
- 110 (POP3)
- 135 (RPC)
- 143 (IMAP)
- 445 (CIFS)
- 1433, 1434 (MSSQL)
- 3000 (marcos de desarrollo Node.js web Go y Ruby)
- 3306 (MySQL)
- 3389 (RDP)
- 4333 (ahsp)
- 5000 (marcos de desarrollo web Python)
- 5432 (postgresql)
- 5500 (fcp-addr-srvr1)
- 5601 (OpenSearch paneles de control)
- 8080 (proxy)
- 8088 (puerto HTTP antiguo)
- 8888 (puerto HTTP alternativo)
- 9200 o 9300 () OpenSearch

Corrección

Para eliminar reglas de un grupo de seguridad, consulte Eliminación de reglas de un grupo de seguridad en la Guía del usuario de Amazon EC2.

[EC2.20] Ambos túneles VPN para un AWS Site-to-Site La conexión VPN debería estar activa

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 SC-5 (2) NIST.800-53.r5 SC-36, NIST.800-53.r5 SI-13 (5), NIST.800-171.r2 3.1.13, 3.1.20 NIST.800-171.r2

Categoría: Recuperación > Resiliencia > Alta disponibilidad

Gravedad: media

Tipo de recurso:`AWS::EC2::VPNConnection`

Regla de AWS Config : `vpc-vpn-2-tunnels-up`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Un túnel VPN es un enlace cifrado por el que los datos pueden pasar desde la red del cliente hacia o desde una conexión VPN AWS . AWS Site-to-Site Cada conexión de VPN incluye dos túneles de VPN que puede utilizar simultáneamente para conseguir alta disponibilidad. Asegurarse de que ambos túneles VPN estén activos para una conexión VPN es importante para confirmar una conexión segura y de alta disponibilidad entre una AWS VPC y su red remota.

Este control comprueba que los dos túneles VPN proporcionados por la AWS Site-to-Site VPN estén en estado ACTIVO. El control falla si uno o ambos túneles están en estado INACTIVO.

Corrección

Para modificar las opciones del túnel VPN, consulte Modificación de las opciones del túnel Site-to-Site VPN en la Guía del usuario de la AWS Site-to-Site VPN.

[EC2.21] Las ACL de red no deberían permitir la entrada desde la versión 0.0.0. 0/0 al puerto 22 o al puerto 3389

Requisitos relacionados: CIS AWS Foundations Benchmark v5.0. 0/5.2, Punto de referencia sobre AWS los fundamentos de la CEI v1.4. 0/5.1, Criterio de referencia sobre AWS los fundamentos

de la CEI v3.0. 0/5.1, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 CA-9 (1), (2) NIST.800-53.r5 CM-2,, NIST.800-53.r5 CM-2 (21) NIST.800-53.r5 CM-7 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (5), NIST.800-171.r2 3.1.3, NIST.800-171.r2 3.1.20, NIST.800-171.r2 3.13.1, PCI DSS v4.0. 1/13.3.1

Categoría: Proteger > Configuración de red segura

Gravedad: media

Tipo de recurso:`AWS::EC2::NetworkAcl`

Regla de AWS Config : `nacl-no-unrestricted-ssh-rdp`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una lista de control de acceso a la red (ACL de red) permite el acceso sin restricciones a los puertos TCP predeterminados para el tráfico de SSH/RDP entrada. El control falla si la entrada entrante de la ACL de la red permite un bloque CIDR de origen de 0.0.0. 0/0' o ': :/0' para los puertos TCP 22 o 3389. El control no genera resultados para una ACL de red predeterminada.

El acceso a los puertos de administración remota del servidor, como el puerto 22 (SSH) y el puerto 3389 (RDP), no debe ser de acceso público, ya que esto puede permitir el acceso no deseado a los recursos de la VPC.

Corrección

Para editar las reglas de tráfico de la ACL de red, consulte Uso de las ACL de red en la Guía del usuario de Amazon VPC.

[EC2.22] Deben eliminarse los grupos de seguridad de Amazon EC2 no utilizados

Categoría: Identificar - Inventario

Gravedad: media

Tipo de recurso: `AWS::EC2::NetworkInterface`, `AWS::EC2::SecurityGroup`

Regla de AWS Config : `ec2-security-group-attached-to-eni-periodic`

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si los grupos de seguridad están asociados a instancias de Amazon Elastic Compute Cloud (Amazon EC2) o a una interfaz de red elástica. El control lanza error si el grupo de seguridad no está asociado a una instancia de Amazon EC2 o a una interfaz de red elástica.

> **Important**
>
> El 20 de septiembre de 2023, Security Hub CSPM eliminó este control de las mejores prácticas de seguridad AWS fundamentales y de los estándares NIST SP 800-53 revisión 5. Este control sigue formando parte del estándar de administración de servicios. AWS Control Tower Este control genera un resultado aprobado si los grupos de seguridad están asociados a instancias de EC2 o a una interfaz de red elástica. Sin embargo, en algunos casos de uso, los grupos de seguridad independientes no representan un riesgo para la seguridad. Puede usar otros controles de EC2, como,, y EC2.2 EC2.13 EC2.14 EC2.18, para monitorear sus grupos de seguridad EC2.19.

Corrección

Para crear, asignar y eliminar grupos de seguridad, consulte Grupos de seguridad para las instancias de EC2 en la Guía del usuario de Amazon EC2.

[EC2.23] Amazon EC2 Transit Gateways no debe aceptar automáticamente las solicitudes de adjuntos de VPC

Requisitos relacionados: NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Categoría: Proteger - Configuración de red segura

Gravedad: alta

Tipo de recurso:`AWS::EC2::TransitGateway`

Regla de AWS Config : `ec2-transit-gateway-auto-vpc-attach-disabled`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si las pasarelas de tránsito de EC2 aceptan automáticamente adjuntos de VPC compartidos. Este control falla en el caso de una pasarela de tránsito que acepta automáticamente las solicitudes de adjuntos de VPC compartidas.

Al activar `AutoAcceptSharedAttachments` se configura una pasarela de tránsito para que acepte automáticamente cualquier solicitud de adjunto de VPC multicuenta sin verificar la solicitud o la cuenta desde la que se origina el archivo adjunto. Para seguir las prácticas recomendadas de autorización y autenticación, recomendamos desactivar esta característica para garantizar que solo se acepten las solicitudes de adjuntos de VPC autorizadas.

Corrección

Para modificar una puerta de enlace de tránsito, consulte Modificación de una puerta de enlace de tránsito en la Guía para desarrolladores de Amazon VPC.

[EC2.24] No se deben utilizar los tipos de instancias paravirtuales de Amazon EC2

Requisitos relacionados: NIST.800-53.r5 CM-2 (NIST.800-53.r5 CM-22)

Categoría: Identificar > Administración de vulnerabilidades, parches y versiones

Gravedad: media

Tipo de recurso:`AWS::EC2::Instance`

Regla de AWS Config : `ec2-paravirtual-instance-check`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si el tipo de virtualización de una instancia EC2 es paravirtual. El control falla si `virtualizationType` de la instancia EC2 está configurada como `paravirtual`.

Las Imágenes de máquina de Amazon (AMI) de Linux utilizan uno de los dos tipos de virtualización: paravirtual (PV) o máquina virtual de hardware (HVM). Las principales diferencias entre las AMI PV y HVM son el modo de arranque y si admiten extensiones de hardware especiales (CPU, red y almacenamiento) para mejorar su rendimiento.

Antes, el rendimiento de los invitados PV era mejor que el de los invitados HVM en muchos casos, pero esto ya no es así debido a las mejoras de la virtualización HVM y a la disponibilidad de

controladores PV para AMI HVM. Para obtener más información, consulte Tipos de virtualización de la AMI de Linux en la Guía del usuario de Amazon EC2.

Corrección

Para actualizar una instancia de EC2 a un nuevo tipo de instancia, consulte Cambio del tipo de instancia en la Guía del usuario de Amazon EC2.

[EC2.25] Las plantillas de lanzamiento de Amazon EC2 no deben asignar direcciones IP públicas a las interfaces de red

Requisitos relacionados: NIST.800-53.r5 AC-21 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 AC-4,, (11) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), PCI DSS v4.0. 1/14.4.4

Categoría: Proteger > Configuración de red segura > Recursos no accesibles públicamente

Gravedad: alta

Tipo de recurso:`AWS::EC2::LaunchTemplate`

Regla de AWS Config : `ec2-launch-template-public-ip-disabled`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si las plantillas de lanzamiento de Amazon EC2 están configuradas para asignar direcciones IP públicas a las interfaces de red en el momento del lanzamiento. El control falla si una plantilla de lanzamiento de EC2 está configurada para asignar una dirección IP pública a las interfaces de red o si hay al menos una interfaz de red que tiene una dirección IP pública.

Una dirección IP pública es una dirección a la que se puede tener acceso desde Internet. Si configura las interfaces de red con una dirección IP pública, es posible que se pueda acceder a los recursos asociados a esas interfaces de red desde Internet. Los recursos de EC2 no deberían ser de acceso público, ya que esto podría permitir el acceso no deseado a sus cargas de trabajo.

Corrección

Para actualizar una plantilla de lanzamiento de EC2, consulte Cambiar la configuración predeterminada de la interfaz de red en la Guía del usuario de Amazon EC2 Auto Scaling.

[EC2.28] Los volúmenes de EBS deben estar cubiertos por un plan de respaldo

Categoría: Recuperación > Resiliencia > Respaldos habilitados

Requisitos relacionados: NIST.800-53.r5 CP-10 NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6 (1), NIST.800-53.r5 CP-6 (2) NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2) NIST.800-53.r5 SI-12, NIST.800-53.r5 SI-13 (5)

Gravedad: baja

Tipo de recurso: `AWS::EC2::Volume`

AWS Config regla: **`ebs-resources-protected-by-backup-plan`**

Tipo de programa: Periódico

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`backupVaultLockCheck`	El control genera un resultado `PASSED` si el parámetro está establecido en `true` y el recurso utiliza el Bloqueo de almacenes de AWS Backup .	Booleano	`true` o `false`	Sin valor predeterminado

Este control evalúa si un volumen de Amazon EBS en el estado `in-use` está cubierto por un plan de copias de seguridad. Se produce un error en el control si un volumen de Amazon EBS no está cubierto por un plan de copias de seguridad. Si establece el `backupVaultLockCheck` parámetro en un valor igual `atrue`, el control solo se activará si el volumen de EBS está guardado en un AWS Backup almacén cerrado con llave.

Las copias de seguridad le ayudan a recuperarse más rápidamente de un incidente de seguridad. También refuerzan la resiliencia de sus sistemas. La inclusión de los volúmenes de Amazon EBS

en un plan de copias de seguridad le ayuda a proteger sus datos contra pérdidas o eliminaciones involuntarias.

Corrección

Para añadir un volumen de Amazon EBS a un plan de AWS Backup respaldo, consulte Asignación de recursos a un plan de respaldo en la Guía para AWS Backup desarrolladores.

[EC2.33] Los archivos adjuntos de la pasarela de tránsito EC2 deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::EC2::TransitGatewayAttachment`

AWS Config regla: `tagged-ec2-transitgatewayattachment` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si una conexión de puerta de enlace de tránsito de Amazon EC2 tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza error si la conexión de puerta de enlace de tránsito no tiene ninguna clave de etiqueta o si no

tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si la conexión de puerta de enlace de tránsito no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas AWS Billing. Para conocer más prácticas recomendadas para el etiquetado, consulte Etiquetado de recursos de AWS en la Referencia general de AWS.

Corrección

Para agregar etiquetas a una conexión de puerta de enlace de tránsito de EC2, consulte Etiquetado de recursos de Amazon EC2 en la Guía del usuario de Amazon EC2.

[EC2.34] Las tablas de rutas de la pasarela de tránsito EC2 deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::EC2::TransitGatewayRouteTable`

AWS Config regla: `tagged-ec2-transitgatewayroutetable` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si una tabla de enrutamiento de una puerta de enlace de tránsito de Amazon EC2 tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza error si la tabla de enrutamiento de la puerta de enlace de tránsito no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si la tabla de enrutamiento de la puerta de enlace de tránsito no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas AWS Billing. Para conocer más prácticas recomendadas para el etiquetado, consulte Etiquetado de recursos de AWS en la Referencia general de AWS.

Corrección

Para agregar etiquetas a una tabla de enrutamiento de una puerta de enlace de tránsito de EC2, consulte Etiquetado de recursos de Amazon EC2 en la Guía del usuario de Amazon EC2.

[EC2.35] Las interfaces de red EC2 deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::EC2::NetworkInterface`

AWS Config regla: `tagged-ec2-networkinterface` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si una interfaz de red de Amazon EC2 tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza error si la interfaz de red no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si la interfaz de red no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas AWS Billing. Para conocer más prácticas recomendadas para el etiquetado, consulte Etiquetado de recursos de AWS en la Referencia general de AWS.

Corrección

Para agregar etiquetas a una interfaz de red de EC2, consulte Etiquetado de recursos de Amazon EC2 en la Guía del usuario de Amazon EC2.

[EC2.36] Las pasarelas de clientes de EC2 deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::EC2::CustomerGateway`

AWS Config regla: `tagged-ec2-customergateway` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si una puerta de enlace de cliente de Amazon EC2 tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza error si la puerta de enlace de cliente no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si la puerta de enlace de cliente no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan

operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas AWS Billing. Para conocer más prácticas recomendadas para el etiquetado, consulte Etiquetado de recursos de AWS en la Referencia general de AWS.

Corrección

Para agregar etiquetas a una puerta de enlace de cliente de EC2, consulte Etiquetado de recursos de Amazon EC2 en la Guía del usuario de Amazon EC2.

[EC2.37] Las direcciones IP elásticas de EC2 deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::EC2::EIP`

AWS Config regla: `tagged-ec2-eip` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que	Sin valor predeterminado

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
	recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.		cumplan los requisitos de AWS.	

Este control comprueba si una dirección IP elástica de Amazon EC2 tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza error si la dirección IP elástica no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si la dirección IP elástica no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas AWS Billing. Para conocer más prácticas recomendadas para el etiquetado, consulte Etiquetado de recursos de AWS en la Referencia general de AWS.

Corrección

Para agregar etiquetas a una dirección IP elástica de EC2, consulte Etiquetado de recursos de Amazon EC2 en la Guía del usuario de Amazon EC2.

[EC2.38] Las instancias EC2 deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::EC2::Instance`

AWS Config regla: `tagged-ec2-instance` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si una instancia de Amazon EC2 tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza error si la instancia no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si la instancia no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas AWS Billing. Para conocer más prácticas recomendadas para el etiquetado, consulte Etiquetado de recursos de AWS en la Referencia general de AWS.

Corrección

Para agregar etiquetas a una instancia de EC2, consulte Etiquetado de recursos de Amazon EC2 en la Guía del usuario de Amazon EC2.

[EC2.39] Las pasarelas de Internet EC2 deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::EC2::InternetGateway`

AWS Config regla: `tagged-ec2-internetgateway` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si una puerta de enlace de Internet de Amazon EC2 tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza error si la puerta de enlace de Internet no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si la puerta de enlace de Internet no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas AWS Billing. Para conocer más prácticas recomendadas para el etiquetado, consulte Etiquetado de recursos de AWS en la Referencia general de AWS.

Corrección

Para agregar etiquetas a una puerta de enlace de Internet de EC2, consulte Etiquetado de recursos de Amazon EC2 en la Guía del usuario de Amazon EC2.

[EC2.40] Las pasarelas NAT EC2 deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::EC2::NatGateway`

AWS Config regla: `tagged-ec2-natgateway` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si una puerta de enlace de traducción de direcciones de red (NAT) de Amazon EC2 tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza error si la puerta de enlace de NAT no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si la puerta de enlace de NAT no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas AWS Billing. Para conocer más prácticas recomendadas para el etiquetado, consulte Etiquetado de recursos de AWS en la Referencia general de AWS.

Corrección

Para agregar etiquetas a una puerta de enlace de NAT de EC2, consulte Etiquetado de recursos de Amazon EC2 en la Guía del usuario de Amazon EC2.

[EC2.41] Las ACL de la red EC2 deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::EC2::NetworkAcl`

AWS Config regla: `tagged-ec2-networkacl` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si una lista de control de acceso de la red (ACL de la red) de Amazon EC2 tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza error si la ACL de la red no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si la ACL de la red no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan

operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas AWS Billing. Para conocer más prácticas recomendadas para el etiquetado, consulte Etiquetado de recursos de AWS en la Referencia general de AWS.

Corrección

Para agregar etiquetas a una ACL de red de EC2, consulte Etiquetado de recursos de Amazon EC2 en la Guía del usuario de Amazon EC2.

[EC2.42] Las tablas de rutas de EC2 deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::EC2::RouteTable`

AWS Config regla: `tagged-ec2-routetable` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que	Sin valor predeterminado

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
	recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.		cumplan los requisitos de AWS.	

Este control comprueba si una tabla de enrutamiento de Amazon EC2 tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza error si la tabla de enrutamiento no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si la tabla de enrutamiento no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas AWS Billing. Para conocer más prácticas recomendadas para el etiquetado, consulte Etiquetado de recursos de AWS en la Referencia general de AWS.

Corrección

Para agregar etiquetas a una tabla de enrutamiento de EC2, consulte Etiquetado de recursos de Amazon EC2 en la Guía del usuario de Amazon EC2.

[EC2.43] Los grupos de seguridad de EC2 deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::EC2::SecurityGroup`

AWS Config regla: `tagged-ec2-securitygroup` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si un grupo de seguridad de Amazon EC2 tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza error si el grupo de seguridad no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si el grupo de seguridad no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas AWS Billing. Para conocer más prácticas recomendadas para el etiquetado, consulte Etiquetado de recursos de AWS en la Referencia general de AWS.

Corrección

Para agregar etiquetas a un grupo de seguridad de EC2, consulte Etiquetado de recursos de Amazon EC2 en la Guía del usuario de Amazon EC2.

[EC2.44] Las subredes EC2 deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::EC2::Subnet`

AWS Config regla: `tagged-ec2-subnet` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si una subred de Amazon EC2 tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza error si la subred no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si la subred no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre

ellas AWS Billing. Para conocer más prácticas recomendadas para el etiquetado, consulte Etiquetado de recursos de AWS en la Referencia general de AWS.

Corrección

Para agregar etiquetas a una subred de EC2, consulte Etiquetado de recursos de Amazon EC2 en la Guía del usuario de Amazon EC2.

[EC2.45] Los volúmenes EC2 deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::EC2::Volume`

AWS Config regla: `tagged-ec2-volume` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si un volumen de Amazon EC2 tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza error si el volumen no tiene ninguna

clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si el volumen no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas AWS Billing. Para conocer más prácticas recomendadas para el etiquetado, consulte Etiquetado de recursos de AWS en la Referencia general de AWS.

Corrección

Para agregar etiquetas a un volumen de EC2, consulte Etiquetado de recursos de Amazon EC2 en la Guía del usuario de Amazon EC2.

[EC2.46] Las Amazon VPC deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::EC2::VPC`

AWS Config regla: `tagged-ec2-vpc` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si una Amazon Virtual Private Cloud (Amazon VPC) tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza error si la Amazon VPC no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si la Amazon VPC no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas AWS Billing. Para conocer más prácticas recomendadas para el etiquetado, consulte Etiquetado de recursos de AWS en la Referencia general de AWS.

Corrección

Para agregar etiquetas a una VPC, consulte Etiquetado de recursos de Amazon EC2 en la Guía del usuario de Amazon EC2.

[EC2.47] Los servicios de punto final de Amazon VPC deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::EC2::VPCEndpointService`

AWS Config regla: `tagged-ec2-vpcendpointservice` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si un servicio de puntos de conexión de Amazon VPC tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza error si el servicio de punto de conexión no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si el servicio de punto de conexión no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas AWS Billing. Para conocer más prácticas recomendadas para el etiquetado, consulte Etiquetado de recursos de AWS en la Referencia general de AWS.

Corrección

Para agregar etiquetas a un servicio de punto de conexión de Amazon VPC, consulte Administración de etiquetas en la sección Configuración de un servicio de punto de conexión de la Guía AWS PrivateLink .

[EC2.48] Los registros de flujo de Amazon VPC deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::EC2::FlowLog`

AWS Config regla: `tagged-ec2-flowlog` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si un registro de flujo de Amazon VPC tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza error si el registro de flujo no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si el registro de flujo no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan

operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas AWS Billing. Para conocer más prácticas recomendadas para el etiquetado, consulte Etiquetado de recursos de AWS en la Referencia general de AWS.

Corrección

Para agregar etiquetas a un registro de flujo de Amazon VPC, consulte Etiquetado de un registro de flujo en la Guía del usuario de Amazon VPC.

[EC2.49] Las conexiones de emparejamiento de Amazon VPC deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::EC2::VPCPeeringConnection`

AWS Config regla: `tagged-ec2-vpcpeeringconnection` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que	Sin valor predeterminado

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
	recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.		cumplan los requisitos de AWS.	

Este control comprueba si una conexión de emparejamiento de Amazon VPC tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza error si la conexión de emparejamiento no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si la conexión de emparejamiento no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas AWS Billing. Para conocer más prácticas recomendadas para el etiquetado, consulte Etiquetado de recursos de AWS en la Referencia general de AWS.

Corrección

Para agregar etiquetas a una conexión de emparejamiento de Amazon VPC, consulte Etiquetado de recursos de Amazon EC2 en la Guía del usuario de Amazon EC2.

[EC2.50] Las pasarelas VPN de EC2 deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::EC2::VPNGateway`

AWS Config regla: `tagged-ec2-vpngateway` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si una puerta de enlace VPN de Amazon EC2 tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza error si la puerta de enlace VPN no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si la puerta de enlace VPN no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas AWS Billing. Para conocer más prácticas recomendadas para el etiquetado, consulte Etiquetado de recursos de AWS en la Referencia general de AWS.

Corrección

Para agregar etiquetas a una puerta de enlace VPN de EC2, consulte Etiquetado de recursos de Amazon EC2 en la Guía del usuario de Amazon EC2.

[EC2.51] Los puntos finales EC2 Client VPN deben tener habilitado el registro de conexiones de clientes

Requisitos relacionados: NIST.800-53.r5 AC-2 (12), NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9),,, NIST.800-53.r5 AU-10, (3) NIST.800-53.r5 AU-12 NIST.800-53.r5 AU-2 NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 AU-6 (7), (7), NIST.800-53.r5 AU-9 (9) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (8), NIST.800-53.r5 SI-3 (20), NIST.800-53.r5 SI-4 (8) NIST.800-53.r5 SI-4, NIST.800-171.r2 3.1.12, NIST.800-53.r5 SI-7 3.1.20, PCI DSS NIST.800-171.r2 v4.0. 1/102.2.1

Categoría: Identificar - Registro

Gravedad: baja

Tipo de recurso: `AWS::EC2::ClientVpnEndpoint`

AWS Config regla: `ec2-client-vpn-connection-log-enabled`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un AWS Client VPN punto final tiene habilitado el registro de conexiones de clientes. Se produce un error en el control si el punto de conexión no tiene habilitado el registro de conexiones de clientes.

Los puntos de conexión de Client VPN permiten a los clientes remotos conectarse de manera segura a los recursos de una nube privada virtual (VPC) en AWS. Los registros de conexión permiten hacer un seguimiento de la actividad de los usuarios en el punto de conexión de la VPN y proporcionan visibilidad. Cuando habilita el registro de conexión, puede especificar el nombre de una secuencia de registros en el grupo de registros. Si no se especifica ningún flujo de registros, el servicio Client VPN crea uno automáticamente.

Corrección

Para habilitar el registro de conexión, consulte Habilitación del registro de conexión en un punto de conexión de Client VPN existente en la Guía del administrador de AWS Client VPN .

[EC2.52] Las pasarelas de tránsito EC2 deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::EC2::TransitGateway`

AWS Config regla: `tagged-ec2-transitgateway` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	`No default value`

Este control comprueba si una puerta de enlace de tránsito de Amazon EC2 tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza error si la puerta de enlace de tránsito no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si la puerta de enlace de tránsito no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas AWS Billing. Para conocer más prácticas recomendadas para el etiquetado, consulte Etiquetado de recursos de AWS en la Referencia general de AWS.

Corrección

Para agregar etiquetas a una puerta de enlace de tránsito de EC2, consulte Etiquetado de recursos de Amazon EC2 en la Guía del usuario de Amazon EC2.

[EC2.53] Los grupos de seguridad de EC2 no deberían permitir la entrada desde la versión 0.0.0. 0/0 a los puertos de administración remota del servidor

Requisitos relacionados: CIS AWS Foundations Benchmark v5.0. 0/5.3, Criterio de referencia sobre AWS los fundamentos de la CEI v3.0. 0/5.2, PCI DSS v4.0. 1/13.3.1

Categoría: Proteger > Configuración de red segura > Configuración de grupos de seguridad

Gravedad: alta

Tipo de recurso: `AWS::EC2::SecurityGroup`

Regla de AWS Config : `vpc-sg-port-restriction-check`

Tipo de programa: Periódico

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`ipType`	La versión de IP	Cadena	No personalizable	`IPv4`

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`restrictPorts`	Lista de puertos que deben rechazar el tráfico de entrada	IntegerList	No personalizable	`22,3389`

Este control comprueba si un grupo de seguridad de Amazon EC2 permite la entrada desde 0.0.0. 0/0 a los puertos de administración remota de servidores (puertos 22 y 3389). El control falla si el grupo de seguridad permite la entrada desde la versión 0.0.0. 0/0 al puerto 22 o 3389.

Los grupos de seguridad proporcionan filtrado con estado del tráfico de red de entrada y salida a los recursos de AWS . Se recomienda que ningún grupo de seguridad permita el acceso sin restricciones a los puertos de administración de servidores remotos, como SSH al puerto 22 y RDP al puerto 3389, mediante los protocolos TDP (6), UDP (17) o ALL (-1). Si se permite el acceso público a estos puertos, crece la superficie expuesta a ataques de los recursos y el riesgo de que los recursos se vean comprometidos.

Corrección

Si desea actualizar una regla de un grupo de seguridad de EC2 para prohibir el tráfico de entrada a los puertos especificados, consulte Actualización de las reglas de un grupo de seguridad en la Guía del usuario de Amazon EC2. Después de seleccionar un grupo de seguridad en la consola de Amazon EC2, elija Acciones y editar reglas de entrada. Elimine la regla que permite el acceso a los puertos 22 o 3389.

[EC2.54] Los grupos de seguridad de EC2 no deberían permitir la entrada desde: :/0 a los puertos de administración remota del servidor

Requisitos relacionados: CIS AWS Foundations Benchmark v5.0. 0/5.4, Criterio de referencia sobre los AWS fundamentos de la CEI v3.0. 0/5.3, PCI DSS v4.0. 1/13.3.1

Categoría: Proteger > Configuración de red segura > Configuración de grupos de seguridad

Gravedad: alta

Tipo de recurso: `AWS::EC2::SecurityGroup`

Regla de AWS Config : `vpc-sg-port-restriction-check`

Tipo de programa: Periódico

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`ipType`	La versión de IP	Cadena	No personalizable	`IPv6`
`restrictPorts`	Lista de puertos que deben rechazar el tráfico de entrada	IntegerList	No personalizable	`22,3389`

Este control comprueba si un grupo de seguridad de Amazon EC2 permite la entrada de ::/0 a puertos de administración de servidores remotos (puertos 22 y 3389). El control lanza error si el grupo de seguridad permite la entrada de ::/0 o a los puertos 22 o 3389.

Los grupos de seguridad proporcionan filtrado con estado del tráfico de red de entrada y salida a los recursos de AWS . Se recomienda que ningún grupo de seguridad permita el acceso sin restricciones a los puertos de administración de servidores remotos, como SSH al puerto 22 y RDP al puerto 3389, mediante los protocolos TDP (6), UDP (17) o ALL (-1). Si se permite el acceso público a estos puertos, crece la superficie expuesta a ataques de los recursos y el riesgo de que los recursos se vean comprometidos.

Corrección

Si desea actualizar una regla de un grupo de seguridad de EC2 para prohibir el tráfico de entrada a los puertos especificados, consulte Actualización de las reglas de un grupo de seguridad en la Guía del usuario de Amazon EC2. Después de seleccionar un grupo de seguridad en la consola de Amazon EC2, elija Acciones y editar reglas de entrada. Elimine la regla que permite el acceso a los puertos 22 o 3389.

[EC2.55] Las VPC deben configurarse con un punto final de interfaz para la API de ECR

Requisitos relacionados: NIST.800-53.r5 AC-21 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7 (11) NIST.800-53.r5 SC-7, (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4) NIST.800-53.r5 SC-7

Categoría: Proteger - Administración de acceso seguro > Control de acceso

Gravedad: media

Tipo de recurso: `AWS::EC2::VPC`, `AWS::EC2::VPCEndpoint`

Regla de AWS Config : vpc-endpoint-enabled

Tipo de programa: Periódico

Parámetros:

Parámetro	Obligatorio	Description (Descripción)	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`serviceNames`	Obligatorio	El nombre del servicio que el control evalúa	Cadena	No personalizable	`ecr.api`
`vpcIds`	Opcional	Comma-separated lista de ID de Amazon VPC para puntos de enlace de VPC. Si se	StringList	Personalización con uno o más ID de VPC	Sin valor predeterminado

Parámetro	Obligatorio	Description (Descripción)	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
		proporciona, el control falla si los servicios especificados en el parámetro `serviceName` no tienen uno de estos puntos de conexión de VPC.			

Este control comprueba si una nube privada virtual (VPC) que administra tiene un punto de conexión de interfaz de VPC para la API de Amazon ECR. El control falla si la VPC no tiene un punto de conexión de VPC de interfaz para la API de ECR. Este control evalúa recursos en una única cuenta.

AWS PrivateLink permite a los clientes acceder a los servicios alojados AWS en ellos de una forma escalable y de alta disponibilidad, manteniendo todo el tráfico de la red dentro de la red. AWS Los usuarios del servicio pueden acceder de forma privada a los servicios con tecnología PrivateLink desde su VPC o desde sus instalaciones, sin utilizar direcciones IP públicas y sin necesidad de que el tráfico atraviese Internet.

Corrección

Para configurar un punto de enlace de VPC, consulte Acceder y Servicio de AWS utilizar un punto de enlace de VPC de interfaz en la Guía.AWS PrivateLink

[EC2.56] Las VPC deben configurarse con un punto final de interfaz para Docker Registry

Requisitos relacionados: NIST.800-53.r5 AC-21 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7 (11) NIST.800-53.r5 SC-7, (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4) NIST.800-53.r5 SC-7

Categoría: Proteger - Administración de acceso seguro > Control de acceso

Gravedad: media

Tipo de recurso: `AWS::EC2::VPC`, `AWS::EC2::VPCEndpoint`

Regla de AWS Config : vpc-endpoint-enabled

Tipo de programa: Periódico

Parámetros:

Parámetro	Obligatorio	Description (Descripción)	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`serviceNames`	Obligatorio	El nombre del servicio que el control evalúa	Cadena	No personalizable	`ecr.dkr`
`vpcIds`	Opcional	Comma-separated lista de ID de Amazon VPC para puntos de enlace de	StringList	Personalización con uno o más ID de VPC	Sin valor predeterminado

Parámetro	Obligatorio	Description (Descripción)	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
		VPC. Si se proporciona, el control falla si los servicios especificados en el parámetro `serviceName` no tienen uno de estos puntos de conexión de VPC.			

Este control comprueba si una nube privada virtual (VPC) que administra tiene un punto de conexión de VPC de interfaz para el registro de Docker. El control falla si la VPC no tiene un punto de conexión de VPC de interfaz para el registro de Docker. Este control evalúa recursos en una única cuenta.

AWS PrivateLink permite a los clientes acceder a los servicios alojados AWS en ellos de una forma escalable y de alta disponibilidad, manteniendo todo el tráfico de la red dentro de la red. AWS Los usuarios del servicio pueden acceder de forma privada a los servicios con tecnología PrivateLink desde su VPC o desde sus instalaciones, sin utilizar direcciones IP públicas y sin necesidad de que el tráfico atraviese Internet.

Corrección

Para configurar un punto de enlace de VPC, consulte Acceder y Servicio de AWS utilizar un punto de enlace de VPC de interfaz en la Guía.AWS PrivateLink

[EC2.57] Las VPC deben configurarse con un punto final de interfaz para Systems Manager

Requisitos relacionados: NIST.800-53.r5 AC-21 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7 (11) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4)

Categoría: Proteger - Administración de acceso seguro > Control de acceso

Gravedad: media

Tipo de recurso: `AWS::EC2::VPC`, `AWS::EC2::VPCEndpoint`

Regla de AWS Config : vpc-endpoint-enabled

Tipo de programa: Periódico

Parámetros:

Parámetro	Obligatorio	Description (Descripción)	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`serviceNames`	Obligatorio	El nombre del servicio que el control evalúa	Cadena	No personalizable	`ssm`
`vpcIds`	Opcional	Comma-separated lista de ID de Amazon	StringList	Personalización con uno o más ID de VPC	Sin valor predeterminado

Parámetro	Obligatorio	Description (Descripción)	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
		VPC para puntos de enlace de VPC. Si se proporciona, el control falla si los servicios especificados en el parámetro `serviceName` no tienen uno de estos puntos de conexión de VPC.			

Este control comprueba si una nube privada virtual (VPC) que administra tiene un punto de conexión de VPC de interfaz para AWS Systems Manager. El control falla si la VPC no tiene un punto de conexión de VPC de interfaz para Systems Manager. Este control evalúa recursos en una única cuenta.

AWS PrivateLink permite a los clientes acceder a los servicios alojados AWS en ellos de una forma escalable y de alta disponibilidad, manteniendo todo el tráfico de la red dentro de la red. AWS Los usuarios del servicio pueden acceder de forma privada a los servicios con tecnología PrivateLink desde su VPC o desde sus instalaciones, sin utilizar direcciones IP públicas y sin necesidad de que el tráfico atraviese Internet.

Corrección

Para configurar un punto de enlace de VPC, consulte Acceder y Servicio de AWS utilizar un punto de enlace de VPC de interfaz en la Guía.AWS PrivateLink

[EC2.58] Las VPC deben configurarse con un punto final de interfaz para los contactos de Systems Manager Incident Manager

Requisitos relacionados: NIST.800-53.r5 AC-21 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7 (11) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4)

Categoría: Proteger - Administración de acceso seguro > Control de acceso

Gravedad: media

Tipo de recurso: `AWS::EC2::VPC`, `AWS::EC2::VPCEndpoint`

Regla de AWS Config : vpc-endpoint-enabled

Tipo de programa: Periódico

Parámetros:

Parámetro	Obligatorio	Description (Descripción)	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`serviceNames`	Obligatorio	El nombre del servicio que el control evalúa	Cadena	No personalizable	`ssm-contacts`
`vpcIds`	Opcional	Comma-separated lista de ID	StringList	Personalización con	Sin valor predeterminado

Parámetro	Obligatorio	Description (Descripción)	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
		de Amazon VPC para puntos de enlace de VPC. Si se proporciona, el control falla si los servicios especificados en el parámetro `serviceName` no tienen uno de estos puntos de conexión de VPC.		uno o más ID de VPC	

Este control comprueba si una nube privada virtual (VPC) que usted administra tiene un punto final de VPC de interfaz para AWS Systems Manager los contactos de Incident Manager. El control falla si la VPC no tiene un punto de conexión de VPC de interfaz para contactos del administrador de incidentes de Systems Manager. Este control evalúa recursos en una única cuenta.

AWS PrivateLink permite a los clientes acceder a los servicios alojados de una AWS manera escalable y de alta disponibilidad, al tiempo que mantiene todo el tráfico de la red dentro de la AWS red. Los usuarios del servicio pueden acceder de forma privada a los servicios con tecnología

PrivateLink desde su VPC o desde sus instalaciones, sin utilizar direcciones IP públicas y sin necesidad de que el tráfico atraviese Internet.

Corrección

Para configurar un punto de enlace de VPC, consulte Acceder y Servicio de AWS utilizar un punto de enlace de VPC de interfaz en la Guía.AWS PrivateLink

[EC2.60] Las VPC deben configurarse con un punto final de interfaz para Systems Manager Incident Manager

Requisitos relacionados: NIST.800-53.r5 AC-21 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4)

Categoría: Proteger - Administración de acceso seguro > Control de acceso

Gravedad: media

Tipo de recurso: `AWS::EC2::VPC`, `AWS::EC2::VPCEndpoint`

Regla de AWS Config : vpc-endpoint-enabled

Tipo de programa: Periódico

Parámetros:

Parámetro	Obligatorio	Description (Descripción)	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`serviceNames`	Obligatorio	El nombre del servicio que el control evalúa	Cadena	No personalizable	`ssm-incidents`

Parámetro	Obligatorio	Description (Descripción)	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`vpcIds`	Opcional	Comma-separated lista de ID de Amazon VPC para puntos de enlace de VPC. Si se proporciona, el control falla si los servicios especificados en el parámetro `serviceName` no tienen uno de estos puntos de conexión de VPC.	StringList	Personalización con uno o más ID de VPC	Sin valor predeterminado

Este control comprueba si una nube privada virtual (VPC) que usted administra tiene un punto final de VPC de interfaz para Incident Manager. AWS Systems Manager El control falla si la VPC no tiene un punto de conexión de VPC de interfaz para el administrador de incidentes de Systems Manager. Este control evalúa recursos en una única cuenta.

AWS PrivateLink permite a los clientes acceder a los servicios alojados de una AWS manera escalable y de alta disponibilidad, al tiempo que mantiene todo el tráfico de la red dentro de la AWS red. Los usuarios del servicio pueden acceder de forma privada a los servicios con tecnología PrivateLink desde su VPC o desde sus instalaciones, sin utilizar direcciones IP públicas y sin necesidad de que el tráfico atraviese Internet.

Corrección

Para configurar un punto de enlace de VPC, consulte Acceder y Servicio de AWS utilizar un punto de enlace de VPC de interfaz en la Guía.AWS PrivateLink

[EC2.170] Las plantillas de lanzamiento de EC2 deben utilizar la versión 2 del servicio de metadatos de instancias (IMDSv2)

Requisitos relacionados: PCI DSS v4.0. 1/22.2.6

Categoría: Proteger > Seguridad de red

Gravedad: baja

Tipo de recurso: `AWS::EC2::LaunchTemplate`

Regla de AWS Config : ec2-launch-template-imdsv2-check

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una plantilla de lanzamiento de Amazon EC2 está configurada con el servicio de metadatos de la instancia versión 2 (IMDSv2). El control tiene errores si `HttpTokens` está configurado como `optional`,

El uso de recursos con versiones de software compatibles garantiza un rendimiento óptimo, seguridad y acceso a las características más recientes. Las actualizaciones periódicas protegen contra las vulnerabilidades, lo que ayuda a garantizar una experiencia de usuario estable y eficaz.

Corrección

Para solicitar IMDSv2 en una plantilla de lanzamiento de EC2, consulte Configuración de las opciones del servicio de metadatos de instancias en la Guía del usuario de Amazon EC2.

[EC2.171] Las conexiones VPN de EC2 deberían tener el registro habilitado

Requisitos relacionados: CIS AWS Foundations Benchmark v3.0. 0/5.3, PCI DSS v4.0. 1/103.4.2

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: `AWS::EC2::VPNConnection`

Regla de AWS Config : ec2-vpn-connection-logging-enabled

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una conexión AWS Site-to-Site VPN tiene Amazon CloudWatch Logs habilitado para ambos túneles. El control falla si una conexión Site-to-Site VPN no tiene habilitados CloudWatch los registros para ambos túneles.

AWS Site-to-Site Los registros de VPN le proporcionan una mayor visibilidad de sus despliegues de Site-to-Site VPN. Con esta función, tiene acceso a los registros de conexión Site-to-Site VPN que proporcionan detalles sobre el establecimiento del túnel de seguridad IP (IPsec), las negociaciones sobre el intercambio de claves de Internet (IKE) y los mensajes del protocolo de detección de pares muertos (DPD). Site-to-Site Los registros de VPN se pueden publicar en Logs. CloudWatch Esta función proporciona a los clientes una forma única y coherente de acceder a los registros detallados de todas sus conexiones Site-to-Site VPN y analizarlos.

Corrección

Para habilitar el registro de túneles en una conexión VPN de EC2, consulte los registros de AWS Site-to-Site VPN en la Guía del usuario de AWS Site-to-Site VPN.

[EC2.172] La configuración de acceso público del bloque de VPC de EC2 debería bloquear el tráfico de la puerta de enlace de Internet

Categoría: Proteger > Configuración de red segura > Recursos no accesibles públicamente

Gravedad: media

Tipo de recurso: `AWS::EC2::VPCBlockPublicAccessOptions`

AWS Config regla: `ec2-vpc-bpa-internet-gateway-blocked` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`vpcBpaInternetGatewayBlockMode`	Valor de cadena del modo de opciones de bloqueo de acceso público de la VPC.	Enum	`block-bidirectional` , `block-ingress`	Sin valor predeterminado

Este control comprueba si la configuración de bloqueo de acceso público (BPA) de las VPC de EC2 está establecida para bloquear el tráfico de puerta de enlace de Internet para todas las VPC de Amazon presentes en la Cuenta de AWS. El control falla si la configuración de bloqueo de acceso público de la VPC no está establecida para bloquear el tráfico de puerta de enlace de Internet. Para que el control pase, la opción de `InternetGatewayBlockMode` de bloqueo de acceso público de la VPC debe estar establecida en `block-bidirectional` o `block-ingress`. Si se proporciona el parámetro `vpcBpaInternetGatewayBlockMode`, el control pasa únicamente si el valor de bloqueo de acceso público de la VPC para `InternetGatewayBlockMode` coincide con el parámetro.

La configuración del BPA de la VPC para su cuenta en y Región de AWS le permite bloquear los recursos de las VPC y subredes de su propiedad en esa región para que no lleguen o sean accesibles desde Internet a través de puertas de enlace de Internet y puertas de enlace de Internet solo de salida. Si necesita que determinadas VPC y subredes puedan acceder o ser accesibles desde Internet, puede excluirlas mediante la configuración de exclusiones de bloqueo de acceso público de la VPC. Para obtener instrucciones sobre cómo crear y eliminar exclusiones, consulte Creación y eliminación de exclusiones en la Guía del usuario de Amazon VPC.

Corrección

Para habilitar el bloqueo de acceso público bidireccional a nivel de la cuenta, consulte Habilitación del modo bidireccional de BPA para la cuenta en la Guía del usuario de Amazon VPC. Para habilitar el bloqueo de acceso público solo de entrada, consulte Cómo cambiar el modo de bloqueo de acceso público de la VPC a solo de entrada. Para habilitar el bloqueo de acceso público de la VPC a nivel de la organización, consulte Habilitación del bloqueo de acceso público de la VPC a nivel de la organización.

[EC2.173] Las solicitudes de EC2 Spot Fleet con parámetros de lanzamiento deberían permitir el cifrado de los volúmenes de EBS adjuntos

Categoría: Proteger > Protección de datos > Cifrado de datos en reposo

Gravedad: media

Tipo de recurso: `AWS::EC2::SpotFleet`

Regla de AWS Config : ec2-spot-fleet-request-ct-encryption-at-rest

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control verifica si una solicitud de flota de Spot de Amazon EC2 que especifica parámetros de lanzamiento está configurada para habilitar el cifrado de todos los volúmenes de Amazon Elastic Block Store (Amazon EBS) asociados a instancias de EC2. El control falla si la solicitud de flota de spot especifica parámetros de lanzamiento y no habilita el cifrado para uno o más volúmenes EBS indicados en la solicitud.

Para mayor seguridad, debe habilitar el cifrado de los volúmenes de Amazon EBS. Las operaciones de cifrado se realizan en los servidores que alojan las instancias de Amazon EC2, lo que ayuda a garantizar la seguridad tanto de los datos en reposo como de los datos en tránsito entre una instancia y el almacenamiento de EBS asociado. El cifrado de Amazon EBS es una solución de cifrado sencilla para los recursos de EBS asociados a las instancias de EC2. Con el cifrado de EBS, no necesita crear, mantener ni proteger una infraestructura de administración de claves propia. El cifrado de EBS AWS KMS keys se utiliza al crear volúmenes cifrados.

> **Notas**
>
> Este control no genera resultados para las solicitudes de flota de spot de Amazon EC2 que usan plantillas de lanzamiento. Tampoco genera resultados para las solicitudes de flota de spot que no especifican explícitamente un valor para el parámetro `encrypted`.

Corrección

No existe una manera directa de cifrar un volumen de Amazon EBS existente que no esté cifrado. Solo puede cifrar un volumen nuevo cuando lo crea.

Sin embargo, si habilita el cifrado de manera predeterminada, Amazon EBS cifra los volúmenes nuevos con la clave predeterminada para el cifrado de EBS. Si no habilita el cifrado de manera predeterminada, puede habilitar el cifrado cuando crea un volumen individual. En ambos casos, puede reemplazar la clave predeterminada para el cifrado de EBS y elegir una clave de AWS KMS key administrada por el cliente. Para obtener más información sobre el cifrado de EBS, consulte el Cifrado de Amazon EBS en la Guía del usuario de Amazon EBS.

Para obtener información sobre cómo crear una solicitud de flota de spot de Amazon EC2, consulte Creación de una flota de spot en la Guía del usuario de Amazon Elastic Compute Cloud.

[EC2.174] Los conjuntos de opciones DHCP de EC2 deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::EC2::DHCPOptions`

Regla de AWS Config : ec2-dhcp-options-tagged

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredKeyTags`	Una lista de claves de etiqueta que no son del sistema y que se deben asignar a un recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control verifica si un conjunto de opciones de DHCP de Amazon EC2 tiene las claves de `requiredKeyTags` especificadas por el parámetro . El control falla si el conjunto de opciones no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas por el parámetro

`requiredKeyTags`. Si no especifica ningún valor para el parámetro `requiredKeyTags`, el control solo verifica la existencia de una clave de etiqueta y falla si el conjunto de opciones no tiene ninguna clave de etiqueta. El control ignora las etiquetas del sistema, que se aplican automáticamente y tienen el prefijo `aws:`.

Una etiqueta es una etiqueta que se crea y se asigna a un AWS recurso. Cada etiqueta consta de una clave de etiqueta necesaria y un valor de etiqueta opcional. Utilice etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. También pueden ayudar a identificar, organizar, buscar y filtrar recursos. También pueden ayudar a rastrear propietarios de recursos para acciones y notificaciones. También puede usar etiquetas para implementar control de acceso basado en atributos (ABAC) como estrategia de autorización. Para obtener más información sobre estrategias ABAC, consulte Definición de permisos basados en atributos con autorización ABAC en la Guía del usuario de IAM. Para obtener más información sobre las etiquetas, consulte los AWS recursos de etiquetado y la Guía del usuario del editor de etiquetas.

> **Note**
>
> No almacene información de identificación personal (PII) ni otra información confidencial en las etiquetas. Se puede acceder a las etiquetas desde muchos Servicios de AWS sitios. No están destinadas a usarse para datos privados o información confidencial.

Corrección

Para obtener información sobre cómo agregar etiquetas a un conjunto de opciones de DHCP de Amazon EC2, consulte Etiquetado de los recursos de Amazon EC2 en la Guía del usuario de Amazon EC2.

[EC2.175] Las plantillas de lanzamiento de EC2 deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::EC2::LaunchTemplate`

Regla de AWS Config : ec2-launch-template-tagged

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredKeyTags`	Una lista de claves de etiqueta que no son del sistema y que se deben asignar a un recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control verifica si una plantilla de lanzamiento de Amazon EC2 tiene las claves de etiqueta especificadas por el parámetro `requiredKeyTags`. El control falla si la plantilla de lanzamiento no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas por el parámetro `requiredKeyTags`. Si usted no especifica ningún valor para el parámetro `requiredKeyTags`, el control solo verifica la existencia de una clave de etiqueta y falla si la plantilla de lanzamiento no tiene ninguna clave de etiqueta. El control ignora las etiquetas del sistema, que se aplican automáticamente y tienen el prefijo `aws:`.

Una etiqueta es una etiqueta que se crea y se asigna a un AWS recurso. Cada etiqueta consta de una clave de etiqueta necesaria y un valor de etiqueta opcional. Utilice etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. También pueden ayudar a identificar, organizar, buscar y filtrar recursos. También pueden ayudar a rastrear propietarios de recursos para acciones y notificaciones. También puede usar etiquetas para implementar control de acceso basado en atributos (ABAC) como estrategia de autorización. Para obtener más información sobre estrategias ABAC, consulte Definición de permisos basados en atributos con autorización ABAC en la Guía del usuario de IAM. Para obtener más información sobre las etiquetas, consulte los AWS recursos de etiquetado y la Guía del usuario del editor de etiquetas.

> **Note**
>
> No almacene información de identificación personal (PII) ni otra información confidencial en las etiquetas. Se puede acceder a las etiquetas desde muchos Servicios de AWS sitios. No están destinadas a usarse para datos privados o información confidencial.

Corrección

Para obtener información sobre cómo agregar tags a una plantilla de lanzamiento de Amazon EC2, consulte Etiquetado de los recursos de Amazon EC2 en la Guía del usuario de Amazon EC2.

[EC2.176] Las listas de prefijos de EC2 deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::EC2::PrefixList`

Regla de AWS Config : ec2-prefix-list-tagged

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredKeyTags`	Una lista de claves de etiqueta que no son del sistema y que se deben asignar a un recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control realiza una comprobación para verificar si una lista de prefijos de Amazon EC2 tiene las claves de etiquetas especificadas por el parámetro `requiredKeyTags`. El control falla si la lista de prefijos no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas por el parámetro `requiredKeyTags`. Si uno especifica valores para el parámetro `requiredKeyTags`, el control solo realiza una comprobación de la existencia de una clave de etiqueta y falla si la lista de prefijos no tiene ninguna clave de etiqueta. El control ignora las etiquetas del sistema, que se aplican automáticamente y tienen el prefijo `aws:`.

Una etiqueta es una etiqueta que se crea y se asigna a un AWS recurso. Cada etiqueta consta de una clave de etiqueta necesaria y un valor de etiqueta opcional. Utilice etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. También pueden ayudar a identificar, organizar, buscar y filtrar recursos. También pueden ayudar a rastrear propietarios de recursos para acciones y notificaciones. También puede usar etiquetas para implementar control de acceso basado en atributos (ABAC) como estrategia de autorización. Para obtener más información sobre estrategias ABAC, consulte Definición de permisos basados en atributos con autorización ABAC en la Guía del usuario de IAM. Para obtener más información sobre las etiquetas, consulte los AWS recursos de etiquetado y la Guía del usuario del editor de etiquetas.

> **Note**
>
> No almacene información de identificación personal (PII) ni otra información confidencial en las etiquetas. Se puede acceder a las etiquetas desde muchos Servicios de AWS sitios. No están destinadas a usarse para datos privados o información confidencial.

Corrección

Para obtener información sobre cómo agregar etiquetas a una lista de prefijos de Amazon EC2, consulte Etiquetad de los recursos de Amazon EC2 en la Guía del usuario de Amazon EC2.

[EC2.177] Las sesiones de réplica de tráfico de EC2 deben etiquetarse

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::EC2::TrafficMirrorSession`

Regla de AWS Config : ec2-traffic-mirror-session-tagged

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredKeyTags`	Una lista de claves de etiqueta que no son del sistema y que se deben asignar a un recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control verifica si una sesión de duplicación de tráfico de Amazon EC2 tiene las claves de etiqueta especificadas por el parámetro `requiredKeyTags`. El control falla si la sesión no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas por el parámetro `requiredKeyTags`. Si no especifica valores para el parámetro `requiredKeyTags`, el control solo realiza una comprobación de la existencia de una clave de de etiqueta y falla si la sesión no tiene ninguna clave de etiqueta. El control ignora las etiquetas del sistema, que se aplican automáticamente y tienen el prefijo `aws:`.

Una etiqueta es una etiqueta que se crea y se asigna a un AWS recurso. Cada etiqueta consta de una clave de etiqueta necesaria y un valor de etiqueta opcional. Utilice etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. También pueden ayudar a identificar, organizar, buscar y filtrar recursos. También pueden ayudar a rastrear propietarios de recursos para acciones y notificaciones. También puede usar etiquetas para implementar control de acceso basado en atributos (ABAC) como estrategia de autorización. Para obtener más información sobre estrategias ABAC, consulte Definición de permisos basados en atributos con autorización ABAC en la Guía del usuario de IAM. Para obtener más información sobre las etiquetas, consulte los AWS recursos de etiquetado y la Guía del usuario del editor de etiquetas.

> **Note**
>
> No almacene información de identificación personal (PII) ni otra información confidencial en las etiquetas. Se puede acceder a las etiquetas desde muchos Servicios de AWS sitios. No están destinadas a usarse para datos privados o información confidencial.

Corrección

Para obtener información sobre cómo agregar etiquetas a una sesión de duplicación de tráfico de Amazon EC2, consulte Etiquetado de los recursos de Amazon EC2 en la Guía del usuario de Amazon EC2.

[EC2.178] Los filtros espejo de tráfico EC2 deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::EC2::TrafficMirrorFilter`

Regla de AWS Config : ec2-traffic-mirror-filter-tagged

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredKeyTags`	Una lista de claves de etiqueta que no son del sistema y que se deben asignar a un recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control verificar si un filtro de duplicación de tráfico de Amazon EC2 tiene las claves de etiqueta especificadas por el parámetro `requiredKeyTags`. El control falla si el filtro no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas por el parámetro `requiredKeyTags`. Si no especifica valores para el parámetro `requiredKeyTags`, el control solo verifica la existencia de una clave de etiqueta y falla si el filtro no tiene ninguna clave de etiqueta. El control ignora las etiquetas del sistema, que se aplican automáticamente y tienen el prefijo `aws:`.

Una etiqueta es una etiqueta que se crea y se asigna a un AWS recurso. Cada etiqueta consta de una clave de etiqueta necesaria y un valor de etiqueta opcional. Utilice etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. También pueden ayudar a identificar, organizar, buscar y filtrar recursos. También pueden ayudar a rastrear propietarios de recursos para acciones y notificaciones. También puede usar etiquetas para implementar control de acceso basado en atributos (ABAC) como estrategia de autorización. Para obtener más información sobre estrategias ABAC, consulte Definición de permisos basados en atributos con autorización ABAC en la Guía del usuario de IAM. Para obtener más información sobre las etiquetas, consulte los AWS recursos de etiquetado y la Guía del usuario del editor de etiquetas.

> **Note**
>
> No almacene información de identificación personal (PII) ni otra información confidencial en las etiquetas. Se puede acceder a las etiquetas desde muchos Servicios de AWS sitios. No están destinadas a usarse para datos privados o información confidencial.

Corrección

Para obtener información sobre cómo agregar etiquetas a un filtro de duplicación de tráfico de Amazon EC2, consulte Etiquetado de los recursos de Amazon EC2 en la Guía del usuario de Amazon EC2.

[EC2.179] Los objetivos del espejo de tráfico de EC2 deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::EC2::TrafficMirrorTarget`

Regla de AWS Config : ec2-traffic-mirror-target-tagged

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredKeyTags`	Una lista de claves de etiqueta que no son del sistema y que se deben asignar a un recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control verifica si un destino de duplicación de tráfico de Amazon EC2 tiene las claves de etiqueta especificadas por el parámetro `requiredKeyTags`. El control falla si el destino no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas por el parámetro `requiredKeyTags`. Si no especifica ningún valor para el parámetro `requiredKeyTags`, el control comprueba únicamente la existencia de una clave de etiqueta y falla si el destino no tiene ninguna clave de etiqueta. El control ignora las etiquetas del sistema, que se aplican automáticamente y tienen el prefijo `aws:`.

Una etiqueta es una etiqueta que se crea y se asigna a un AWS recurso. Cada etiqueta consta de una clave de etiqueta necesaria y un valor de etiqueta opcional. Utilice etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. También pueden ayudar a identificar, organizar, buscar y filtrar recursos. También pueden ayudar a rastrear propietarios de recursos para acciones y notificaciones. También puede usar etiquetas para implementar control de acceso basado en atributos (ABAC) como estrategia de autorización. Para obtener más información sobre estrategias ABAC, consulte Definición de permisos basados en atributos con autorización ABAC en la Guía del usuario de IAM. Para obtener más información sobre las etiquetas, consulte los AWS recursos de etiquetado y la Guía del usuario del editor de etiquetas.

> **Note**
>
> No almacene información de identificación personal (PII) ni otra información confidencial en las etiquetas. Se puede acceder a las etiquetas desde muchos Servicios de AWS sitios. No están destinadas a usarse para datos privados o información confidencial.

Corrección

Para obtener información sobre cómo agregar etiquetas a un destino de duplicación de tráfico de Amazon EC2, consulte Etiquetado de los recursos de Amazon EC2 en la Guía del usuario de Amazon EC2.

[EC2.180] Las interfaces de red EC2 deberían tener habilitada source/destination la verificación

Categoría: Proteger > Seguridad de red

Gravedad: media

Tipo de recurso: `AWS::EC2::NetworkInterface`

Regla de AWS Config : ec2-enis-source-destination-check-enabled

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si la source/destination comprobación está habilitada para una interfaz de red elástica (ENI) Amazon EC2 administrada por los usuarios. El control falla si la source/destination verificación está deshabilitada para la ENI administrada por el usuario. Este control verifica únicamente los siguientes tipos de ENI: `aws_codestar_connections_managed`, `branch`, `efa`, `interface`, `lambday quicksight`.

Source/destination la comprobación de las instancias de Amazon EC2 y los ENI adjuntos debe estar habilitada y configurada de forma coherente en todas las instancias de EC2. Cada ENI tiene su propia configuración de comprobaciones. source/destination Si la source/destination comprobación está habilitada, Amazon EC2 aplica la validación de source/destination direcciones, lo que garantiza que una instancia sea el origen o el destino del tráfico que reciba. Esto proporciona un nivel adicional de seguridad de red al evitar que los recursos procesen tráfico no deseado y al impedir la suplantación de direcciones IP.

> **Note**
>
> Si utiliza una instancia EC2 como instancia de NAT y ha desactivado la source/destination comprobación de su ENI, puede utilizar una puerta de enlace NAT en su lugar.

Corrección

Para obtener información sobre cómo habilitar las source/destination comprobaciones para una ENI de Amazon EC2, consulte Modificar los atributos de la interfaz de red en la Guía del usuario de Amazon EC2.

[EC2.181] Las plantillas de lanzamiento de EC2 deberían permitir el cifrado de los volúmenes de EBS adjuntos

Categoría: Proteger > Protección de datos > Cifrado de datos en reposo

Gravedad: media

Tipo de recurso: `AWS::EC2::LaunchTemplate`

Regla de AWS Config : ec2-launch-templates-ebs-volume-encrypted

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control verifica si una plantilla de lanzamiento de Amazon EC2 habilita el cifrado para todos los volúmenes de EBS asociados. El control falla si el parámetro de cifrado está establecido en `False` para cualquiera de los volúmenes de EBS especificados por la plantilla de lanzamiento de EC2.

El cifrado de Amazon EBS es una solución de cifrado sencilla para los recursos de EBS asociados a las instancias de Amazon EC2. Con el cifrado de EBS, no necesita crear, mantener ni proteger una infraestructura de administración de claves propia. El cifrado de EBS usa AWS KMS keys al crear volúmenes cifrados e instantáneas. Las operaciones de cifrado se realizan en los servidores que alojan instancias de EC2, lo que ayuda a garantizar la seguridad de los datos en reposo y en tránsito entre una instancia de EC2 y su almacenamiento EBS asociado. Para obtener más información, consulte Cifrado de Amazon EBS en la Guía del usuario de Amazon EBS.

Puede habilitar el cifrado de EBS durante los lanzamientos manuales de instancias individuales de EC2. Sin embargo, existen varios beneficios al usar plantillas de lanzamiento de EC2 y configurar ajustes de cifrado en esas plantillas. Puede aplicar el cifrado como estándar y garantizar el uso de configuraciones de cifrado coherentes. También puede reducir el riesgo de errores y brechas de seguridad que podrían ocurrir con lanzamientos manuales de instancias.

> **Note**
>
> Cuando este control verifica una plantilla de lanzamiento de EC2, solo evalúa los ajustes de cifrado de EBS que se especifican explícitamente en la plantilla. La evaluación no incluye configuraciones de cifrado heredadas del cifrado a nivel de cuenta para EBS, asignaciones de dispositivos de bloque de AMI o estados de cifrado de instantáneas de origen.

Corrección

Después de crear una plantilla de lanzamiento de Amazon EC2, no puede modificarla. Sin embargo, puede crear una nueva versión de una plantilla de lanzamiento y cambiar los ajustes de cifrado en esa nueva versión de la plantilla. También puede especificar la nueva versión como la versión predeterminada de la plantilla de lanzamiento. Luego, si lanza una instancia de EC2 desde una plantilla de lanzamiento y no especifica una versión de plantilla, EC2 usa los ajustes de la versión predeterminada cuando lanza la instancia. Para obtener más información, consulte Modificación de una plantilla de lanzamiento en la Guía del usuario de Amazon EC2.

[EC2.182] La configuración de bloqueo de acceso público debe estar habilitada para las instantáneas de Amazon EBS

Categoría: Proteger > Configuración de red segura > Recursos no accesibles públicamente

Gravedad: alta

Tipo de recurso: `AWS::EC2::SnapshotBlockPublicAccess`

Regla de AWS Config : ebs-snapshot-block-public-access

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si el bloqueo de acceso público a nivel de cuenta está habilitado para impedir que se compartan las instantáneas de Amazon EBS con todos. El control fallará si la opción Bloquear el acceso público no está habilitada para impedir que todos puedan compartir las instantáneas de Amazon EBS.

Para evitar que se compartan públicamente sus instantáneas de Amazon EBS, puede habilitar el bloqueo del acceso público a las instantáneas. Una vez activado el bloqueo del acceso público

a las instantáneas en una región, se bloquea automáticamente cualquier intento de compartir públicamente las instantáneas en esa región. Esto ayuda a mejorar la seguridad de las instantáneas y a proteger los datos de las instantáneas contra el acceso no autorizado o no intencionado.

Corrección

Para habilitar el acceso público bloqueado para las instantáneas, consulte Configurar el acceso público bloqueado para las instantáneas de Amazon EBS en la Guía del usuario de Amazon EBS. En Bloquear el acceso público, seleccione Bloquear todo el acceso público.

[EC2.183] Las conexiones VPN de EC2 deben utilizar el protocolo IKEv2

Categoría: Proteger > Protección de datos > Cifrado de datos en tránsito

Gravedad: media

Tipo de recurso: `AWS::EC2::VPNConnection`

Regla de AWS Config : ec2-vpn-connection-ike-version-check

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una conexión AWS Site-to-Site VPN está configurada para utilizar el protocolo IKEv2. El control falla si una conexión Site-to-Site VPN permite el protocolo IKEv1 o no lo restringe explícitamente a IKEv2 en todos los túneles VPN.

El IKEv2 proporciona algoritmos criptográficos más sólidos y funciones de seguridad mejoradas en comparación con el protocolo IKEv1 anterior, incluida la protección integrada contra los ataques de denegación de servicio y los mecanismos de autenticación mejorados. El IKEv1 tiene vulnerabilidades y debilidades conocidas en su proceso de intercambio de claves que los atacantes pueden aprovechar para comprometer la seguridad de los túneles VPN. Al reforzar IKEv2-only las conexiones, se reduce la superficie de ataque y se asegura de que las comunicaciones por VPN utilicen protocolos de cifrado modernos y estándares del sector que protegen mejor los datos en tránsito.

Corrección

Para actualizar la versión IKE para un túnel VPN en una conexión VPN de EC2, consulte Modificar las opciones del túnel AWS Site-to-Site VPN en la Guía del usuario de AWS Site-to-Site VPN.

Controles CSPM de Security Hub para Auto Scaling

Estos controles CSPM de Security Hub evalúan el servicio y los recursos de Amazon EC2 Auto Scaling.

Es posible que estos controles no estén disponibles en todos. Regiones de AWS Para obtener más información, consulte Disponibilidad de los controles por región.

[AutoScaling.1] Los grupos de Auto Scaling asociados a un balanceador de cargas deben usar comprobaciones de estado del ELB

Requisitos relacionados: PCI DSS v3.2. 1/2.2, (2 NIST.800-53.r5 CP-2) NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-2

Categoría: Identificar - Inventario

Gravedad: baja

Tipo de recurso: `AWS::AutoScaling::AutoScalingGroup`

Regla de AWS Config: `autoscaling-group-elb-healthcheck-required`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un grupo de Amazon EC2 Auto Scaling que está asociado a un equilibrador de carga, utiliza comprobaciones de estado de Elastic Load Balancing (ELB). El control falla si el grupo de escalado automático no utiliza comprobaciones de estado de ELB.

Las comprobaciones de estado de ELB ayudan a garantizar que el grupo de escalado automático pueda determinar el estado de una instancia en función de las pruebas adicionales que proporciona el equilibrador de carga. El uso de las comprobaciones de estado del equilibrador de carga elástico también puede ayudar a respaldar la disponibilidad de las aplicaciones que usan grupos de escalado automático de EC2.

Corrección

Para agregar comprobaciones de estado de Equilibrador de carga elástico, consulte Adición de comprobaciones de estado de Equilibrador de carga elástico en la Guía del usuario de Amazon EC2 Auto Scaling.

[AutoScaling.2] El grupo Amazon EC2 Auto Scaling debe cubrir varias zonas de disponibilidad

Requisitos relacionados: NIST.800-53.r5 CP-10 NIST.800-53.r5 CP-2 (2), NIST.800-53.r5 CP-6 (2) NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoría: Recuperación > Resiliencia > Alta disponibilidad

Gravedad: media

Tipo de recurso: `AWS::AutoScaling::AutoScalingGroup`

Regla de AWS Config: `autoscaling-multiple-az`

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub	
`minAvailabilityZones`	Cantidad mínima de zonas de disponibilidad	Enum	`2, 3, 4, 5, 6`	`2`	

Este control comprueba si un grupo de Amazon EC2 Auto Scaling abarca al menos la cantidad especificada de zonas de disponibilidad (AZ). Se produce un error en el control si un grupo de escalado automático no abarca al menos la cantidad especificada de AZ. A menos que proporcione un valor de parámetro personalizado para el número mínimo de zonas de disponibilidad, el CSPM de Security Hub utiliza un valor predeterminado de dos zonas de disponibilidad.

Un grupo de escalado automático que no abarque varias AZ no puede lanzar instancias en otra AZ para compensar si la AZ única configurada deja de estar disponible. Sin embargo, en algunos casos de uso, puede preferirse un grupo de escalado automático con una sola zona de disponibilidad, como los trabajos por lotes o cuando los costos de transferencia entre zonas de disponibilidad deben mantenerse al mínimo. En esos casos, puede deshabilitar este control o suprimir sus resultados.

Corrección

Para agregar AZ a un grupo de escalado automático existente, consulte Agregación o eliminación de zonas de disponibilidad en la Guía del usuario de Amazon EC2 Auto Scaling.

[AutoScaling.3] Las configuraciones de lanzamiento grupal de Auto Scaling deberían configurar las instancias EC2 para que requieran la versión 2 del Servicio de Metadatos de Instancia (IMDSv2)

Requisitos relacionados: NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-3 (15), (7), NIST.800-53.r5 AC-3 NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 AC-6 NIST.800-53.r5 CM-2, PCI DSS v4.0. 1/22.2.6

Categoría: Proteger - Configuración de red segura

Gravedad: alta

Tipo de recurso: `AWS::AutoScaling::LaunchConfiguration`

Regla de AWS Config: `autoscaling-launchconfig-requires-imdsv2`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si IMDSv2 está habilitado en todas las instancias lanzadas por los grupos de Amazon EC2 Auto Scaling. El control falla si la versión del servicio de metadatos de instancias (IMDS) no está incluida en la configuración de lanzamiento o está configurada como`token optional`, que es una configuración que permite IMDSv1 o IMDSv2.

El IMDS brinda datos sobre una instancia que puede utilizar para configurar o administrar la instancia en ejecución.

La versión 2 del IMDS añade nuevas protecciones que no estaban disponibles en IMDSv1 para proteger aún más las instancias de EC2.

Corrección

Un grupo de escalado automático asocia con una configuración de lanzamiento cada vez. No se puede modificar una configuración de lanzamiento después de crearla. Para cambiar la configuración de lanzamiento de un grupo de escalado automático, utilice una configuración de lanzamiento existente como punto de partida para una nueva configuración de lanzamiento con IMDSv2

habilitado. Para obtener más información, consulte Configurar las opciones de metadatos de la instancia para nuevas instancias en la Guía del usuario de Amazon EC2.

[AutoScaling.4] La configuración de inicio de grupo de Auto Scaling no debe tener un límite de saltos de respuesta de metadatos superior a 1

> **Important**
>
> Security Hub CSPM retiró este control en abril de 2024. Para obtener más información, consulte Registro de cambios de los controles del CSPM de Security Hub.

Requisitos relacionados: NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoría: Proteger - Configuración de red segura

Gravedad: alta

Tipo de recurso: `AWS::AutoScaling::LaunchConfiguration`

Regla de AWS Config: `autoscaling-launch-config-hop-limit`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba el número de saltos de red que puede recorrer un token de metadatos. El control falla si el límite de saltos de respuesta de los metadatos es superior a 1.

El servicio de metadatos de instancias (IMDS) proporciona información de metadatos sobre una instancia de Amazon EC2 y resulta útil para la configuración de aplicaciones. Restringir la respuesta HTTP de PUT del servicio de metadatos a solo la instancia EC2 protege al IMDS del uso no autorizado.

El campo Tiempo de vida (TTL) del paquete IP se reduce en uno en cada salto. Esta reducción se puede utilizar para garantizar que el paquete no viaje fuera de EC2. IMDSv2 protege las instancias de EC2 que pueden estar mal configuradas como enrutadores abiertos, firewalls de capa 3, VPN, túneles o dispositivos NAT, lo que impide que usuarios no autorizados recuperen los metadatos. Con IMDSv2, la respuesta de PUT que contiene el token secreto no puede viajar fuera de la instancia porque el límite de saltos de respuesta de metadatos predeterminado se ha establecido como 1. Sin embargo, si este valor es superior a 1, el token puede salir de la instancia EC2.

Corrección

Para modificar el límite de saltos de respuesta de metadatos para una configuración de lanzamiento existente, consulte Modificar las opciones de metadatos de la instancia para las instancias existentes en la Guía del usuario de Amazon EC2.

[Autoscaling.5] Las instancias de Amazon EC2 lanzadas mediante configuraciones de lanzamiento grupal de Auto Scaling no deben tener direcciones IP públicas

Requisitos relacionados: NIST.800-53.r5 AC-21 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), (21) NIST.800-53.r5 AC-4,, NIST.800-53.r5 AC-4 (11) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (21), (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), PCI DSS v4.0. 1/14.4.4

Categoría: Proteger > Configuración de red segura > Recursos no accesibles públicamente

Gravedad: alta

Tipo de recurso: `AWS::AutoScaling::LaunchConfiguration`

Regla de AWS Config: `autoscaling-launch-config-public-ip-disabled`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si la configuración de lanzamiento asociada a un grupo de escalado automático asigna una dirección IP pública a las instancias del grupo. El control falla si la configuración de lanzamiento asociada asigna una dirección IP pública.

Las instancias de Amazon EC2 en una configuración de lanzamiento grupal de Auto Scaling no deben tener una dirección IP pública asociada, excepto en casos extremos limitados. Solo se debe acceder a las instancias de Amazon EC2 desde detrás de un equilibrador de carga, en lugar de estar expuestas directamente a Internet.

Corrección

Un grupo de escalado automático asocia con una configuración de lanzamiento cada vez. No se puede modificar una configuración de lanzamiento después de crearla. Para cambiar la configuración de lanzamiento de un grupo de escalado automático, utilice una configuración de lanzamiento

existente como punto de partida para una nueva configuración de lanzamiento. A continuación, actualice el grupo de escalado automático para utilizar la nueva configuración de lanzamiento. Para obtener instrucciones paso a paso, consulte Cambiar la configuración de lanzamiento de un grupo de escalado automático en la Guía del usuario de Amazon EC2 Auto Scaling. Al crear la nueva configuración de lanzamiento, en Configuración adicional, en Detalles avanzados, tipo de dirección IP, seleccione No asignar una dirección IP pública a ninguna instancia.

Después de cambiar la configuración de lanzamiento, Auto Scaling lanza nuevas instancias con las nuevas opciones de configuración. Las instancias existentes no se ven afectadas. Para actualizar una instancia existente, le recomendamos que actualice su instancia o permita que el escalado automático reemplace gradualmente las instancias más antiguas por instancias más recientes en función de sus políticas de terminación. Para obtener más información acerca de cómo actualizar un grupo de Amazon EC2 Auto Scaling, consulte Grupos de escalado automático en la Guía del usuario de Amazon EC2 Auto Scaling.

[AutoScaling.6] Los grupos de Auto Scaling deben usar varios tipos de instancias en múltiples zonas de disponibilidad

Requisitos relacionados: NIST.800-53.r5 CP-10 NIST.800-53.r5 CP-2 (2), NIST.800-53.r5 CP-6 (2) NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoría: Recuperación > Resiliencia > Alta disponibilidad

Gravedad: media

Tipo de recurso: `AWS::AutoScaling::AutoScalingGroup`

Regla de AWS Config: `autoscaling-multiple-instance-types`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un grupo de Amazon EC2 Auto Scaling utiliza varios tipos de instancias. El control falla si el grupo de escalado automático solo tiene un tipo de instancia definido.

Puede mejorar la disponibilidad si implementa la aplicación en varios tipos de instancia que se ejecutan en varias zonas de disponibilidad. Security Hub CSPM recomienda usar varios tipos de instancias para que el grupo de Auto Scaling pueda lanzar otro tipo de instancia si la capacidad de instancias es insuficiente en las zonas de disponibilidad elegidas.

Corrección

Para crear un grupo de escalado automático con varios tipos de instancias, consulte Grupos de escalado automático con varios tipos de instancias y opciones de compra en la Guía del usuario de Amazon EC2 Auto Scaling.

[AutoScaling.9] Los grupos de Amazon EC2 Auto Scaling deben utilizar las plantillas de lanzamiento de Amazon EC2

Requisitos relacionados: NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoría: Identificar > Configuración de recursos

Gravedad: media

Tipo de recurso: `AWS::AutoScaling::AutoScalingGroup`

Regla de AWS Config: `autoscaling-launch-template`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si se crea un grupo de Amazon EC2 Auto Scaling a partir de una plantilla de lanzamiento de EC2. Este control falla si no se crea un grupo de Amazon EC2 Auto Scaling con una plantilla de lanzamiento o si no se especifica una plantilla de lanzamiento en una política de instancias mixtas.

Un grupo de escalado automático puede crearse a partir de una plantilla de lanzamiento de EC2 o una configuración de lanzamiento. Sin embargo, el uso de una plantilla de lanzamiento para crear un grupo de escalado automático garantiza que tenga acceso a las funciones y mejoras más recientes.

Corrección

Para crear un grupo de escalado automático con una plantilla de lanzamiento de EC2, consulte Creación de un grupo de escalado automático mediante una plantilla de lanzamiento en la Guía del usuario de Amazon EC2 Auto Scaling. Para obtener información sobre cómo reemplazar una configuración de lanzamiento por una plantilla de lanzamiento, consulte Reemplazar una configuración de lanzamiento por una plantilla de lanzamiento en la Guía del usuario de Amazon EC2.

[AutoScaling.10] Los grupos de Auto Scaling de EC2 deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::AutoScaling::AutoScalingGroup`

AWS Configregla: `tagged-autoscaling-autoscalinggroup` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si un grupo de Amazon EC2 Auto Scaling tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control falla si el grupo de escalado automático no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y falla si el grupo de escalado automático no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno

u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, incluidasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte Etiquetar sus AWS recursos en el. Referencia general de AWS

Corrección

Para agregar etiquetas a un grupo de escalado automático, consulte Etiquetar grupos de escalado automático e instancias en la Guía del usuario de Amazon EC2 Auto Scaling.

Controles de CSPM de Security Hub para Amazon ECR

Estos controles CSPM de Security Hub evalúan el servicio y los recursos de Amazon Elastic Container Registry (Amazon ECR).

Es posible que estos controles no estén disponibles en todos los casos. Regiones de AWS Para obtener más información, consulte Disponibilidad de los controles por región.

[ECR.1] Los repositorios privados de ECR deben tener configurado el escaneo de imágenes

Requisitos relacionados: PCI NIST.800-53.r5 RA-5 DSS v4.0. 1/63.2.3, PCI DSS v4.0. 1/62.2.4

Categoría: Identificar > Administración de vulnerabilidades, parches y versiones

Gravedad: alta

Tipo de recurso: `AWS::ECR::Repository`

Regla de AWS Config : ecr-private-image-scanning-enabled

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si un repositorio privado de Amazon ECR tiene configurado el escaneo de imágenes. El control falla si el repositorio de ECR privado no está configurado para el escaneo instantáneo o continuo.

El escaneo de imágenes de ECR ayuda a identificar vulnerabilidades de software en las imágenes de contenedor. La configuración del escaneo de imágenes en los repositorios de ECR añade un nivel de verificación de la integridad y la seguridad de las imágenes que se almacenan.

Corrección

Para configurar el escaneo de imágenes para un repositorio de ECR, consulte el Escaneo de imágenes en la Guía del usuario de Amazon Elastic Container Registry.

[ECR.2] Los repositorios privados de ECR deben tener configurada la inmutabilidad de etiquetas

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2 (1) NIST.800-53.r5 CM-8

Categoría: Identificar > Inventario > Etiquetado

Gravedad: media

Tipo de recurso: `AWS::ECR::Repository`

Regla de AWS Config : ecr-private-tag-immutability-enabled

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un repositorio de ECR privado tiene habilitada la inmutabilidad de etiquetas. Este control falla si un repositorio de ECR privado tiene deshabilitada la inmutabilidad de etiquetas. Esta regla se aplica si la inmutabilidad de la etiqueta está habilitada y tiene el valor `IMMUTABLE`.

La inmutabilidad de las etiquetas ECR de Amazon permite a los clientes confiar en las etiquetas descriptivas de una imagen como un mecanismo fiable para rastrear e identificar las imágenes de

forma única. Una etiqueta inmutable es estática, lo que significa que cada etiqueta hace referencia a una imagen única. Esto mejora la fiabilidad y la escalabilidad, ya que el uso de una etiqueta estática siempre tendrá como resultado la implementación de la misma imagen. Cuando se configura, la inmutabilidad de las etiquetas evita que se anulen, lo que reduce la superficie expuesta a ataques.

Corrección

Para crear un repositorio con etiquetas inmutables configuradas o para actualizar la configuración de mutabilidad de las etiquetas de imagen de un repositorio existente, consulte la Mutabilidad de las etiquetas de imagen en la Guía del usuario de Amazon Elastic Container registry.

[ECR.3] Los repositorios de ECR deben tener configurada al menos una política de ciclo de vida

Requisitos relacionados: NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoría: Identificar > Configuración de recursos

Gravedad: media

Tipo de recurso: `AWS::ECR::Repository`

Regla de AWS Config : ecr-private-lifecycle-policy-configured

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un repositorio de Amazon ECR tiene configurada al menos una política de ciclo de vida. Este control falla si un repositorio de ECR no tiene ninguna política de ciclo de vida configurada.

Las políticas de ciclo de vida de Amazon ECR permiten especificar la administración de ciclo de vida de las imágenes de un repositorio. Al configurar las políticas del ciclo de vida, puede automatizar la limpieza de las imágenes sin utilizar y la caducidad de las imágenes en función de su antigüedad o recuento. La automatización de estas tareas puede ayudarte a evitar el uso involuntario de imágenes desactualizadas en tu repositorio.

Corrección

Para configurar una política de ciclo de vida, consulte la Vista previa sobre cómo crear una política de ciclo de vida en la Guía del usuario de Amazon Elastic Container Registry.

[ECR.4] Los repositorios públicos de ECR deben etiquetarse

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::ECR::PublicRepository`

AWS Config regla: `tagged-ecr-publicrepository` (regla CSPM personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub CSPM
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si un repositorio público de Amazon ECR tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control falla si el repositorio público no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y falla si el repositorio público no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y se compone de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El

etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWSen la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Las etiquetas son accesibles para muchos Servicios de AWS, incluso AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulta Cómo etiquetar tus AWS recursos en. Referencia general de AWS

Corrección

Para agregar etiquetas a un repositorio público de ECR, consulte Tagging an Amazon ECR public repository en la Guía del usuario de Amazon Elastic Container Registry.

[ECR.5] Los repositorios de ECR deben estar cifrados y ser gestionados por el cliente AWS KMS keys

Requisitos relacionados: NIST.800-53.r5 SC-12 (2), NIST.800-53.r5 CM-3 (6),, NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 SI-7 (6), NIST.800-53.r5 AU-9

Categoría: Proteger > Protección de datos > Cifrado de datos en reposo

Gravedad: media

Tipo de recurso: `AWS::ECR::Repository`

Regla de AWS Config : ecr-repository-cmk-encryption-enabled

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub CSPM
`kmsKeyArns`	Una lista de los nombres de recursos de Amazon (ARN) AWS KMS keys para incluir en la evaluación. El control genera un resultado `FAILED` si un repositorio de ECR no está cifrado con una clave de KMS incluida en la lista.	StringList (máximo de 10 artículos)	Entre 1 y 10 ARN de claves de KMS existentes. Por ejemplo: `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`	Sin valor predeterminado

Este control verifica si un repositorio de Amazon ECR está cifrado en reposo con una clave de AWS KMS key administrada por el cliente. El control falla si el repositorio de ECR no está cifrado con una clave de KMS administrada por el cliente. Puede especificar opcionalmente una lista de claves de KMS para que el control las incluya en la evaluación.

De forma predeterminada, Amazon ECR cifra los datos del repositorio con las claves administradas de Amazon S3 (SSE-S3) mediante un AES-256 algoritmo. Para obtener un control adicional, puede configurar Amazon ECR para cifrar los datos con un AWS KMS key (SSE-KMS o) en su lugar. DSSE-KMS La clave de KMS puede ser: una Clave administrada de AWS que Amazon ECR crea y administra en su nombre, y tiene el alias `aws/ecr`, o una clave administrada por el cliente que crea y administra en la Cuenta de AWS. Con una clave de KMS administrada por el cliente, ejerce control pleno sobre la clave. Esto incluye definir y mantener la política de claves, administrar concesiones, rotar el material criptográfico, asignar etiquetas, crear alias, y habilitar y deshabilitar la clave.

> **Note**
>
> AWS KMS admite el acceso multicuenta a las claves de KMS. Si un repositorio de ECR está cifrado con una clave de KMS que pertenece a otra cuenta, este control no realiza comprobaciones entre cuentas cuando evalúa el repositorio. El control no evalúa si Amazon ECR puede acceder y usar la clave al realizar operaciones criptográficas para el repositorio.

Corrección

No puede cambiar la configuración de cifrado de un repositorio de ECR existente. Sin embargo, puede especificar configuraciones de cifrado diferentes para los repositorios de ECR que cree posteriormente. Amazon ECR admite el uso de configuraciones de cifrado diferentes para repositorios individuales.

Para obtener más información sobre las opciones de cifrado para repositorios de ECR, consulte Cifrado en reposo en la Guía del usuario de Amazon ECR. Para obtener más información sobre la administración por el cliente AWS KMS keys, consulte AWS KMS keys la Guía para AWS Key Management Service desarrolladores.

Controles CSPM de Security Hub para Amazon ECS

Estos controles CSPM de Security Hub evalúan el servicio y los recursos de Amazon Elastic Container Service (Amazon ECS). Es posible que los controles no estén disponibles en todos. Regiones de AWS Para obtener más información, consulte Disponibilidad de los controles por región.

[ECS.2] Los servicios de ECS no deberían tener direcciones IP públicas asignadas automáticamente

Requisitos relacionados: NIST.800-53.r5 AC-21 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-6, (11) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), PCI DSS v4.0. 1/14.4.4

Categoría: Proteger > Configuración de red segura > Recursos no accesibles públicamente

Gravedad: alta

Tipo de recurso: `AWS::ECS::Service`

AWS Configregla: `ecs-service-assign-public-ip-disabled` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si los servicios de Amazon ECS están configurados para asignar direcciones IP públicas de forma automática. Este control tiene errores si `AssignPublicIP` figura como `ENABLED`. Este control se aprueba si `AssignPublicIP` figura como `DISABLED`.

Una dirección IP pública es una dirección IP a la que se puede tener acceso desde Internet. Si lanza sus instancias de Amazon ECS con una dirección IP pública, podrá acceder a sus instancias de Amazon ECS desde Internet. Los servicios de Amazon ECS no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a los servidores de aplicaciones contenedoras.

Corrección

En primer lugar, debe crear una definición de tareas para el clúster que utilice el modo de red `awsvpc` y especifique FARGATE para `requiresCompatibilities`. A continuación, para la configuración de cómputo, elija el Tipo de lanzamiento y FARGATE. Por último, en el campo Redes, desactive la IP pública para deshabilitar la asignación automática de IP pública para su servicio.

[ECS.3] Las definiciones de tareas de ECS no deben compartir el espacio de nombres del proceso del host

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Categoría: Identificar > Configuración de recursos

Gravedad: alta

Tipo de recurso: `AWS::ECS::TaskDefinition`

Regla de AWS Config: ecs-task-definition-pid-mode-check

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si las definiciones de tareas de Amazon ECS están configuradas para compartir el espacio de nombres de procesos de un host con sus contenedores. El control falla si la definición de la tarea comparte el espacio de nombres del proceso del host con los contenedores

que se ejecutan en él. Este control solo evalúa la última revisión activa de una definición de tarea de Amazon ECS.

Un espacio de nombres de ID de proceso (PID) proporciona separación entre los procesos. Evita que los procesos del sistema estén visibles y permite reutilizar los PID, incluido el PID 1. Si el espacio de nombres PID del host se comparte con los contenedores, los contenedores podrían ver todos los procesos del sistema anfitrión. Esto reduce la ventaja del aislamiento a nivel de proceso entre el host y los contenedores. Estas circunstancias podrían provocar el acceso no autorizado a los procesos del propio host, incluida la posibilidad de manipularlos y cancelarlos. Los clientes no deberían compartir el espacio de nombres de los procesos del anfitrión con los contenedores que se ejecuten en él.

Corrección

Para configurar el `pidMode` de la definición de una tarea, consulte Parámetros de definición de tareas en la Guía para desarrolladores de Amazon Elastic Container Service.

[ECS.4] Los contenedores ECS deben ejecutarse sin privilegios

Requisitos relacionados: NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7),, NIST.800-53.r5 AC-5 NIST.800-53.r5 AC-6

Categoría: Proteger > Gestión del acceso seguro > Restricciones de acceso para los usuarios raíz

Gravedad: alta

Tipo de recurso: `AWS::ECS::TaskDefinition`

Regla de AWS Config: ecs-containers-nonprivileged

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si el parámetro `privileged` de la definición de contenedor de las definiciones de tareas de Amazon ECS se establece como `true`. El control falla si este parámetro es igual a `true`. Este control solo evalúa la última revisión activa de una definición de tarea de Amazon ECS.

Le recomendamos que elimine los privilegios elevados de las definiciones de tareas de ECS. Cuando el parámetro de privilegio es `true`, al contenedor se le conceden privilegios elevados en la instancia de contenedor de host (similares a los de un usuario raíz).

Corrección

Para configurar el parámetro `privileged` en una definición de tarea, consulte Parámetros de definición avanzada de contenedor en la Guía para desarrolladores de Amazon Elastic Container Service.

[ECS.5] Las definiciones de tareas de ECS deben configurar los contenedores para que se limiten al acceso de solo lectura a los sistemas de archivos raíz

Requisitos relacionados: NIST.800-53.r5 AC-2 (1), (15) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7),, NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-5 NIST.800-53.r5 AC-6

Categoría: Proteger - Administración de acceso seguro

Gravedad: alta

Tipo de recurso: `AWS::ECS::TaskDefinition`

Regla de AWS Config: ecs-containers-readonly-access

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si las definiciones de tareas de ECS configuran los contenedores para que se limite al acceso de solo lectura a los sistemas de archivos raíz montados. El control falla si el `readonlyRootFilesystem` parámetro de las definiciones de contenedor de la definición de tareas de ECS está establecido en`false`, o si el parámetro no existe en la definición de contenedor dentro de la definición de tarea. Este control evalúa únicamente la última revisión activa de una definición de tarea de Amazon ECS.

Si el parámetro `readonlyRootFilesystem` está establecido en `true` en una definición de tarea de Amazon ECS, al contenedor de ECS se le concede acceso de solo lectura al sistema de archivos raíz. Esto reduce los vectores de ataque de seguridad, porque el sistema de archivos raíz de la instancia del contenedor no puede ser modificado ni escrito sin montajes de volúmenes explícitos que tengan permisos de lectura y escritura para carpetas y directorios del sistema de archivos. Habilitar esta opción también contribuye a aplicar el principio de privilegio mínimo.

> **Note**
>
> El `readonlyRootFilesystem` parámetro no es compatible con los contenedores de Windows. Las definiciones de tareas `runtimePlatform` configuradas para especificar una

familia de `WINDOWS_SERVER` sistemas operativos se marcan como `NOT_APPLICABLE` y no generarán resultados para este control.

Corrección

Para otorgar a un contenedor de Amazon ECS acceso de solo lectura a su sistema de archivos raíz, agregue el parámetro `readonlyRootFilesystem` a la definición de la tarea para el contenedor y establezca el valor del parámetro en `true`. Para obtener información sobre los parámetros de definición de tareas y cómo agregarlos a una definición de tarea, consulte Definiciones de tareas de Amazon ECS y Actualización de una definición de tarea en la Guía para desarrolladores de Amazon Elastic Container Service.

[ECS.8] Los secretos no deben transmitirse como variables de entorno de contenedores

Requisitos relacionados: NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, PCI DSS v4.0. 1/82.6.2

Categoría: Proteger > Desarrollo seguro > Credenciales no codificadas

Gravedad: alta

Tipo de recurso: `AWS::ECS::TaskDefinition`

Regla de AWS Config: ecs-no-environment-secrets

Tipo de horario: provocado por un cambio

Parámetros: `secretKeys`: `AWS_ACCESS_KEY_ID`,`AWS_SECRET_ACCESS_KEY`,`ECS_ENGINE_AUTH_DATA` (no personalizable)

Este control comprueba si el valor clave de alguna variable del parámetro `environment` de las definiciones de contenedores incluye `AWS_ACCESS_KEY_ID`, `AWS_SECRET_ACCESS_KEY`, o `ECS_ENGINE_AUTH_DATA`. Este control falla si una sola variable de entorno en cualquier definición de contenedor es igual a `AWS_ACCESS_KEY_ID`, `AWS_SECRET_ACCESS_KEY`, o `ECS_ENGINE_AUTH_DATA`. Este control no cubre las variables de entorno que se transmiten desde otras ubicaciones, como Amazon S3. Este control solo evalúa la última revisión activa de una definición de tarea de Amazon ECS.

AWS Systems ManagerParameter Store puede ayudarlo a mejorar la postura de seguridad de su organización. Le recomendamos que utilice el almacén de parámetros para almacenar los secretos y las credenciales en lugar de pasarlos directamente a las instancias contenedoras o codificarlos en el código.

Corrección

Para crear parámetros mediante SSM, consulte Creación de parámetros de Systems Manager en la Guía del usuario de AWS Systems Manager. Para obtener más información sobre cómo crear una definición de tarea que especifique un secreto, consulte Especificar datos confidenciales mediante Secrets Manager en la Guía para desarrolladores de Amazon Elastic Container Service.

[ECS.9] Las definiciones de tareas de ECS deben tener una configuración de registro

Requisitos relacionados: NIST.800-53.r5 AC-4 (26) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-7 (8)

Categoría: Identificar - Registro

Gravedad: alta

Tipo de recurso: `AWS::ECS::TaskDefinition`

Regla de AWS Config ecs-task-definition-log-configuration

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si la última definición de tarea activa de Amazon ECS tiene una configuración de registro especificada. El control falla si la definición de la tarea no tiene la propiedad definida `logConfiguration` o si el valor `logDriver` es null en al menos una definición de contenedor.

El registro le ayuda a mantener la fiabilidad, la disponibilidad y el rendimiento de Amazon ECS. La recopilación de datos de las definiciones de tareas proporciona visibilidad, lo que puede ayudarle a depurar los procesos y encontrar la causa raíz de los errores. Si utiliza una solución de registro que no tiene que estar definida en la definición de tareas de ECS (como una solución de registro de terceros), puede deshabilitar este control después de asegurarse de que los registros se capturan y entregan correctamente.

Corrección

Para definir una configuración de registro para las definiciones de tareas de Amazon ECS, consulte Especificar una configuración de registro en la definición de tareas de la Guía para desarrolladores de Amazon Elastic Container Service.

[ECS.10] Los servicios Fargate de ECS deberían ejecutarse en la última versión de la plataforma Fargate

Requisitos relacionados: NIST.800-53.r5 SI-2 (2) NIST.800-53.r5 SI-2, (4), NIST.800-53.r5 SI-2 NIST.800-53.r5 SI-2 (5), PCI DSS v4.0. 1/63.3.3

Categoría: Identificar > Administración de vulnerabilidades, parches y versiones

Gravedad: media

Tipo de recurso: `AWS::ECS::Service`

Regla de AWS Config: ecs-fargate-latest-platform-version

Tipo de horario: provocado por un cambio

Parámetros:

- `latestLinuxVersion: 1.4.0` (no personalizable)
- `latestWindowsVersion: 1.0.0` (no personalizable)

Este control comprueba si los servicios Fargate de Amazon ECS ejecutan la versión más reciente de la versión de la plataforma Fargate. Este control falla si la versión de la plataforma no es la más reciente.

AWS Fargatelas versiones de plataforma se refieren a un entorno de ejecución específico para la infraestructura de tareas de Fargate, que es una combinación de versiones de ejecución de kernel y contenedor. Se lanzan nuevas versiones de la plataforma a medida que evoluciona el tiempo de ejecución. Por ejemplo, se puede lanzar una nueva versión de kernel o del sistema operativo, características nuevas, correcciones de errores o actualizaciones de seguridad. Las actualizaciones y los parches de seguridad se implementan automáticamente para las tareas de Fargate. Si se detecta un problema de seguridad que afecte a una versión de la plataforma, corrija AWS la versión de la plataforma.

Corrección

Para actualizar un servicio existente, incluida su versión de la plataforma, consulte Actualización de un servicio en la Guía para desarrolladores de Amazon Elastic Container Service.

[ECS.12] Los clústeres de ECS deben usar Container Insights

Requisitos relacionados: NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4) NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-2

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: `AWS::ECS::Cluster`

Regla de AWS Config: ecs-container-insights-enabled

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si los clústeres de ECS utilizan Container Insights. Este control falla si Container Insights no está configurado para un clúster.

La monitorización es una parte importante del mantenimiento de la fiabilidad, la disponibilidad y el rendimiento de los clústeres de Amazon ECS. Utilice CloudWatch Container Insights para recopilar, agregar y resumir las métricas y los registros de sus aplicaciones y microservicios contenerizados. CloudWatch recopila automáticamente las métricas de muchos recursos, como la CPU, la memoria, el disco y la red. Información de contenedores también proporciona información de diagnóstico, como, por ejemplo, errores de reinicio de contenedores, para ayudarlo a aislar problemas y solucionarlos rápidamente. También puedes configurar CloudWatch alarmas en las métricas que recopila Container Insights.

Corrección

Para usar Container Insights, consulta Actualización de un servicio en la Guía del CloudWatch usuario de Amazon.

[ECS.13] Los servicios de ECS deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::ECS::Service`

AWS Configregla: `tagged-ecs-service` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si un servicio de Amazon ECS tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control falla si el servicio no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y falla si el servicio no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte Etiquetar sus AWS recursos en el. Referencia general de AWS

Corrección

Para agregar etiquetas a un servicio de ECS, consulte Etiquetado de los recursos de Amazon ECS en la Guía para desarrolladores de Amazon Elastic Container Service.

[ECS.14] Los clústeres de ECS deben etiquetarse

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::ECS::Cluster`

AWS Configregla: `tagged-ecs-cluster` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si un clúster de Amazon ECS tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza un error si el clúster no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si el clúster no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte Etiquetar sus AWS recursos en el. Referencia general de AWS

Corrección

Para agregar etiquetas a un clúster de ECS, consulte Etiquetado de los recursos de Amazon ECS en la Guía para desarrolladores de Amazon Elastic Container Service.

[ECS.15] Las definiciones de las tareas de ECS deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::ECS::TaskDefinition`

AWS Configregla: `tagged-ecs-taskdefinition` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si una definición de tarea de Amazon ECS tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control falla si la definición de la tarea no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y falla si la definición de la tarea no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan

operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte Etiquetar sus AWS recursos en el. Referencia general de AWS

Corrección

Para agregar etiquetas a una definición de tarea de ECS, consulte Etiquetado de los recursos de Amazon ECS en la Guía para desarrolladores de Amazon Elastic Container Service.

[ECS.16] Los conjuntos de tareas de ECS no deben asignar automáticamente direcciones IP públicas

Requisitos relacionados: PCI DSS v4.0. 1/14.4.4

Categoría: Proteger > Configuración de red segura > Recursos no accesibles públicamente

Gravedad: alta

Tipo de recurso: `AWS::ECS::TaskSet`

AWS Configregla: `ecs-taskset-assign-public-ip-disabled` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si los conjuntos de tareas de Amazon ECS están configurados para asignar direcciones IP públicas de forma automática. El control tiene errores si `AssignPublicIP` está configurado como `ENABLED`,

Una dirección IP pública es una dirección a la que se puede tener acceso desde Internet. Si configura el conjunto de tareas con una dirección IP pública, se puede acceder a los recursos asociados al conjunto de tareas desde Internet. Los conjuntos de tareas de ECS no deben ser de

acceso público, ya que esto podría permitir el acceso no deseado a los servidores de aplicaciones contenedoras.

Corrección

Para actualizar un conjunto de tareas de ECS para que no utilice una dirección IP pública, consulte Actualización de una definición de tareas de Amazon ECS mediante la consola en la Guía para desarrolladores de Amazon Elastic Container Service.

[ECS.17] Las definiciones de tareas de ECS no deben usar el modo de red host

Requisitos relacionados: NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-5, NIST.800-53.r5 AC-6

Categoría: Proteger - Configuración de red segura

Gravedad: media

Tipo de recurso: `AWS::ECS::TaskDefinition`

Regla de AWS Config: ecs-task-definition-network-mode-not-host

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control verifica si la última revisión activa de una definición de tarea de Amazon ECS utiliza el modo de red de `host`. El control falla si la última revisión activa de la definición de tarea de ECS usa el modo de red de `host`.

Cuando se usa el modo de red de `host`, la red de un contenedor de Amazon ECS está vinculada directamente al host subyacente que ejecuta el contenedor. Como consecuencia, este modo permite que los contenedores se conecten a los servicios de red de retrobucle privados del host y que puedan hacerse pasar por el propio host. Otros inconvenientes importantes son que no existe ninguna forma de reasignar un puerto del contenedor cuando se utiliza el modo de red `host`, y que no puede ejecutar más de una sola instanciación de una tarea en cada host.

Corrección

Para obtener información sobre los modos y las opciones de red para tareas de Amazon ECS que se alojan en instancias de Amazon EC2, consulte Opciones de redes de tareas de Amazon ECS para el tipo de lanzamiento de EC2 en la Guía del desarrollador de Amazon Elastic Container Service. Para

obtener información sobre cómo crear una nueva revisión de una definición de tarea y especificar un modo de red diferente, consulte Actualización de una definición de tarea de Amazon ECS en esa guía.

Si la definición de tarea de Amazon ECS la creóAWS Batch, consulte Modos de red para AWS Batch trabajos para obtener información sobre los modos de red y el uso típico de los tipos de AWS Batch trabajo y para elegir una opción segura.

[ECS.18] Las definiciones de tareas de ECS deben utilizar el cifrado en tránsito para los volúmenes de EFS

Categoría: Proteger > Cifrado de datos en tránsito

Gravedad: media

Tipo de recurso: `AWS::ECS::TaskDefinition`

Regla de AWS Config: ecs-task-definition-efs-encryption-enabled

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si la última revisión activa de una definición de tarea de Amazon ECS utiliza el cifrado en tránsito para los volúmenes de EFS. El control falla si la última revisión activa de la definición de tareas de ECS tiene el cifrado en tránsito deshabilitado para los volúmenes de EFS.

Los volúmenes de Amazon EFS proporcionan un almacenamiento de archivos compartido simple, escalable y persistente para usarlo en sus tareas de Amazon ECS. Amazon EFS admite el cifrado de datos en tránsito con seguridad de la capa de transporte (TLS). Cuando el cifrado de datos en tránsito se declara como una opción de montaje para su sistema de archivos de EFS, Amazon EFS establece una conexión TLS segura con su sistema de archivos de EFS al montarlo.

Corrección

Para obtener información sobre cómo habilitar el cifrado en tránsito para la definición de tareas de Amazon ECS con volúmenes de EFS, consulte el paso 5: Crear una definición de tarea en la Guía para desarrolladores de Amazon Elastic Container Service.

[ECS.19] Los proveedores de capacidad de ECS deberían tener habilitada la protección de terminación gestionada

Categoría: Proteger > Protección de datos

Gravedad: media

Tipo de recurso: `AWS::ECS::CapacityProvider`

Regla de AWS Config: ecs-capacity-provider-termination-check

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un proveedor de capacidad de Amazon ECS ha activado la protección de terminación gestionada. El control falla si la protección de terminación administrada no está habilitada en un proveedor de capacidad de ECS.

Los proveedores de capacidad de Amazon ECS administran el escalado de la infraestructura para las tareas de los clústeres. Cuando utiliza instancias de Amazon EC2 para su capacidad, utiliza grupos de escalado automático para administrar las instancias de Amazon EC2. La protección contra la terminación administrada permite que el escalado automático de clústeres controle qué instancias se terminan. Cuando utiliza la protección contra la terminación administrada, Amazon ECS solo termina las instancias de EC2 que no tienen ninguna tarea de Amazon ECS en ejecución.

> **Note**
>
> Cuando se utiliza la protección de terminación administrada, también se debe usar el escalado administrado, porque, de lo contrario, la protección de terminación administrada no funciona.

Corrección

Para habilitar la protección de terminación administrada para un proveedor de capacidad de Amazon ECS, consulte Actualización de la protección de terminación administrada para los proveedores de capacidad de Amazon ECS en la Guía para desarrolladores de Amazon Elastic Container Service.

[ECS.20] Las definiciones de tareas de ECS deben configurar a los usuarios no root en las definiciones de contenedores de Linux

Categoría: Proteger > Gestión del acceso seguro > Restricciones de acceso para los usuarios raíz

Gravedad: media

Tipo de recurso: `AWS::ECS::TaskDefinition`

Regla de AWS Config: ecs-task-definition-linux-user-non-root

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si la última revisión activa de una definición de tarea de Amazon ECS configura los contenedores de Linux para que se ejecuten como usuarios no root. El control falla si hay configurado un usuario root predeterminado o si no hay ninguna configuración de usuario para algún contenedor.

Cuando los contenedores de Linux se ejecutan con privilegios de root, presentan varios riesgos de seguridad importantes. Los usuarios root tienen acceso ilimitado al contenedor. Este acceso elevado aumenta el riesgo de que se produzcan ataques de escape de contenedores, en los que un atacante podría romper el aislamiento del contenedor y acceder al sistema host subyacente. Si un contenedor que funciona como root se ve comprometido, los atacantes podrían aprovecharlo para acceder a los recursos del sistema anfitrión o modificarlos, lo que afectaría a otros contenedores o al propio host. Además, el acceso root podría permitir ataques de escalada de privilegios, lo que permitiría a los atacantes obtener permisos adicionales más allá del alcance previsto para el contenedor. El parámetro de usuario de las definiciones de tareas de ECS puede especificar los usuarios en varios formatos, como el nombre de usuario, el ID de usuario, el nombre de usuario con grupo o el UID con ID de grupo. Es importante tener en cuenta estos diversos formatos al configurar las definiciones de tareas para garantizar que no se conceda ningún acceso root por error. Siguiendo el principio de privilegios mínimos, los contenedores deben ejecutarse con los permisos mínimos requeridos y utilizarlos para usuarios que no sean root. Este enfoque reduce considerablemente la posible superficie de ataque y mitiga el impacto de las posibles infracciones de seguridad.

> **Note**
>
> Este control solo evalúa las definiciones de contenedor en una definición de tarea si `operatingSystemFamily` está configurado `LINUX` o `operatingSystemFamily` no en la definición de tarea. El control generará un `FAILED` resultado para una definición de tarea evaluada si alguna de las definiciones de contenedor de la definición de tarea `user` no se ha configurado o `user` configurado como usuario root predeterminado. Los usuarios raíz predeterminados de los `LINUX` contenedores son `"root"` y`"0"`.

Corrección

Para obtener información sobre la creación de una nueva revisión de una definición de tarea de Amazon ECS y la actualización del `user` parámetro en la definición del contenedor, consulte Actualización de una definición de tarea de Amazon ECS en la Guía para desarrolladores de Amazon Elastic Container Service.

[ECS.21] Las definiciones de tareas de ECS deberían configurar a los usuarios no administradores en las definiciones de contenedores de Windows

Categoría: Proteger > Gestión del acceso seguro > Restricciones de acceso para los usuarios raíz

Gravedad: media

Tipo de recurso: `AWS::ECS::TaskDefinition`

Regla de AWS Config: ecs-task-definition-windows-user-non-admin

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si la última revisión activa de una definición de tarea de Amazon ECS configura los contenedores de Windows para que se ejecuten como usuarios que no son administradores predeterminados. El control falla si un administrador predeterminado está configurado como usuario o si no hay ninguna configuración de usuario en ningún contenedor.

Cuando los contenedores de Windows se ejecutan con privilegios de administrador, presentan varios riesgos de seguridad importantes. Los administradores tienen acceso ilimitado al contenedor. Este acceso elevado aumenta el riesgo de que se produzcan ataques de escape de contenedores, en los que un atacante podría romper el aislamiento del contenedor y acceder al sistema host subyacente.

> **Note**
>
> Este control solo evalúa las definiciones de contenedor en una definición de tarea si `operatingSystemFamily` está configurado `WINDOWS_SERVER` o `operatingSystemFamily` no en la definición de tarea. El control generará un `FAILED` resultado para una definición de tarea evaluada si alguna definición de contenedor de la definición de tarea `user` no se ha configurado o `user` configurado como administrador predeterminado para `WINDOWS_SERVER` los contenedores, es `"containeradministrator"` decir.

Corrección

Para obtener información sobre la creación de una nueva revisión de una definición de tarea de Amazon ECS y la actualización del `user` parámetro en la definición del contenedor, consulte Actualización de una definición de tarea de Amazon ECS en la Guía para desarrolladores de Amazon Elastic Container Service.

Controles de CSPM de Security Hub para Amazon EFS

Estos controles CSPM de Security Hub evalúan el servicio y los recursos de Amazon Elastic File System (Amazon EFS). Es posible que los controles no estén disponibles en todos los casos. Regiones de AWS Para obtener más información, consulte Disponibilidad de los controles por región.

[EFS.1] Elastic File System debe configurarse para cifrar los datos de los archivos en reposo mediante AWS KMS

Requisitos relacionados: CIS AWS Foundations Benchmark v5.0. 0/2.3.1, CIS AWS Foundations Benchmark v3.0. 0/2.4.1, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6) NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28 (1) NIST.800-53.r5 SC-28, (10), NIST.800-53.r5 SC-7 (6) NIST.800-53.r5 SI-7

Categoría: Proteger > Protección de datos > Cifrado de datos en reposo

Gravedad: media

Tipo de recurso: `AWS::EFS::FileSystem`

Regla de AWS Config : efs-encrypted-check

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si Amazon Elastic File System está configurado para cifrar los datos del archivo mediante. AWS KMS La comprobación falla en los siguientes casos.

- `Encrypted` se establece en `false` en la respuesta de `DescribeFileSystems`.
- La clave `KmsKeyId` de la respuesta de `DescribeFileSystems` no coincide con el parámetro `KmsKeyId` de `efs-encrypted-check`.

Tenga en cuenta que este control no utiliza el parámetro `KmsKeyId` para `efs-encrypted-check`. Solo comprueba el valor de `Encrypted`.

Para añadir un nivel de seguridad a sus datos confidenciales en Amazon EFS, debe crear sistemas de archivos cifrados. Amazon EFS admite el cifrado de sistemas de archivos en reposo. Puede habilitar el cifrado de datos en reposo cuando cree un sistema de archivos de Amazon EFS. Para obtener más información acerca del cifrado de Amazon EFS, consulte Cifrado de datos en Amazon EFS en la Guía del usuario de Amazon Elastic File System.

Corrección

Para obtener información detallada sobre cómo cifrar un nuevo sistema de archivos de Amazon EFS, consulte Cifrado de datos en reposo en la Guía del usuario de Amazon Elastic File System.

[EFS.2] Los volúmenes de Amazon EFS deben figurar en los planes de copia de seguridad

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6 (1), NIST.800-53.r5 CP-6 (2) NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2) NIST.800-53.r5 SI-12, NIST.800-53.r5 SI-13 (5)

Categoría: Recuperación > Resiliencia > Backup

Gravedad: media

Tipo de recurso: `AWS::EFS::FileSystem`

Regla de AWS Config : efs-in-backup-plan

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si los sistemas de archivos de Amazon Elastic File System (Amazon EFS) se han agregado a los planes de copia de seguridad en AWS Backup. El control falla si los sistemas de archivos Amazon EFS no están incluidos en los planes de backup.

La inclusión de los sistemas de archivos EFS en los planes de copia de seguridad le ayuda a proteger sus datos contra la eliminación y la pérdida de datos.

Corrección

Para habilitar las copias de seguridad automáticas para un sistema de archivos Amazon EFS existente, consulte Introducción 4: Creación de copias de seguridad automáticas de Amazon EFS en la Guía para desarrolladores de AWS Backup .

[EFS.3] Los puntos de acceso EFS deben exigir un directorio raíz

Requisitos relacionados: NIST.800-53.r5 AC-6 (10)

Categoría: Proteger - Administración de acceso seguro

Gravedad: media

Tipo de recurso: `AWS::EFS::AccessPoint`

Regla de AWS Config : efs-access-point-enforce-root-directory

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si los puntos de acceso de Amazon EFS están configurados para aplicar un directorio raíz. El control falla si el valor `Path` se establece como `/` (el directorio raíz predeterminado del sistema de archivos).

Cuando se aplica un directorio raíz, el cliente NFS que utiliza el punto de acceso utiliza el directorio raíz configurado en el punto de acceso en lugar del directorio raíz del sistema de archivos. La aplicación de un directorio raíz para un punto de acceso ayuda a restringir el acceso a los datos, ya que garantiza que los usuarios del punto de acceso solo puedan acceder a los archivos del subdirectorio especificado.

Corrección

Para obtener instrucciones sobre cómo aplicar un directorio raíz para un punto de acceso de Amazon EFS, consulte Aplicación de un directorio raíz con un punto de acceso en la Guía del usuario de Amazon Elastic File System.

[EFS.4] Los puntos de acceso EFS deben exigir la identidad del usuario

Requisitos relacionados: NIST.800-53.r5 AC-6 (2), PCI DSS v4.0. 1/73.3.1

Categoría: Proteger - Administración de acceso seguro

Gravedad: media

Tipo de recurso: `AWS::EFS::AccessPoint`

Regla de AWS Config : efs-access-point-enforce-user-identity

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si los puntos de acceso de Amazon EFS están configurados para imponer la identidad de un usuario. Este control falla si no se define una identidad de usuario POSIX al crear el punto de acceso EFS.

Los puntos de accesode Amazon EFS son puntos de entrada específicos que la aplicación utiliza para acceder a un sistema de archivos de EFS y que facilitan la administración del acceso de las aplicaciones a conjuntos de datos compartidos. Los puntos de acceso pueden imponer una identidad de usuario, incluidos los grupos POSIX del usuario, para todas las solicitudes del sistema de archivos que se realizan a través del punto de acceso. Los puntos de acceso también pueden imponer un directorio raíz diferente para el sistema de archivos, de modo que los clientes solo puedan acceder a los datos del directorio especificado o de sus subdirectorios.

Corrección

Para hacer cumplir la identidad de un usuario para un punto de acceso de Amazon EFS, consulte Imponer una identidad de usuario mediante un punto de acceso en la Guía del usuario de Amazon Elastic File System.

[EFS.5] Los puntos de acceso EFS deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::EFS::AccessPoint`

AWS Config regla: `tagged-efs-accesspoint` (regla CSPM personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub CSPM
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si un punto de acceso de Amazon EFS tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza error si el punto de acceso no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si el punto de acceso no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y se compone de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWSen la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Las etiquetas son accesibles para muchos Servicios de AWS, incluso AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulta Cómo etiquetar tus AWS recursos en. Referencia general de AWS

Corrección

Para agregar etiquetas a un punto de acceso de EFS, consulte Tagging Amazon EFS resources en la Guía del usuario de Amazon Elastic File System.

[EFS.6] Los destinos de montaje de EFS no deben asociarse a subredes que asignan direcciones IP públicas en el momento del lanzamiento

Requisitos relacionados: NIST.800-171.r2 3.1.20 NIST.800-53.r5 SC-7, PCI DSS v4.0. 1/14.4.4

Categoría: Proteger > Seguridad de red > Recursos no accesibles públicamente

Gravedad: media

Tipo de recurso: `AWS::EFS::FileSystem`

Regla de AWS Config : efs-mount-target-public-accessible

Tipo de programa: Periódico

Parámetros: ninguno

Esta comprobación verifica si un destino de montaje de Amazon EFS está asociado a subredes que asignan direcciones IP públicas durante el lanzamiento. El control falla si el destino de montaje está asociado a subredes que asignan direcciones IP públicas durante el lanzamiento.

Las subredes tienen atributos que determinan si las interfaces de red creadas en la subred reciben automáticamente direcciones IP públicas. En IPv4, el `MapPublicIpOnLaunch` atributo se establece como para las subredes predeterminadas y `TRUE` `FALSE` para las subredes no predeterminadas (con la excepción de las subredes no predeterminadas creadas mediante el asistente de lanzamiento de instancias de EC2, donde se establece en). `TRUE` Para IPv6, el `AssignIpv6AddressOnCreation` atributo está establecido en todas las subredes de forma predeterminada. `FALSE`

Si bien a los destinos de montaje de Amazon EFS no se les pueden asignar direcciones IPv4 públicas, colocarlos en subredes configuradas para asignar direcciones IP públicas al lanzarlos indica que las instancias de ubicación conjunta lanzadas en esas subredes que puedan montar el sistema de archivos EFS podrían recibir automáticamente direcciones IP públicas, lo que podría correr el riesgo de que los datos del sistema de archivos fueran accesibles desde los hosts con direcciones públicas.

Los destinos montados en subredes que tengan habilitada la asignación automática de direcciones IPv6 públicas pueden recibir direcciones IPv6 enrutables globalmente.

> **Note**
>
> El 3 de agosto de 2026, Security Hub CSPM retiró este control del estándar Fundational Security Best Practices (FSBP). AWS Este control estará disponible en el estándar NIST SP 800-53 Rev. 5, el estándar NIST SP 800-171 Revisión 2 y el estándar PCI DSS v4.0.1. https://docs.aws.amazon.com/securityhub/latest/userguide/pci-standard.html

Corrección

Para asociar un destino de montaje existente a una subred diferente, debe crear un nuevo destino de montaje en una subred que no asigne direcciones IP públicas en el lanzamiento y luego eliminar el destino de montaje anterior. Para obtener información acerca de la administración de destinos de montaje, consulte Creación y administración de destinos de montaje y grupos de seguridad en la Guía del usuario de Amazon Elastic File System.

[] Los sistemas de archivos EFS deben tener habilitadas las copias de seguridad automáticas EFS.7

Categoría: Recuperación > Resiliencia > Respaldos habilitados

Gravedad: media

Tipo de recurso: `AWS::EFS::FileSystem`

Regla de AWS Config : efs-automatic-backups-enabled

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un sistema de archivos de Amazon EFS tiene habilitadas las copias de seguridad automáticas. Este control lanza error si el sistema de archivos de EFS no tiene habilitadas las copias de seguridad automáticas.

Una copia de seguridad de datos es una copia de los datos del sistema, la configuración o la aplicación que se almacena por separado del original. La habilitación de copias de seguridad periódicas ayuda a proteger los datos valiosos frente a eventos imprevistos, como errores del sistema, ciberataques o eliminaciones accidentales. Contar con una estrategia de copia de seguridad sólida también permite una recuperación más rápida, una continuidad empresarial y brinda tranquilidad frente a una posible pérdida de datos.

Corrección

Para obtener información sobre el uso AWS Backup de sistemas de archivos EFS, consulte la sección Cómo hacer copias de seguridad de los sistemas de archivos EFS en la Guía del usuario de Amazon Elastic File System.

[EFS.8] Los sistemas de archivos EFS deben cifrarse en reposo

Requisitos relacionados: CIS AWS Foundations Benchmark v5.0. 0/23.3.1

Categoría: Proteger > Protección de datos > Cifrado de datos en reposo

Gravedad: media

Tipo de recurso: `AWS::EFS::FileSystem`

Regla de AWS Config : efs-filesystem-ct-encrypted

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un sistema de archivos Amazon EFS cifra los datos con AWS Key Management Service ()AWS KMS. El control lanza error si un sistema de archivos no está cifrado.

Los datos en reposo hacen referencia a los datos que se almacenan en un almacenamiento persistente y no volátil durante cualquier periodo de tiempo. El cifrado de datos en reposo permite proteger la confidencialidad de los datos, lo que reduce el riesgo de que un usuario no autorizado pueda acceder a ellos.

Corrección

Para habilitar el cifrado en reposo para un sistema de archivos de EFS nuevo, consulte Cifrado de datos en reposo en la Guía del usuario de Amazon Elastic File System.

Controles de CSPM de Security Hub para Amazon EKS

Estos controles CSPM de Security Hub evalúan el servicio y los recursos de Amazon Elastic Kubernetes Service (Amazon EKS). Es posible que los controles no estén disponibles en todos los casos. Regiones de AWS Para obtener más información, consulte Disponibilidad de los controles por región.

[EKS.1] Los puntos finales del clúster EKS no deben ser de acceso público

Requisitos relacionados: NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7 (11) NIST.800-53.r5 SC-7, (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), PCI DSS v4.0. 1/14.4.4

Categoría: Proteger > Configuración de red segura > Recursos no accesibles públicamente

Gravedad: alta

Tipo de recurso: `AWS::EKS::Cluster`

Regla de AWS Config : eks-endpoint-no-public-access

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si un punto de conexión de un clúster de Amazon EKS es de acceso público. El control falla si un clúster de EKS tiene un punto de conexión al que se puede acceder públicamente.

Cuando crea un clúster nuevo, Amazon EKS genera un punto de conexión para el servidor de la API de Kubernetes administrado que utiliza a fin de comunicarse con su clúster. De forma predeterminada, este punto de conexión del servidor API está disponible públicamente en Internet. El acceso al servidor de API está protegido mediante una combinación de AWS Identity and Access Management (IAM) y un control de acceso basado en funciones (RBAC) nativo de Kubernetes. Al

eliminar el acceso público al punto de conexión, puede evitar la exposición y el acceso involuntarios a su clúster.

Corrección

Para modificar el acceso a los puntos de conexión de un clúster de EKS existente, consulte Modificación del acceso a los puntos de conexión de un clúster en la Guía del usuario de Amazon EKS. Puede configurar el acceso a los puntos de conexión para un nuevo clúster de EKS al crearlo. Para obtener instrucciones sobre cómo crear un nuevo clúster de Amazon EKS, consulte Creación de un clúster de Amazon EKS en la Guía del usuario de Amazon EKS.

[EKS.2] Los clústeres de EKS deben ejecutarse en una versión de Kubernetes compatible

Requisitos relacionados: NIST.800-53.r5 CA-9 (1),, NIST.800-53.r5 CM-2, NIST.800-53.r5 SI-2 (2) NIST.800-53.r5 SI-2, (4), NIST.800-53.r5 SI-2 NIST.800-53.r5 SI-2 (5), PCI DSS v4.0. 1/12.3.4

Categoría: Identificar > Administración de vulnerabilidades, parches y versiones

Gravedad: alta

Tipo de recurso: `AWS::EKS::Cluster`

Regla de AWS Config : eks-cluster-supported-version

Tipo de horario: provocado por un cambio

Parámetros:

- `oldestVersionSupported`: `1.34` (no personalizable)

Este control comprueba si un clúster de Amazon Elastic Kubernetes Service (Amazon EKS) se ejecuta en una versión de Kubernetes de soporte estándar. El control falla si el clúster de Amazon EKS se ejecuta en una versión de soporte extendido o no compatible.

Si su aplicación no requiere una versión específica de Kubernetes, recomendamos que use la versión más reciente de Kubernetes disponible admitida por EKS para sus clústeres. Para obtener más información, consulte Calendario de versiones de Amazon EKS Kubernetes y Comprensión del ciclo de vida de versiones de Kubernetes en Amazon EKS en la Guía del usuario de Amazon EKS.

Corrección

Para actualizar un clúster de EKS, consulte Actualización de un clúster existente a una nueva versión de Kubernetes en la Guía del usuario de Amazon EKS.

[EKS.3] Los clústeres de EKS deben usar secretos de Kubernetes cifrados

Requisitos relacionados: NIST.800-53.r5 SC-8,, NIST.800-53.r5 SC-12 NIST.800-53.r5 SC-13, PCI DSS NIST.800-53.r5 SC-28 v4.0. 1/8.3.2

Categoría: Proteger > Protección de datos > Cifrado de datos en reposo

Gravedad: media

Tipo de recurso: `AWS::EKS::Cluster`

Regla de AWS Config : eks-cluster-secrets-encrypted

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si un clúster de Amazon EKS utiliza secretos de Kubernetes cifrados. El control lanza un error si los secretos de Kubernetes del clúster no están cifrados.

Al cifrar secretos, puedes usar claves AWS Key Management Service (AWS KMS) para cifrar en sobres los secretos de Kubernetes almacenados en etcd para tu clúster. Este cifrado se suma al cifrado de volúmenes de EBS, que está habilitado de forma predeterminada para todos los datos (incluidos los secretos) que se almacenan en etcd como parte de un clúster de EKS. El uso del cifrado de secretos para su clúster de EKS le permite implementar una estrategia de defensa exhaustiva para las aplicaciones de Kubernetes mediante el cifrado de los secretos de Kubernetes con una clave de KMS que usted defina y administre.

> **Note**
>
> Este control se retirará después del 10 de agosto de 2026 y se eliminará de todos los estándares CSPM de Security Hub aplicables. A partir de la versión 1.28 de Kubernetes, los clústeres de Amazon EKS protegen los secretos de Kubernetes mediante el cifrado de sobres de forma predeterminada.

Corrección

Para habilitar el cifrado de secretos en un clúster de EKS, consulte Habilitar el cifrado de secretos en un clúster existente en la Guía del usuario de Amazon EKS.

[] Los clústeres de EKS deben etiquetarse EKS.6

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::EKS::Cluster`

AWS Config regla: `tagged-eks-cluster` (regla CSPM personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub CSPM
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si un clúster de Amazon EKS tiene etiquetas con claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza un error si el clúster no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si el clúster no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y se compone de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los

propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWSen la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Las etiquetas son accesibles para muchos Servicios de AWS, incluso AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulta Cómo etiquetar tus AWS recursos en. Referencia general de AWS

Corrección

Para agregar etiquetas a un clúster de EKS, consulte Etiquetado de los recursos de Amazon EKS en la Guía del usuario de Amazon EKS.

[EKS.7] Las configuraciones del proveedor de identidad de EKS deben etiquetarse

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::EKS::IdentityProviderConfig`

AWS Config regla: `tagged-eks-identityproviderconfig` (regla CSPM personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub CSPM
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si una configuración de los proveedores de identidad de Amazon EKS tiene etiquetas con claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza un error si la configuración no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si la configuración no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y se compone de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWSen la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Las etiquetas son accesibles para muchos Servicios de AWS, incluso AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulta Cómo etiquetar tus AWS recursos en. Referencia general de AWS

Corrección

Para agregar etiquetas a las configuraciones de los proveedores de identidad de EKS, consulte Etiquetado de los recursos de Amazon EKS en la Guía del usuario de Amazon EKS.

[EKS.8] Los clústeres de EKS deben tener habilitado el registro de auditoría

Requisitos relacionados: NIST.800-53.r5 AC-2 (12), NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 AU-9 (7) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-3 (8), (20) NIST.800-53.r5 SI-4, NIST.800-53.r5 SI-4 NIST.800-53.r5 SI-7 (8), PCI DSS v4.0. 1/10.2.1

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: `AWS::EKS::Cluster`

Regla de AWS Config : eks-cluster-log-enabled

Tipo de horario: provocado por un cambio

Parámetros:

- `logTypes: audit` (no personalizable)

Este control comprueba si un clúster de Amazon EKS tiene habilitado el registro de auditoría. Se produce un error en el control si el registro de auditoría no está habilitado para el clúster.

> **Note**
>
> Este control no comprueba si el registro de auditoría de Amazon EKS está habilitado a través de Amazon Security Lake para la Cuenta de AWS.

El registro del plano de control de EKS proporciona los registros de auditoría y diagnóstico directamente desde el plano de control de EKS a CloudWatch los registros de Amazon de su cuenta. Puede seleccionar los tipos de registro que necesita y los registros se envían como secuencias de registros a un grupo por cada clúster de EKS en el que se encuentre CloudWatch. El registro proporciona visibilidad del acceso y el rendimiento de los clústeres de EKS. Al enviar los registros del plano de control de EKS de sus clústeres de EKS a CloudWatch Logs, puede registrar las operaciones con fines de auditoría y diagnóstico en una ubicación central.

Corrección

Para habilitar los registros de auditoría para el clúster de EKS, consulte Habilitación y deshabilitación de registros de plano de control en la Guía del usuario de Amazon EKS.

[EKS.9] Los grupos de nodos de EKS deben ejecutarse en una versión de Kubernetes compatible

Categoría: Identificar > Administración de vulnerabilidades, parches y versiones

Gravedad: alta

Tipo de recurso: `AWS::EKS::Nodegroup`

Regla de AWS Config : eks-nodegroup-supported-version-check

Tipo de horario: provocado por un cambio

Parámetros:

- `oldestVersionSupported`: `1.34` (no personalizable)

Este control comprueba si un grupo de nodos de Amazon EKS se ejecuta en una versión estándar de Kubernetes compatible. El control falla si el grupo de nodos de Amazon EKS se ejecuta en una versión de soporte extendido o no compatible.

La ejecución de grupos de nodos de EKS en versiones de Kubernetes no compatibles significa que esos nodos ya no reciben parches de seguridad, correcciones de errores ni actualizaciones de

compatibilidad. AWS Las versiones no compatibles pueden contener vulnerabilidades conocidas que se han corregido en las versiones más recientes, y pueden presentar problemas de compatibilidad con las imágenes de contenedor actualizadas Servicios de AWS y las herramientas de terceros del ecosistema de Kubernetes. Si su aplicación no requiere una versión específica de Kubernetes, le recomendamos que utilice la última versión de Kubernetes disponible que sea compatible con Amazon EKS para sus grupos de nodos. Para obtener más información, consulte el calendario de lanzamientos de Kubernetes de Amazon EKS y conozca cada fase de las actualizaciones de los nodos en la guía del usuario de Amazon EKS.

Corrección

Para actualizar un grupo de nodos de EKS, consulte Actualizar un grupo de nodos gestionado para su clúster en la guía del usuario de Amazon EKS.

Controles CSPM de Security Hub para ElastiCache

Estos AWS Security Hub CSPM controles evalúan el ElastiCache servicio y los recursos de Amazon. Es posible que los controles no estén disponibles en todosRegiones de AWS. Para obtener más información, consulte Disponibilidad de los controles por región.

[ElastiCache.1] ElastiCache (Redis OSS) los clústeres deben tener habilitadas las copias de seguridad automáticas

Requisitos relacionados: NIST.800-53.r5 CP-10 NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6 (1), NIST.800-53.r5 CP-6 (2) NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2) NIST.800-53.r5 SI-12, NIST.800-53.r5 SI-13 (5)

Categoría: Recuperación > Resiliencia > Respaldos habilitados

Gravedad: alta

Tipo de recurso: `AWS::ElastiCache::CacheCluster`, `AWS:ElastiCache:ReplicationGroup`

Regla de AWS Config: elasticache-redis-cluster-automatic-backup-check

Tipo de programa: Periódico

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`snapshotRetentionPeriod`	Periodo mínimo de retención de instantáneas en días	Entero	De 1 a 35	1

Este control evalúa si un clúster de Amazon ElastiCache (Redis OSS) tiene habilitadas las copias de seguridad automáticas. El control falla si el `SnapshotRetentionLimit` para el clúster de Redis OSS es inferior al periodo de tiempo especificado. A menos que proporciones un valor de parámetro personalizado para el período de retención de instantáneas, Security Hub CSPM utiliza un valor predeterminado de 1 día.

ElastiCache (Redis OSS) los clústeres pueden hacer copias de seguridad de sus datos. Puede utilizar la característica de copia de seguridad para restaurar un clúster o para propagar datos en un nuevo clúster. La copia de seguridad consiste en los metadatos del clúster, junto con todos los datos del clúster. Todas las copias de seguridad se escriben en Amazon S3, que proporciona un almacenamiento duradero. Puede restaurar los datos creando un nuevo ElastiCache clúster y rellenándolo con los datos de una copia de seguridad. Puede gestionar las copias de seguridad mediante la Consola de administración de AWSAWS CLI, la y la ElastiCache API.

> **Note**
>
> Este control también evalúa los grupos de ElastiCache replicación (Redis OSS y Valkey).

Corrección

Para obtener información sobre la programación de copias de seguridad automáticas para un ElastiCache clúster, consulte Programar copias de seguridad automáticas en la Guía del ElastiCache usuario de Amazon.

[ElastiCache.2] ElastiCache los clústeres deberían tener habilitadas las actualizaciones automáticas de las versiones secundarias

Requisitos relacionados: NIST.800-53.r5 SI-2 NIST.800-53.r5 SI-2 (2), NIST.800-53.r5 SI-2 (4), NIST.800-53.r5 SI-2 (5) PCI DSS v4.0. 1/63.3.3

Categoría: Identificar > Administración de vulnerabilidades, parches y versiones

Gravedad: alta

Tipo de recurso: `AWS::ElastiCache::CacheCluster`

Regla de AWS Config: elasticache-auto-minor-version-upgrade-check

Tipo de programa: Periódico

Parámetros: ninguno

Este control evalúa si Amazon aplica ElastiCache automáticamente las actualizaciones de versiones menores a un clúster de caché. El control falla si el clúster de caché no tiene habilitadas las actualizaciones automáticas de versiones secundarias.

> **Note**
>
> Este control no se aplica a los clústeres de ElastiCache Memcached.

La actualización automática de versiones secundarias es una función que puedes activar en Amazon ElastiCache para actualizar automáticamente tus clústeres de caché cuando haya disponible una nueva versión del motor de caché secundaria. Estas actualizaciones pueden incluir parches de seguridad y correcciones de errores. Mantenerse al día con la instalación de los parches es un paso importante para proteger los sistemas.

Corrección

Para aplicar automáticamente actualizaciones de versiones menores a un clúster de ElastiCache caché existente, consulte Gestión de versiones ElastiCache en la Guía del ElastiCache usuario de Amazon.

[ElastiCache.3] los grupos de ElastiCache replicación deberían tener habilitada la conmutación por error automática

Requisitos relacionados: NIST.800-53.r5 CP-10 NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoría: Recuperación > Resiliencia > Alta disponibilidad

Gravedad: media

Tipo de recurso: `AWS::ElastiCache::ReplicationGroup`

Regla de AWS Config: elasticache-repl-grp-auto-failover-enabled

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si un grupo de ElastiCache réplicas tiene habilitada la conmutación por error automática. El control falla si la conmutación por error automática no está habilitada para un grupo de replicación.

Cuando se habilita la conmutación por error automática para un grupo de replicación, la característica del nodo principal tendrá una conmutación por error automática en una de las réplicas de lectura. Esta conmutación por error y promoción de réplica garantizan que pueda reanudar la escritura en la réplica principal tan pronto como se complete la promoción, lo cual reduce el tiempo de inactividad general en caso de falla.

Corrección

Para habilitar la conmutación por error automática para un grupo de ElastiCache replicación existente, consulte Modificación de un ElastiCache clúster en la Guía del ElastiCache usuario de Amazon. Si utiliza la ElastiCache consola, active la conmutación por error automática.

[ElastiCache.4] los grupos de ElastiCache replicación deben cifrarse en reposo

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6) NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6)

Categoría: Proteger > Protección de datos > Cifrado de datos en reposo

Gravedad: media

Tipo de recurso: `AWS::ElastiCache::ReplicationGroup`

Regla de AWS Config: elasticache-repl-grp-encrypted-at-rest

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si un grupo de ElastiCache replicación está cifrado en reposo. El control falla si el grupo de replicación no está cifrado en reposo.

El cifrado de los datos en reposo reduce el riesgo de que un usuario no autenticado acceda a los datos almacenados en el disco. ElastiCache Los grupos de replicación (Redis OSS) deben cifrarse en reposo para ofrecer un nivel de seguridad adicional.

Corrección

Para configurar el cifrado en reposo en un grupo de ElastiCache replicación, consulte Habilitar el cifrado en reposo en la Guía ElastiCache del usuario de Amazon.

[ElastiCache.5] los grupos de ElastiCache replicación deben cifrarse en tránsito

Requisitos relacionados: NIST.800-53.r5 AC-17 (2) NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), NIST.800-53.r5 SC-12 (3) NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23 (3) NIST.800-53.r5 SC-23, (4), NIST.800-53.r5 SC-7 (1) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SC-8 NIST.800-53.r5 SI-7 (6), PCI DSS v4.0. 1/42.2.1

Categoría: Proteger > Protección de datos > Cifrado de datos en tránsito

Gravedad: media

Tipo de recurso: `AWS::ElastiCache::ReplicationGroup`

Regla de AWS Config: elasticache-repl-grp-encrypted-in-transit

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si un grupo de ElastiCache replicación está cifrado en tránsito. El control falla si el grupo de replicación no está cifrado en tránsito.

El cifrado de los datos en tránsito reduce el riesgo de que un usuario no autorizado pueda espiar el tráfico de la red. Al habilitar el cifrado en tránsito en un grupo de ElastiCache replicación, se cifran los

datos siempre que se mueven de un lugar a otro, por ejemplo, entre los nodos del clúster o entre el clúster y la aplicación.

Corrección

Para configurar el cifrado en tránsito en un grupo de ElastiCache replicación, consulte Habilitar el cifrado en tránsito en la Guía ElastiCache del usuario de Amazon.

[ElastiCache.6] ElastiCache (Redis OSS) Los grupos de replicación de versiones anteriores deberían tener habilitada la autenticación de Redis OSS

Requisitos relacionados: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-6, PCI DSS v4.0. 1/83.3.1

Categoría: Proteger - Administración de acceso seguro

Gravedad: media

Tipo de recurso: `AWS::ElastiCache::ReplicationGroup`

Regla de AWS Config: elasticache-repl-grp-redis-auth-enabled

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si un grupo de replicación ElastiCache (Redis OSS) tiene habilitada la autenticación de Redis OSS. Se produce un error en el control si la versión de Redis OSS de los nodos del grupo de replicación es inferior a la 6.0 y `AuthToken` no está en uso.

Cuando utiliza los tokens de autenticación o contraseñas de Redis, Redis solicita una contraseña antes de permitir que los clientes ejecuten comandos, lo cual mejora la seguridad de los datos. Para Redis 6.0 y versiones posteriores, recomendamos utilizar el control de Role-Based acceso (RBAC). Como el RBAC no es compatible con las versiones de Redis anteriores a la 6.0, este control solo evalúa las versiones que no pueden usar la característica RBAC.

Corrección

Para usar Redis AUTH en un grupo de replicación ElastiCache (Redis OSS), consulte Modificación del token AUTH en un clúster existente ElastiCache (Redis OSS) en la Guía del usuario de Amazon. ElastiCache

[ElastiCache.7] los ElastiCache clústeres no deben usar el grupo de subredes predeterminado

Requisitos relacionados: NIST.800-53.r5 AC-4 NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (5)

Categoría: Proteger - Configuración de red segura

Gravedad: alta

Tipo de recurso: `AWS::ElastiCache::CacheCluster`

Regla de AWS Config: elasticache-subnet-group-check

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si un ElastiCache clúster está configurado con un grupo de subredes personalizado. El control falla si `CacheSubnetGroupName` un ElastiCache clúster tiene el valor`default`.

Al lanzar un ElastiCache clúster, se crea un grupo de subredes predeterminado si aún no existe ninguno. El grupo predeterminado utiliza subredes de la nube privada virtual (VPC) predeterminada. Recomendamos usar grupos de subredes personalizados que restrinjan más las subredes en las que reside el clúster y las redes que el clúster hereda de las subredes.

Corrección

Para crear un nuevo grupo de subredes para un ElastiCache clúster, consulte Creación de un grupo de subredes en la Guía del ElastiCache usuario de Amazon.

Controles CSPM de Security Hub para Elastic Beanstalk

Estos AWS Security Hub CSPM controles evalúan el AWS Elastic Beanstalk servicio y los recursos.

Es posible que estos controles no estén disponibles en todosRegiones de AWS. Para obtener más información, consulte Disponibilidad de los controles por región.

[ElasticBeanstalk.1] Los entornos de Elastic Beanstalk deberían tener habilitados los informes de estado mejorados

Requisitos relacionados:, NIST.800-53.r5 CA-7 NIST.800-53.r5 SI-2

Categoría: Detectar > Servicios de detección > Supervisión de aplicaciones

Gravedad: baja

Tipo de recurso: `AWS::ElasticBeanstalk::Environment`

Regla de AWS Config: `beanstalk-enhanced-health-reporting-enabled`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si los informes de estado mejorados están habilitados para sus entornos AWS Elastic Beanstalk.

Los informes de estado mejorados de Elastic Beanstalk permiten una respuesta más rápida a los cambios en el estado de la infraestructura subyacente. Estos cambios podrían provocar una falta de disponibilidad de la aplicación.

Los informes de estado mejorados de Elastic Beanstalk proporcionan un descriptor de estado para evaluar la gravedad de los problemas identificados e identificar las posibles causas que se deben investigar. El agente de estado de Elastic Beanstalk, incluido en las Imágenes de máquina de Amazon (AMI) compatibles, evalúa los registros y las métricas de las instancias EC2 del entorno.

Para obtener información adicional, consulte la Supervisión y los informes de estado mejorados en la Guía para desarrolladores de AWS Elastic Beanstalk.

Corrección

Para obtener instrucciones sobre cómo habilitar los informes de estado mejorados, consulte Habilitar los informes de estado mejorados mediante la consola de Elastic Beanstalk en la Guía para desarrolladores de AWS Elastic Beanstalk.

[ElasticBeanstalk.2] Las actualizaciones de la plataforma gestionada de Elastic Beanstalk deben estar habilitadas

Requisitos relacionados: NIST.800-53.r5 SI-2 (2) NIST.800-53.r5 SI-2, (4), NIST.800-53.r5 SI-2 NIST.800-53.r5 SI-2 (5), PCI DSS v4.0. 1/63.3.3

Categoría: Identificar > Administración de vulnerabilidades, parches y versiones

Gravedad: alta

Tipo de recurso: `AWS::ElasticBeanstalk::Environment`

Regla de AWS Config: `elastic-beanstalk-managed-updates-enabled`

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`UpdateLevel`	Nivel de actualización de la versión	Enum	`minor`, `patch`	Sin valor predeterminado

Este control comprueba si las actualizaciones de la plataforma administradas están habilitadas para un entorno de Elastic Beanstalk. Se produce un error en el control si no están habilitadas las actualizaciones de la plataforma administradas. De manera predeterminada, el control pasa si algún tipo de actualización de la plataforma está habilitado. De manera opcional, puede proporcionar un valor personalizado de parámetro para requerir un nivel de actualización específico.

Al habilitar las actualizaciones de plataforma administradas, se garantiza que se instalen las últimas correcciones, actualizaciones y funciones de la plataforma disponibles para el entorno. Mantenerse al día con la instalación de los parches es un paso importante para proteger los sistemas.

Corrección

Para habilitar las actualizaciones de la plataforma administradas, consulte Configuración de las actualizaciones de la plataforma administradas en la sección Actualizaciones de la plataforma administradas de la Guía para desarrolladores de AWS Elastic Beanstalk.

[ElasticBeanstalk.3] Elastic Beanstalk debería transmitir los registros a CloudWatch

Requisitos relacionados: PCI DSS v4.0. 1/104.4.2

Categoría: Identificar - Registro

Gravedad: alta

Tipo de recurso: `AWS::ElasticBeanstalk::Environment`

Regla de AWS Config: `elastic-beanstalk-logs-to-cloudwatch`

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`RetentionInDays`	Cantidad de días que se van a conservar los eventos de registro antes de que expiren	Enum	`1`, `3`, `5`, `7`, `14`, `30`, `60`, `90`, `120`, `150`, `180`, `365` , `400`, `545`, `731`, `1827`, `3653`	Sin valor predeterminado

Este control comprueba si un entorno de Elastic Beanstalk está configurado para enviar registros a Logs. CloudWatch El control falla si el entorno de Elastic Beanstalk no está configurado para enviar registros a Logs. CloudWatch De manera opcional, puede proporcionar un valor personalizado para el parámetro `RetentionInDays` si quiere que el control pase únicamente si los registros se retienen durante la cantidad de días especificada antes de que expiren.

CloudWatch le ayuda a recopilar y monitorear diversas métricas para sus aplicaciones y recursos de infraestructura. También se puede utilizar CloudWatch para configurar acciones de alarma en función de métricas específicas. Recomendamos integrar Elastic CloudWatch Beanstalk con para obtener una mayor visibilidad del entorno de Elastic Beanstalk. Los registros de Elastic Beanstalk incluyen el archivo eb-activity.log, los registros de acceso del entorno nginx o el servidor proxy Apache y los registros específicos de un entorno.

Corrección

Para integrar Elastic CloudWatch Beanstalk con Logs, consulte Transmitir registros de instancias a Logs en la Guía para CloudWatch desarrolladores. AWS Elastic Beanstalk

Controles de CSPM de Security Hub para Elastic Load Balancing

Estos AWS Security Hub CSPM controles evalúan el servicio y los recursos de Elastic Load Balancing. Es posible que los controles no estén disponibles en todos los casos Regiones de AWS. Para obtener más información, consulte Disponibilidad de los controles por región.

[ELB.1] El balanceador de carga de aplicaciones debe configurarse para redirigir todas las solicitudes HTTP a HTTPS

Requisitos relacionados: PCI DSS v3.2. 1/22.3, PCI DSS v3.2. 1/4.1, NIST.800-53.r5 AC-17 (2) NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), NIST.800-53.r5 SC-12 (3) NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23 (3) NIST.800-53.r5 SC-23, (4), NIST.800-53.r5 SC-7 (1) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SC-8 (6) NIST.800-53.r5 SI-7

Categoría: Detectar - Servicios de detección

Gravedad: media

Tipo de recurso: `AWS::ElasticLoadBalancingV2::LoadBalancer`

Regla de AWS Config : alb-http-to-https-redirection-check

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si el redireccionamiento de HTTP a HTTPS está configurado en todos los oyentes HTTP de los equilibradores de carga de aplicación. El control falla si alguno de los detectores HTTP de los equilibradores de carga de aplicaciones no tiene configurada la redirección de HTTP a HTTPS.

Antes de comenzar a utilizar el equilibrador de carga de aplicación, debe agregar al menos uno o más oyentes. Un agente de escucha es un proceso que utiliza el protocolo y el puerto configurados para comprobar las solicitudes de conexión. Los oyentes admiten los protocolos HTTP y HTTPS. Puede utilizar un oyente HTTPS para descargar el trabajo de cifrado y descifrado a su equilibrador de carga. Para forzar el cifrado en tránsito, debe usar acciones de redireccionamiento con los equilibradores de carga de aplicación para redirigir las solicitudes HTTP del cliente hacia una solicitud HTTPS en el puerto 443.

Para obtener más información, consulte Creación de un agente de escucha para el Equilibrador de carga de aplicación en la Guía del usuario de Equilibrador de carga de aplicacións.

Corrección

Para redirigir las solicitudes HTTP a HTTPS, debe agregar una regla de escucha de Equilibrador de carga de aplicación o editar una regla existente.

Para obtener instrucciones sobre cómo agregar una nueva regla, consulte Agregar una regla en la Guía del usuario de los equilibradores de carga de aplicaciones. En Protocolo : Puerto, elija HTTP y luego ingrese **80**. En Añadir acción, Redirigir a, elija HTTPS y, a continuación, introduzca **443**.

Para obtener instrucciones sobre cómo editar una regla existente, consulte Editar una regla en la Guía del usuario de los equilibradores de carga de aplicaciones. En Protocolo : Puerto, elija HTTP y luego ingrese **80**. En Añadir acción, Redirigir a, elija HTTPS y, a continuación, introduzca **443**.

[ELB.2] Los balanceadores de carga clásicos con SSL/HTTPS oyentes deben usar un certificado proporcionado por AWS Gestor de certificados

Requisitos relacionados: NIST.800-53.r5 AC-17 (2) NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), NIST.800-53.r5 SC-12 (3),, NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (5), (4), NIST.800-53.r5 SC-7 (1) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SC-8 NIST.800-53.r5 SI-7 (6), 3.13.8 NIST.800-171.r2

Categoría: Proteger > Protección de datos > Cifrado de datos en tránsito

Gravedad: media

Tipo de recurso: `AWS::ElasticLoadBalancing::LoadBalancer`

Regla de AWS Config : elb-acm-certificate-required

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si el balanceador de carga clásico usa HTTPS/SSL los certificados proporcionados por AWS Gestor de certificados (ACM). El control falla si el balanceador de carga clásico configurado con el HTTPS/SSL listener no usa un certificado proporcionado por ACM.

Para crear un certificado, puede utilizar ACM o una herramienta que admita los protocolos SSL y TLS, como OpenSSL. El CSPM de Security Hub recomienda usar ACM para crear o importar certificados para el balanceador de cargas.

ACM se integra con Equilibrador de carga clásico, lo que le permite implementar el certificado en el equilibrador de carga. También debe renovar estos certificados automáticamente.

Corrección

Para obtener información sobre cómo asociar un SSL/TLS certificado de ACM a un balanceador de cargas clásico, consulte el artículo de AWS Knowledge Center ¿Cómo puedo asociar un SSL/TLS certificado de ACM a un balanceador de cargas clásico, de aplicaciones o de red?

[ELB.3] Los oyentes de Classic Load Balancer deben configurarse con terminación HTTPS o TLS

Requisitos relacionados: NIST.800-53.r5 AC-17 (2), NIST.800-53.r5 IA-5 (1) NIST.800-53.r5 AC-4, (3),, NIST.800-53.r5 SC-12 (3) NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (4), NIST.800-53.r5 SC-7 (1), (2) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 NIST.800-53.r5 SI-7 (6), NIST.800-53.r5 SC-8 NIST.800-171.r2 3.13.8, 3.13.15, PCI DSS v4.0 NIST.800-171.r2 . 1/42.2.1

Categoría: Proteger > Protección de datos > Cifrado de datos en tránsito

Gravedad: media

Tipo de recurso: `AWS::ElasticLoadBalancing::LoadBalancer`

Regla de AWS Config : elb-tls-https-listeners-only

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si los agentes de escucha de Equilibrador de carga clásico están configurados con el protocolo HTTPS o TLS para las conexiones frontend (entre el cliente y el equilibrador de carga). El control se aplica si un Equilibrador de carga clásico tiene oyentes. Si su Equilibrador de carga clásico no tiene un listener configurado, el control no informa de ningún resultado.

El control pasa si los oyentes de Equilibrador de carga clásico están configurados con TLS o HTTPS para las conexiones front-end.

El control falla si el listener no está configurado con TLS o HTTPS para las conexiones front-end.

Antes de comenzar a utilizar un equilibrador de carga, debe agregar uno o más oyentes. Un agente de escucha es un proceso que utiliza el protocolo y el puerto configurados para comprobar las solicitudes de conexión. Los oyentes pueden admitir tanto HTTP como los protocolos. HTTPS/TLS Siempre debe usar un agente de escucha HTTPS o TLS para que el equilibrador de cargas se encargue de cifrar y desencriptar en tránsito.

Corrección

Para solucionar este problema, actualiza tus oyentes para que usen el protocolo TLS o HTTPS.

Para cambiar todos los oyentes que no cumplan con los requisitos por oyentes TLS/HTTPS

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Equilibración de carga, elija equilibradores de carga.
3. Etiquetado del equilibrador de carga clásico
4. En la pestaña Listeners (Agentes de escucha), seleccione Edit (Editar).
5. Para todos los oyentes en los que el Protocolo Equilibrador de carga no esté configurado en HTTPS o SSL, cambie la configuración a HTTPS o SSL.
6. Para todos los oyentes modificados, en la pestaña Certificados, seleccione Cambiar el valor predeterminado.
7. Para los certificados ACM e IAM, seleccione un certificado.
8. Seleccione Guardar como predeterminado.
9. Tras actualizar todos los oyentes, selecciona Guardar.

[ELB.4] El balanceador de carga de aplicaciones debe configurarse para eliminar los encabezados http no válidos

Requisitos relacionados: NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-8 (2), PCI DSS v4.0. 1/64.2.4

Categoría: Proteger > Seguridad de red

Gravedad: media

Tipo de recurso: `AWS::ElasticLoadBalancingV2::LoadBalancer`

Regla de AWS Config : alb-http-drop-invalid-header-enabled

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control evalúa si un equilibrador de carga de aplicación está configurado para eliminar los encabezados HTTP no válidos. El control falla si el valor `routing.http.drop_invalid_header_fields.enabled` se establece como `false`.

De forma predeterminada, los equilibradores de carga de aplicaciones no están configurados para eliminar valores de encabezado HTTP no válidos. La eliminación de estos valores de encabezado evita los ataques de desincronización de HTTP.

> **Note**
>
> Le recomendamos que desactive este control si ELB.12 está activado en su cuenta. Para obtener más información, consulte [ELB.12] El balanceador de carga de aplicaciones debe configurarse con el modo defensivo o de mitigación de desincronización más estricto.

Corrección

Para solucionar este problema, configura tu equilibrador de cargas para eliminar los campos de encabezado no válidos.

Cómo configurar el equilibrador de carga para eliminar campos de encabezado no válidos

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Load balancers (Balanceadores de carga).
3. Eliminación de un Equilibrador de carga de aplicación
4. Para Acciones, elija Editar atributos.
5. En Eliminar campos de encabezado no válidos, selecciona Activar.
6. Seleccione Save.

[ELB.5] El registro de los balanceadores de carga clásicos y de aplicaciones debería estar activado

Requisitos relacionados: NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-7 (8)

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: `AWS::ElasticLoadBalancing::LoadBalancer`, `AWS::ElasticLoadBalancingV2::LoadBalancer`

Regla de AWS Config : elb-logging-enabled

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si el Equilibrador de carga de aplicación y el Equilibrador de carga clásico tienen el registro activado. El control tiene errores si `access_logs.s3.enabled` es `false`.

Elastic Load Balancing proporciona registros de acceso que capturan información detallada sobre las solicitudes enviadas al equilibrador de carga. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud, la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor. Puede utilizar estos registros de acceso para analizar los patrones de tráfico y solucionar problemas.

Para obtener más información, consulte Etiquetado del Equilibrador de carga clásico en la Guía del usuario de Equilibrador de carga clásicos.

Corrección

Para habilitar los registros de acceso, consulte el Paso 3: Configurar los registros de acceso en la Guía del usuario de los equilibradores de carga de aplicaciones.

[ELB.6] Los balanceadores de cargas de aplicaciones, puertas de enlace y red deben tener habilitada la protección contra eliminaciones

Requisitos relacionados: NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2) NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2)

Categoría: Recuperación > Resiliencia > Alta disponibilidad

Gravedad: media

Tipo de recurso: `AWS::ElasticLoadBalancingV2::LoadBalancer`

Regla de AWS Config : elb-deletion-protection-enabled

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si el equilibrador de carga de red, de puerta de enlace o de aplicación tiene habilitada la protección contra eliminación. El control falla si la protección contra la eliminación está deshabilitada.

Habilite la protección contra eliminación para evitar que el equilibrador de carga de red, de puerta de enlace o de aplicación se elimine.

Corrección

Para evitar que el equilibrador de carga se elimine por error, puede habilitar la protección contra eliminación. De forma predeterminada, la protección contra eliminación del equilibrador de carga está deshabilitada.

Si habilita la protección contra eliminación del equilibrador de carga, deberá deshabilitarla para poder eliminarlo.

Para habilitar la protección contra la eliminación de un equilibrador de carga de aplicación, consulte la sección Protección contra la eliminación en la Guía del usuario de los equilibradores de carga de aplicaciones. Para habilitar la protección contra la eliminación de un equilibrador de carga de puerta de enlace, consulte la sección Protección contra la eliminación en la Guía del usuario de los equilibradores de carga de puerta de enlace. Para habilitar la protección contra la eliminación de un equilibrador de carga de red, consulte la sección Protección contra la eliminación en la Guía del usuario de los equilibradores de carga de red.

[ELB.7] Los balanceadores de carga clásicos deben tener activado el drenaje de conexiones

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Categoría: Recuperación > Resiliencia

Gravedad: baja

Tipo de recurso: `AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config regla: `elb-connection-draining-enabled` (regla CSPM personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si los equilibradores de carga clásicos tienen habilitado el drenaje de conexión.

Al habilitar el drenaje de conexiones en los Equilibradores de carga clásicos se garantiza que el equilibrador de carga deje de enviar solicitudes a instancias que están en proceso de anulación

del registro o se encuentran en mal estado. Mantiene abiertas las conexiones existentes. Esto es particularmente útil para instancias en grupos de escalado automático, para garantizar que las conexiones no se interrumpan abruptamente.

Corrección

Para habilitar el drenaje de conexión en Equilibrador de carga clásico, consulte Configuración del drenaje de conexión para el Equilibrador de carga clásico en la Guía del usuario de Equilibrador de carga clásico.

[ELB.8] Los balanceadores de carga clásicos con receptores SSL deben usar una política de seguridad predefinida que sea sólida AWS Config Duración

Requisitos relacionados: NIST.800-53.r5 AC-17 (2), NIST.800-53.r5 IA-5 (1) NIST.800-53.r5 AC-4, (3), NIST.800-53.r5 SC-12 (3) NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23 (3) NIST.800-53.r5 SC-23, (4), NIST.800-53.r5 SC-7 (1) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SC-8 NIST.800-53.r5 SI-7 (6), NIST.800-171.r2 3.13.8, NIST.800-171.r2 3.13.15, PCI DSS v4.0. 1/42.2.1

Categoría: Proteger > Protección de datos > Cifrado de datos en tránsito

Gravedad: media

Tipo de recurso: `AWS::ElasticLoadBalancing::LoadBalancer`

Regla de AWS Config : elb-predefined-security-policy-ssl-check

Tipo de horario: provocado por un cambio

Parámetros:

- `predefinedPolicyName`: `ELBSecurityPolicy-TLS-1-2-2017-01` (no personalizable)

Este control comprueba si los HTTPS/SSL oyentes de Classic Load Balancer utilizan la política predefinida. `ELBSecurityPolicy-TLS-1-2-2017-01` El control falla si los HTTPS/SSL oyentes de Classic Load Balancer no la utilizan. `ELBSecurityPolicy-TLS-1-2-2017-01`

Una política de seguridad es una combinación de protocolos SSL, cifrados y la opción de preferencia del orden del servidor. Las políticas predefinidas controlan los cifrados, los protocolos y los órdenes de preferencia que se deben admitir durante las negociaciones SSL entre un cliente y un equilibrador de carga.

Usar `ELBSecurityPolicy-TLS-1-2-2017-01` puede ayudarlo a cumplir con los estándares de cumplimiento y seguridad que requieren que deshabilite versiones específicas de SSL y TLS. Para obtener más información, consulte Agentes de escucha para el Equilibrador de carga clásico en la Guía del usuario de Equilibrador de carga clásicos.

Corrección

Para obtener información sobre cómo utilizar la política de seguridad predefinida de `ELBSecurityPolicy-TLS-1-2-2017-01` con un Equilibrador de carga clásico, consulte Configurar los ajustes de seguridad en la Guía del usuario de Equilibrador de carga clásicos.

[ELB.9] Los balanceadores de carga clásicos deben tener habilitado el balanceo de cargas entre zonas

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2) NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoría: Recuperación > Resiliencia > Alta disponibilidad

Gravedad: media

Tipo de recurso: `AWS::ElasticLoadBalancing::LoadBalancer`

Regla de AWS Config : elb-cross-zone-load-balancing-enabled

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si el equilibrio de carga entre zonas está habilitado para los equilibradores de carga clásicos (CLB). El control falla si el equilibrio de carga entre zonas no está habilitado para un CLB.

Cada nodo del equilibrador de carga distribuye el tráfico entre los destinos registrados en su zona de disponibilidad solamente. Cuando el equilibrio de carga entre zonas está deshabilitado, cada nodo del equilibrador de carga distribuye el tráfico únicamente entre los destinos registrados de su zona de disponibilidad. Si el número de destinos registrados no es el mismo en todas las zonas de disponibilidad, el tráfico no se distribuirá de manera uniforme y las instancias de una zona podrían terminar sobreutilizadas en comparación con las instancias de otra zona. Con cross-zone load balancing, cada nodo del equilibrador de carga de su equilibrador de carga clásico

distribuye las solicitudes equitativamente entre todas las instancias registradas en todas las zonas de disponibilidad habilitadas. Para obtener más información, consulta el equilibrio de Cross-zone carga en la Guía del usuario de Elastic Load Balancing.

Corrección

Para habilitar el balanceo de cargas entre zonas en un Equilibrador de carga clásico, consulta Habilitar el balanceo de cargas entre zonas en la Guía del usuario de Equilibrador de carga clásicos.

[ELB.10] El balanceador de carga clásico debe abarcar varias zonas de disponibilidad

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2) NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoría: Recuperación > Resiliencia > Alta disponibilidad

Gravedad: media

Tipo de recurso: `AWS::ElasticLoadBalancing::LoadBalancer`

Regla de AWS Config : clb-multiple-az

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub CSPM
`minAvailabilityZones`	Cantidad mínima de zonas de disponibilidad	Enum	`2, 3, 4, 5, 6`	2

Este control comprueba si se configuró un Equilibrador de carga clásico para abarcar al menos la cantidad especificada de zonas de disponibilidad (AZ). Se produce un error en el control si el equilibrador de carga clásico no abarca al menos la cantidad especificada de AZ. A menos

que proporcione un valor de parámetro personalizado para la cantidad mínima de zonas de disponibilidad, el CSPM de Security Hub utiliza un valor predeterminado de dos zonas de disponibilidad.

Puede configurar el equilibrador de carga clásico para que las solicitudes de entrada se distribuyan entre las instancias de Amazon EC2 de una única zona de disponibilidad o de varias. Un Equilibrador de carga clásico que no abarque varias zonas de disponibilidad no puede redirigir el tráfico a destinos de otra zona de disponibilidad si la única zona de disponibilidad configurada deja de estar disponible.

Corrección

Para agregar zonas de disponibilidad a un equilibrador de carga clásico, consulte Add or remove subnets for your Classic Load Balancer en la Guía del usuario para los Equilibradores de carga clásicos.

[ELB.12] El balanceador de carga de aplicaciones debe configurarse con el modo defensivo o de mitigación de desincronización más estricto

Requisitos relacionados: NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 CA-9 (1), PCI DSS v4.0 NIST.800-53.r5 CM-2. 1/62.2.4

Categoría: Protección > Protección de datos > Integridad de los datos

Gravedad: media

Tipo de recurso: `AWS::ElasticLoadBalancingV2::LoadBalancer`

Regla de AWS Config : alb-desync-mode-check

Tipo de horario: provocado por un cambio

Parámetros:

- `desyncMode`: `defensive, strictest` (no personalizable)

Este control comprueba si un Equilibrador de carga de aplicación está configurado con el modo defensivo o con el modo de mitigación de desincronización más estricto. El control falla si un Equilibrador de carga de aplicación no está configurado con el modo defensivo o de mitigación de desincronización más estricto.

Los problemas de desincronización de HTTP pueden provocar el contrabando de solicitudes y hacer que las aplicaciones sean vulnerables al envenenamiento de las colas de solicitudes o de la caché. A su vez, estas vulnerabilidades pueden provocar el uso indebido de credenciales o la ejecución de comandos no autorizados. Los equilibradores de carga de aplicaciones configurados con el modo defensivo o el modo de mitigación de desincronización más estricto protegen tu aplicación de los problemas de seguridad que pueda provocar la desincronización de HTTP.

Corrección

Para actualizar el modo de mitigación de desincronización de un Equilibrador de carga de aplicación, consulte el modo de mitigación de desincronización en la Guía del usuario de Equilibrador de carga de aplicaciones.

[ELB.13] Los balanceadores de carga de aplicaciones, redes y puertas de enlace deben abarcar varias zonas de disponibilidad

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2) NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoría: Recuperación > Resiliencia > Alta disponibilidad

Gravedad: media

Tipo de recurso: `AWS::ElasticLoadBalancingV2::LoadBalancer`

Regla de AWS Config : elbv2-multiple-az

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub CSPM
`minAvailabilityZones`	Cantidad mínima de zonas de disponibilidad	Enum	`2, 3, 4, 5, 6`	2

Este control comprueba si un Elastic Load Balancer V2 (equilibrador de carga de aplicaciones, redes o puertas de enlace) registró instancias de al menos la cantidad especificada de zonas de disponibilidad (AZ). Se produce un error en el control si un Elastic Load Balancer V2 no tiene instancias registradas en al menos la cantidad especificada de AZ. A menos que proporcione un valor de parámetro personalizado para la cantidad mínima de zonas de disponibilidad, el CSPM de Security Hub utiliza un valor predeterminado de dos zonas de disponibilidad.

Elastic Load Balancing distribuye automáticamente el tráfico entrante entre varios destinos, por ejemplo, instancias EC2, contenedores y direcciones IP en una o varias zonas de disponibilidad. Elastic Load Balancing escala el equilibrador de carga a medida que el tráfico entrante va cambiando con el tiempo. Se recomienda configurar al menos dos zonas de disponibilidad para garantizar la disponibilidad de los servicios, ya que el Elastic Load Balancer podrá dirigir el tráfico a otra zona de disponibilidad si alguna deja de estar disponible. Tener configuradas varias zonas de disponibilidad ayudará a evitar que la aplicación tenga un único punto de error.

Corrección

Para agregar una zona de disponibilidad a un Equilibrador de carga de aplicación, consulte Zonas de disponibilidad para el equilibrador de carga de aplicaciones en la Guía del usuario para equilibradores de carga de aplicaciones. Para crear un equilibrador de carga de red, consulte Introducción a los equilibradores de carga de red en la Guía del usuario de los equilibradores de carga de red. Para añadir una zona de disponibilidad a un equilibrador de carga de puerta de enlace, consulte Crear un equilibrador de carga de puerta de enlace en la Guía del usuario de equilibradores de carga de puerta de enlace.

[ELB.14] El balanceador de carga clásico debe configurarse con el modo defensivo o de mitigación de desincronización más estricto

Requisitos relacionados: NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 CA-9 (1), PCI DSS v4.0 NIST.800-53.r5 CM-2. 1/62.2.4

Categoría: Protección > Protección de datos > Integridad de los datos

Gravedad: media

Tipo de recurso: `AWS::ElasticLoadBalancing::LoadBalancer`

Regla de AWS Config : clb-desync-mode-check

Tipo de horario: provocado por un cambio

Parámetros:

- `desyncMode`: `defensive, strictest` (no personalizable)

Este control comprueba si un Equilibrador de carga clásico está configurado con el modo defensivo o con el modo de mitigación de desincronización más estricto. El control falla si el Equilibrador de carga clásico no está configurado con el modo defensivo o de mitigación de desincronización más estricto.

Los problemas de desincronización de HTTP pueden provocar el contrabando de solicitudes y hacer que las aplicaciones sean vulnerables al envenenamiento de las colas de solicitudes o de la caché. A su vez, estas vulnerabilidades pueden provocar el secuestro de credenciales o la ejecución de comandos no autorizados. Los equilibradores de carga clásicos configurados con el modo defensivo o el modo de mitigación de desincronización más estricto protegen tu aplicación de los problemas de seguridad que pueda provocar la desincronización de HTTP.

Corrección

Para actualizar el modo de mitigación de desincronización en un Equilibrador de carga clásico, consulte Modificar el modo de mitigación de desincronización en la Guía del usuario de Equilibrador de carga clásico.

[ELB.16] Los balanceadores de carga de aplicaciones deben estar asociados a un AWS WAF ACL web

Requisitos relacionados: NIST.800-53.r5 AC-4 (21)

Categoría: Proteger > Servicios de protección

Gravedad: media

Tipo de recurso: `AWS::ElasticLoadBalancingV2::LoadBalancer`

Regla de AWS Config : alb-waf-enabled

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un balanceador de carga de aplicaciones está asociado a una lista de control de acceso AWS WAF web (ACL web) AWS WAF clásica o web. El control falla si el `Enabled` campo de la AWS WAF configuración está establecido en. `false`

AWS WAF es un firewall de aplicaciones web que ayuda a proteger las aplicaciones web y las API de los ataques. Con AWS WAFél, puede configurar una ACL web, que es un conjunto de reglas que permiten, bloquean o cuentan las solicitudes web en función de las reglas y condiciones de seguridad web personalizables que defina. Te recomendamos que asocies tu balanceador de carga de aplicaciones a una ACL AWS WAF web para protegerlo de ataques malintencionados.

Corrección

Para asociar un balanceador de carga de aplicaciones a una ACL web, consulta Cómo asociar o desvincular una ACL web a un recurso en la Guía para desarrolladores. AWS AWS WAF

[ELB.17] Los balanceadores de cargas de aplicaciones y redes con oyentes deben usar las políticas de seguridad recomendadas

Requisitos relacionados: NIST.800-53.r5 AC-17 (2) NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), NIST.800-53.r5 SC-12 (3),, (3) NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (3), NIST.800-53.r5 SC-7 (4) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SI-7 (6)

Categoría: Proteger > Protección de datos > Cifrado de datos en tránsito

Gravedad: media

Tipo de recurso: `AWS::ElasticLoadBalancingV2::Listener`

Regla de AWS Config : elbv2-predefined-security-policy-ssl-check

Tipo de horario: provocado por un cambio

Parámetros: `sslPolicies`: `ELBSecurityPolicy-TLS13-1-3-2021-06, ELBSecurityPolicy-TLS13-1-3-FIPS-2023-04, ELBSecurityPolicy-TLS13-1-2-Res-2021-06, ELBSecurityPolicy-TLS13-1-2-Res-FIPS-2023-04, ELBSecurityPolicy-TLS13-1-2-Res-PQ-2025-09, ELBSecurityPolicy-TLS13-1-3-PQ-2025-09, ELBSecurityPolicy-TLS13-1-2-Res-FIPS-PQ-2025-09, ELBSecurityPolicy-TLS13-1-3-FIPS-PQ-2025-09` (no personalizables)

Este control comprueba si el oyente HTTPS de un equilibrador de carga de aplicación o el oyente TLS de un equilibrador de carga de red están configurados para cifrar los datos en tránsito mediante una política de seguridad recomendada. El control falla si el oyente HTTPS o TLS del equilibrador de carga no está configurado para usar una política de seguridad recomendada.

Elastic Load Balancing usa una configuración de negociación SSL, conocida como una política de seguridad, para negociar las conexiones entre un cliente y un equilibrador de carga. La política de seguridad especifica una combinación de protocolos y cifrados. El protocolo establece una conexión segura entre un cliente y un servidor. Un cifrado es un algoritmo de cifrado que usa claves de cifrado para crear un mensaje codificado. Durante el proceso de negociación de conexiones, el cliente y el equilibrador de carga presentan una lista con los cifrados y protocolos que admite cada uno por orden de preferencia. El uso de una política de seguridad recomendada para un equilibrador de carga contribuye a cumplir los estándares de cumplimiento y seguridad.

Corrección

Para obtener información sobre las políticas de seguridad recomendadas y cómo actualizar los oyentes, consulte las siguientes secciones de la Guía del usuario de Elastic Load Balancing: Políticas de seguridad para equilibradores de carga de aplicación, Políticas de seguridad para equilibradores de carga de red, Actualización de un oyente HTTPS para un equilibrador de carga de aplicación y Actualización de un oyente para un equilibrador de carga de red.

[ELB.18] Los oyentes del balanceador de cargas de red y aplicaciones deben usar protocolos seguros para cifrar los datos en tránsito

Categoría: Proteger > Protección de datos > Cifrado de datos en tránsito

Gravedad: media

Tipo de recurso: `AWS::ElasticLoadBalancingV2::Listener`

Regla de AWS Config : elbv2-listener-encryption-in-transit

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control verifica si el oyente de un equilibrador de carga de aplicación o de un equilibrador de carga de red está configurado para usar un protocolo seguro para cifrar los datos en tránsito. El control falla si el oyente de un equilibrador de carga de aplicación no usa el protocolo HTTPS o si el oyente de un equilibrador de carga de red no usa el protocolo TLS.

Para cifrar los datos transmitidos entre un cliente y un equilibrador de carga, los oyentes de Elastic Load Balancing se deben configurar con protocolos de seguridad estándar del sector: HTTPS para equilibradores de carga de aplicación o TLS para equilibradores de carga de red. De lo contrario, los datos transmitidos entre un cliente y un equilibrador de carga quedan expuestos a interceptación,

manipulación y acceso no autorizado. El uso de HTTPS o TLS por parte de un oyente se ajusta a las prácticas recomendadas de seguridad y ayuda a garantizar la confidencialidad e integridad de los datos durante la transmisión. Esto es especialmente importante para aplicaciones que manejan información confidencial o que deben cumplir con estándares de seguridad que requieren cifrado de los datos en tránsito.

Corrección

Para obtener información sobre cómo configurar protocolos de seguridad para los oyentes, consulte las siguientes secciones de la Guía del usuario de Elastic Load Balancing: Creación de un oyente HTTPS para el equilibrador de carga de aplicación y Creación de un oyente para el equilibrador de carga de red.

[ELB.21] Los grupos destinatarios de Application and Network Load Balancer deben utilizar protocolos de control de estado cifrados

Categoría: Proteger > Protección de datos > Cifrado de datos en tránsito

Gravedad: media

Tipo de recurso: `AWS::ElasticLoadBalancingV2::TargetGroup`

Regla de AWS Config : elbv2-targetgroup-healthcheck-protocol-encrypted

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si el grupo objetivo de las comprobaciones de estado del balanceador de cargas de aplicaciones y redes utiliza un protocolo de transporte cifrado. El control falla si el protocolo de verificación de estado no usa HTTPS. Este control no se aplica a los tipos de destino de Lambda.

Los balanceadores de carga envían solicitudes de verificación de estado a los destinos registrados para determinar su estado y dirigir el tráfico en consecuencia. El protocolo de comprobación del estado especificado en la configuración del grupo objetivo determina cómo se realizan estas comprobaciones. Cuando los protocolos de verificación del estado utilizan una comunicación no cifrada, como HTTP, las solicitudes y respuestas pueden interceptarse o manipularse durante la transmisión. Esto permite a los atacantes obtener información sobre la configuración de la infraestructura, alterar los resultados de las comprobaciones de estado o llevar a cabo ataques intermedios que afectan a las decisiones de enrutamiento. El uso de HTTPS para las

comprobaciones de estado proporciona una comunicación cifrada entre el balanceador de cargas y sus objetivos, lo que protege la integridad y la confidencialidad de la información sobre el estado de salud.

Corrección

Para configurar las comprobaciones de estado cifradas para tu grupo objetivo de Application Load Balancer, consulta Cómo actualizar la configuración de las comprobaciones de estado de un grupo objetivo de Application Load Balancer en la guía del usuario de Elastic Load Balancing. Para configurar las comprobaciones de estado cifradas para tu grupo objetivo de Network Load Balancer, consulta Actualizar la configuración de las comprobaciones de estado de un grupo objetivo de Network Load Balancer en la Guía del usuario de Elastic Load Balancing.

[ELB.22] Los grupos objetivo del ELB deben usar protocolos de transporte cifrados

Categoría: Proteger > Protección de datos > Cifrado de datos en tránsito

Gravedad: media

Tipo de recurso: `AWS::ElasticLoadBalancingV2::TargetGroup`

Regla de AWS Config : elbv2-targetgroup-protocol-encrypted

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un grupo objetivo de Elastic Load Balancing usa un protocolo de transporte cifrado. Este control no se aplica a los grupos objetivo con un tipo de destino de Lambda o ALB, ni a los grupos objetivo que utilizan el protocolo GENEVE. El control falla si el grupo objetivo no usa los protocolos HTTPS, TLS o QUIC.

El cifrado de los datos en tránsito los protege de la interceptación por parte de usuarios no autorizados. Los grupos objetivo que utilizan protocolos no cifrados (HTTP, TCP, UDP) transmiten datos sin cifrar, lo que los hace vulnerables a las escuchas clandestinas. El uso de protocolos cifrados (HTTPS, TLS, QUIC) garantiza la protección de los datos transmitidos entre los balanceadores de carga y los objetivos.

Corrección

Para usar un protocolo cifrado, debes crear un nuevo grupo de destino con los protocolos HTTPS, TLS o QUIC. El protocolo del grupo objetivo no se puede modificar después de la creación. Para

crear un grupo objetivo para Application Load Balancer, consulta Cómo crear un grupo objetivo para tu Application Load Balancer en la guía del usuario de Elastic Load Balancing. Para crear un grupo objetivo de Network Load Balancer, consulta Cómo crear un grupo objetivo para tu Network Load Balancer en la guía del usuario de Elastic Load Balancing.

Security Hub CSPM para Elasticsearch

Estos AWS Security Hub CSPM controles evalúan el servicio y los recursos de Elasticsearch.

Es posible que estos controles no estén disponibles en todos los casos. Regiones de AWS Para obtener más información, consulte Disponibilidad de los controles por región.

[ES.1] Los dominios de Elasticsearch deben tener habilitado el cifrado en reposo

Requisitos relacionados: PCI DSS v3.2. 1/34., NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28 (1) NIST.800-53.r5 SC-28, (10), NIST.800-53.r5 SC-7 (6) NIST.800-53.r5 SI-7

Categoría: Proteger > Protección de datos > Cifrado de datos en reposo

Gravedad: media

Tipo de recurso: `AWS::Elasticsearch::Domain`

Regla de AWS Config : `elasticsearch-encrypted-at-rest`

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si los dominios de Elasticsearch tienen habilitada la configuración de cifrado en reposo. La comprobación falla si el cifrado en reposo no está habilitado.

Para añadir un nivel de seguridad adicional a sus datos confidenciales OpenSearch, debe configurarlos OpenSearch para que estén cifrados en reposo. Los dominios Elasticsearch ofrecen cifrado de datos en reposo. La función se utiliza AWS KMS para almacenar y administrar tus claves de cifrado. Para realizar el cifrado, utiliza el algoritmo estándar de cifrado avanzado con claves de 256 bits ()AES-256.

Para obtener más información sobre el OpenSearch cifrado en reposo, consulte el artículo Cifrado de datos en reposo para Amazon OpenSearch Service en la Guía para desarrolladores de Amazon OpenSearch Service.

Algunos tipos de instancias, como `t.small` y `t.medium`, no admiten el cifrado de datos en reposo. Para obtener más información, consulta los tipos de instancias compatibles en la Guía para desarrolladores de Amazon OpenSearch Service.

Corrección

Para habilitar el cifrado en reposo para los dominios de Elasticsearch nuevos y existentes, consulte Cómo habilitar el cifrado de datos en reposo en la Guía para desarrolladores de Amazon OpenSearch Service.

[ES.2] Los dominios de Elasticsearch no deben ser de acceso público

Requisitos relacionados: PCI DSS v3.2. 1/11.2.1, PCI DSS v3.2. 1/11.3.1, PCI DSS v3.2. 1/13.3.2, PCI DSS v3.2. 1/13.3.4, PCI DSS v3.2. 1/1.3.6, NIST.800-53.r5 AC-21 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), (21) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (11) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SC-7 PCI DSS v4.0. 1/1.4.4

Categoría: Proteger > Configuración de red segura > Recursos dentro de VPC

Gravedad: crítica

Tipo de recurso: `AWS::Elasticsearch::Domain`

Regla de AWS Config : `elasticsearch-in-vpc-only`

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si los dominios de Elasticsearch están en una VPC. No evalúa la configuración de direccionamiento de subred de VPC para determinar el acceso público. Debe asegurarse de que los dominios de Elasticsearch no están asociados a subredes públicas. Consulta Resource-based las políticas en la Guía para desarrolladores OpenSearch de Amazon Service. También debe asegurarse de que la VPC esté configurada de acuerdo con las prácticas recomendadas. Consulte Prácticas recomendadas de seguridad para su VPC en la Guía del usuario de Amazon VPC.

Los dominios de Elasticsearch implementados en una VPC pueden comunicarse con los recursos de la VPC a través de la AWS red privada, sin necesidad de atravesar la Internet pública. Esta

configuración aumenta la posición de seguridad al limitar el acceso a los datos en tránsito. Las VPC proporcionan una serie de controles de red para proteger el acceso a los dominios de Elasticsearch, incluidas las ACL de red y los grupos de seguridad. El CSPM de Security Hub recomienda migrar los dominios públicos de Elasticsearch a las VPC para aprovechar estos controles.

Corrección

Si crea un dominio con un punto de enlace público, no podrá colocarlo posteriormente en una VPC. En lugar de ello, se debe crear un dominio nuevo y migrar los datos. y viceversa. Si crea un dominio dentro de una VPC, no puede tener un punto de enlace público. En su lugar, debe crear otro dominio o deshabilitar este control.

Consulte Cómo lanzar sus dominios de Amazon OpenSearch Service en una VPC en la Guía para desarrolladores de Amazon Service. OpenSearch

[ES.3] Los dominios de Elasticsearch deben cifrar los datos enviados entre nodos

Requisitos relacionados: NIST.800-53.r5 AC-4,, NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (3), NIST.800-53.r5 SC-7 (4), (1) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 NIST.800-53.r5 SC-8 (2), PCI DSS v4.0. 1/42.2.1

Categoría: Proteger > Protección de datos > Cifrado de datos en tránsito

Gravedad: media

Tipo de recurso: `AWS::Elasticsearch::Domain`

Regla de AWS Config : `elasticsearch-node-to-node-encryption-check`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un dominio de Elasticsearch tiene habilitado el cifrado de nodo a nodo. El control falla si el dominio de Elasticsearch no tiene habilitado el cifrado de nodo a nodo. El control también produce resultados fallidos si una versión de Elasticsearch no admite los controles de cifrado de nodo a nodo.

HTTPS (TLS) puede utilizarse para ayudar a evitar posibles ataques de espionaje o de manipulación del tráfico de red con ataques de «persona en medio» o similares. Solo se deben permitir las conexiones cifradas a través de HTTPS (TLS). Habilitar el cifrado de nodo a nodo para los dominios de Elasticsearch garantiza que las comunicaciones dentro del clúster se cifren en tránsito.

Puede haber una penalización en el rendimiento asociada a esta configuración. Debe conocer y probar la compensación de rendimiento antes de activar esta opción.

Corrección

Para obtener información sobre cómo habilitar el cifrado de nodo a nodo en dominios nuevos y existentes, consulte Habilitar el cifrado de nodo a nodo en la Guía para desarrolladores de Amazon OpenSearch Service.

[ES.4] Debería estar habilitado el registro de errores de dominio de Elasticsearch en Logs CloudWatch

Requisitos relacionados: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2 NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 SC-7 (9) NIST.800-53.r5 CA-7, (8), NIST.800-53.r5 SI-3 (20), NIST.800-53.r5 SI-4 NIST.800-53.r5 SI-7 (8)

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: `AWS::Elasticsearch::Domain`

Regla de AWS Config : `elasticsearch-logs-to-cloudwatch`

Tipo de horario: provocado por un cambio

Parámetros:

- `logtype = 'error'` (no personalizable)

Este control comprueba si los dominios de Elasticsearch están configurados para enviar registros de errores a CloudWatch Logs.

Debes habilitar los registros de errores para los dominios de Elasticsearch y enviarlos a CloudWatch Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

Corrección

Para obtener información sobre cómo habilitar la publicación de registros, consulte Habilitar la publicación de registros (consola) en la Guía para desarrolladores de Amazon OpenSearch Service.

[ES.5] Los dominios de Elasticsearch deben tener habilitado el registro de auditoría

Requisitos relacionados: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9),, NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2 NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), (9) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (8), NIST.800-53.r5 SI-3 (20), NIST.800-53.r5 SI-4 NIST.800-53.r5 SI-7 (8), PCI DSS v4.0. 1/104.2.2

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: `AWS::Elasticsearch::Domain`

AWS Config regla: `elasticsearch-audit-logging-enabled` (regla CSPM personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

- `cloudWatchLogsLogGroupArnList` (no personalizable). El CSPM de Security Hub no rellena este parámetro. Comma-separated lista de grupos de CloudWatch registros que se deben configurar para los registros de auditoría.

  Esta regla se aplica `NON_COMPLIANT` si el grupo de CloudWatch registros de registros del dominio de Elasticsearch no está especificado en esta lista de parámetros.

Este control comprueba si los dominios de Elasticsearch tienen habilitado el registro de auditoría. Este control falla si un dominio de Elasticsearch no tiene habilitado el registro de auditoría.

Los registros de auditoría son altamente personalizables. Te permiten realizar un seguimiento de la actividad de los usuarios en tus clústeres de Elasticsearch, incluidos los éxitos y los errores de autenticación, las solicitudes, los cambios de índice y las consultas de búsqueda entrantes. OpenSearch

Corrección

Para obtener instrucciones detalladas sobre cómo habilitar los registros de auditoría, consulte Habilitar los registros de auditoría en la Guía para desarrolladores de Amazon OpenSearch Service.

[ES.6] Los dominios de Elasticsearch deben tener al menos tres nodos de datos

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2) NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoría: Recuperación > Resiliencia > Alta disponibilidad

Gravedad: media

Tipo de recurso: `AWS::Elasticsearch::Domain`

AWS Config regla: `elasticsearch-data-node-fault-tolerance` (regla CSPM personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si los dominios de Elasticsearch están configurados con al menos tres nodos de datos y `zoneAwarenessEnabled` es `true`.

Un dominio de Elasticsearch requiere al menos tres nodos de datos para una alta disponibilidad y tolerancia a errores. La implementación de un dominio de Elasticsearch con al menos tres nodos de datos garantiza las operaciones del clúster en caso de que un nodo falle.

Corrección

Cómo modificar la cantidad de nodos de datos en un dominio de Elasticsearch

1. Abre la consola de Amazon OpenSearch Service en. https://console.aws.amazon.com/aos/
2. En Dominios, elija el nombre del dominio que desea editar.
3. Elija Edit domain (Editar dominio).
4. En Nodos de datos, estableza Número de nodos en un número mayor o igual a `3`.

   Para tres implementaciones de zonas de disponibilidad, establézcalo en un múltiplo de tres para garantizar una distribución equitativa entre las zonas de disponibilidad.
5. Seleccione Enviar.

[ES.7] Los dominios de Elasticsearch deben configurarse con al menos tres nodos maestros dedicados

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2) NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoría: Recuperación > Resiliencia > Alta disponibilidad

Gravedad: media

Tipo de recurso: `AWS::Elasticsearch::Domain`

AWS Config regla: `elasticsearch-primary-node-fault-tolerance` (regla CSPM personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si los dominios de Elasticsearch están configurados con al menos tres nodos principales dedicados. Este control falla si el dominio no utiliza nodos principales dedicados. Este control pasa si los dominios de Elasticsearch tienen cinco nodos principales dedicados. Sin embargo, el uso de más de tres nodos principales puede ser innecesario para mitigar el riesgo de disponibilidad y generará un costo adicional.

Un dominio de Elasticsearch requiere al menos tres nodos principales dedicados para una alta disponibilidad y tolerancia a los errores. Los recursos del nodo principal dedicado pueden agotarse durante las blue/green implementaciones de los nodos de datos porque hay nodos adicionales que administrar. La implementación de un dominio de Elasticsearch con al menos tres nodos principales dedicados garantiza una capacidad suficiente de recursos del nodo principal y operaciones de clúster en caso de que un nodo falle.

Corrección

Para modificar la cantidad de nodos principales dedicados en un dominio OpenSearch

1. Abre la consola OpenSearch de Amazon Service en https://console.aws.amazon.com/aos/.
2. En Dominios, elija el nombre del dominio que desea editar.
3. Elija Edit domain (Editar dominio).
4. En Nodos maestros dedicados, defina el tipo de instancia en el tipo de instancia deseado.

5. Establezca el Número de nodos maestros en tres o más.
6. Seleccione Enviar.

[ES.8] Las conexiones a los dominios de Elasticsearch deben cifrarse con la política de seguridad TLS más reciente

Requisitos relacionados: NIST.800-53.r5 AC-17 (2), NIST.800-53.r5 IA-5 (1) NIST.800-53.r5 AC-4, (3),, NIST.800-53.r5 SC-12 (3) NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (3), NIST.800-53.r5 SC-7 (4), (1) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SC-8 NIST.800-53.r5 SI-7 (6), PCI DSS v4.0. 1/42.2.1

Categoría: Proteger > Protección de datos > Cifrado de datos en tránsito

Gravedad: media

Tipo de recurso: `AWS::Elasticsearch::Domain`

AWS Config regla: `elasticsearch-https-required` (regla CSPM personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un punto de conexión del dominio de Elasticsearch está configurado para utilizar la política de seguridad TLS más reciente. El control falla si el punto de conexión del dominio de Elasticsearch no está configurado para usar la política compatible más reciente o si HTTP no está habilitado. La política de seguridad TLS compatible más reciente es `Policy-Min-TLS-1-2-PFS-2023-10`.

Puede utilizar HTTPS (TLS) para ayudarle a evitar posibles ataques de tipo “intermediario”, de espionaje o de manipulación del tráfico de red. Solo se deben permitir las conexiones cifradas a través de HTTPS (TLS). El cifrado de los datos en tránsito puede afectar al rendimiento. Debe probar su aplicación con esta característica para comprender el perfil de rendimiento y el impacto del TLS. TLS 1.2 proporciona varias mejoras de seguridad con respecto a las versiones anteriores de TLS.

Corrección

Para habilitar el cifrado TLS, utilice la operación de la API UpdateDomainConfig para configurar el objeto DomainEndpointOptions. Esto establece la `TLSSecurityPolicy`.

[ES.9] Los dominios de Elasticsearch deben etiquetarse

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::Elasticsearch::Domain`

AWS Config regla: `tagged-elasticsearch-domain` (regla CSPM personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub CSPM
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	`No default value`

Este control comprueba si un dominio de Elasticsearch tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control falla si el dominio no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si el dominio no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y se compone de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los

propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWSen la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Las etiquetas son accesibles para muchos Servicios de AWS, incluso AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulta Cómo etiquetar tus AWS recursos en. Referencia general de AWS

Corrección

Para agregar etiquetas a un dominio de Elasticsearch, consulte Cómo trabajar con etiquetas en la Guía para desarrolladores de Amazon OpenSearch Service.

Controles CSPM de Security Hub para Amazon EMR

Estos AWS Security Hub CSPM controles evalúan el servicio y los recursos de Amazon EMR (anteriormente denominado Amazon Elastic MapReduce). Es posible que los controles no estén disponibles en todosRegiones de AWS. Para obtener más información, consulte Disponibilidad de los controles por región.

[EMR.1] Los nodos principales del clúster de Amazon EMR no deben tener direcciones IP públicas

Requisitos relacionados: PCI DSS v3.2. 1/12.2.1, PCI DSS v3.2. 1/1.3.1, PCI DSS v3.2. 1/1.3.2, PCI DSS v3.2. 1/1.3.4, PCI DSS v3.2. 1/1.3.6, PCI DSS v4.0. 1/1.4.4, NIST.800-53.r5 AC-21 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 AC-4,, (11) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9) NIST.800-53.r5 SC-7

Categoría: Proteger - Configuración de red segura

Gravedad: alta

Tipo de recurso: `AWS::EMR::Cluster`

AWS Configregla: emr-master-no-public-ip

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si los nodos maestros de los clústeres de Amazon EMR tienen direcciones IP públicas. El control falla si hay direcciones IP públicas asociadas a alguna de las instancias del nodo maestro.

Las direcciones IP públicas se designan en el campo `PublicIp` de la configuración de `NetworkInterfaces` de la instancia. Este control solo comprueba los clústeres de Amazon EMR que se encuentran en un estado `RUNNING` o`WAITING`.

Corrección

Durante el lanzamiento, puede controlar si su instancia en una subred predeterminada o no predeterminada tiene asignada una dirección IPv4 pública. De forma predeterminada, las subredes predeterminadas tienen este atributo configurado como `true`. Las subredes no predeterminadas tienen el atributo de direcciones IPv4 públicas configurado como `false`, a menos que lo haya creado el asistente de inicialización de instancias de Amazon EC2. En ese caso, el atributo se establece como `true`.

Después del lanzamiento, no puede desasociar manualmente una dirección IPv4 pública.

Para corregir un error en el resultado, debe lanzar un nuevo clúster en una VPC con una subred privada que tenga el atributo de direccionamiento público IPv4 establecido como `false`. Para obtener instrucciones, consulte Lanzamiento de clústeres en una VPC en la Guía de administración de Amazon EMR.

[EMR.2] La configuración de acceso público del bloque Amazon EMR debe estar habilitada

Requisitos relacionados: PCI DSS v4.0. 1/1.4.4, NIST.800-53.r5 AC-21 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 AC-4,, (11) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9) NIST.800-53.r5 SC-7

Categoría: Proteger > Gestión del acceso seguro > Recurso no accesible públicamente

Gravedad: crítica

Tipo de recurso: `AWS::::Account`

AWS Configregla: emr-block-public-access

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si su cuenta está configurada con el bloqueo de acceso público de Amazon EMR. Se produce un error en el control si la configuración de bloqueo de acceso público no está habilitada o si se permite cualquier puerto que no sea el 22.

El bloqueo de acceso público de Amazon EMR evita que lance un clúster en una subred pública si el clúster tiene una configuración de seguridad que permite el tráfico entrante desde direcciones IP públicas en un puerto. Cuando un usuario de su Cuenta de AWS lanza un clúster, Amazon EMR comprueba las reglas de puerto del grupo de seguridad del clúster y las compara con las reglas de tráfico entrante. Si el grupo de seguridad tiene una regla de entrada que abre los puertos a las direcciones IP públicas IPv4 0.0.0. 0/0 o IPv6: :/0, y esos puertos no están especificados como excepciones para su cuenta, Amazon EMR no permite que el usuario cree el clúster.

> **Note**
>
> Bloquear el acceso público está habilitado de forma predeterminada. Si desea aumentar la protección de la cuenta, le recomendamos que lo mantenga habilitado.

Corrección

Para configurar el bloqueo de acceso público para Amazon EMR, consulte Uso de Bloquear el acceso público de Amazon EMR en la Guía de administración de Amazon EMR.

[EMR.3] Las configuraciones de seguridad de Amazon EMR deben cifrarse en reposo

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CP-9 (8), NIST.800-53.r5 SI-12

Categoría: Proteger > Protección de datos > Cifrado de datos en reposo

Gravedad: media

Tipo de recurso: `AWS::EMR::SecurityConfiguration`

Regla de AWS Config: emr-security-configuration-encryption-rest

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control verifica si una configuración de seguridad de Amazon EMR tiene habilitado el cifrado en reposo. El control falla si la configuración de seguridad no habilita el cifrado en reposo.

Los datos en reposo hacen referencia a los datos que se almacenan en un almacenamiento persistente y no volátil durante cualquier periodo de tiempo. El cifrado de datos en reposo permite proteger la confidencialidad de los datos, lo que reduce el riesgo de que un usuario no autorizado pueda acceder a ellos.

Corrección

Para habilitar el cifrado en reposo en una configuración de seguridad de Amazon EMR, consulte Configuración del cifrado de datos en la Guía de administración de Amazon EMR.

[EMR.4] Las configuraciones de seguridad de Amazon EMR deben cifrarse en tránsito

Requisitos relacionados: NIST.800-53.r5 AC-4 NIST.800-53.r5 SC-7 (4) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (2),, NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (3)

Categoría: Proteger > Protección de datos > Cifrado de datos en tránsito

Gravedad: media

Tipo de recurso: `AWS::EMR::SecurityConfiguration`

Regla de AWS Config: emr-security-configuration-encryption-transit

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control verifica si una configuración de seguridad de Amazon EMR tiene habilitado el cifrado en tránsito. El control falla si la configuración de seguridad no habilita el cifrado en tránsito.

Los datos en tránsito hacen referencia a los datos que se mueven de una ubicación a otra, por ejemplo, entre los nodos del clúster o entre el clúster y la aplicación. Los datos pueden moverse a

través de Internet o dentro de una red privada. El cifrado de los datos en tránsito reduce el riesgo de que un usuario no autorizado pueda espiar el tráfico de la red.

Corrección

Para habilitar el cifrado en tránsito en una configuración de seguridad de Amazon EMR, consulte Configuración del cifrado de datos en la Guía de administración de Amazon EMR.

Controles CSPM de Security Hub para EventBridge

Estos AWS Security Hub CSPM controles evalúan el EventBridge servicio y los recursos de Amazon.

Es posible que estos controles no estén disponibles en todosRegiones de AWS. Para obtener más información, consulte Disponibilidad de los controles por región.

[EventBridge.2] los autobuses de EventBridge eventos deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::Events::EventBus`

AWS Configregla: `tagged-events-eventbus` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si un bus de EventBridge eventos de Amazon tiene etiquetas con las claves específicas definidas en el parámetro`requiredTagKeys`. El control falla si el bus de eventos no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y falla si el bus de eventos no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, incluidasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte Etiquetar sus AWS recursos en el. Referencia general de AWS

Corrección

Para añadir etiquetas a un autobús de EventBridge eventos, consulta las EventBridge etiquetas de Amazon en la Guía del EventBridge usuario de Amazon.

[EventBridge.3] los autobuses de eventos EventBridge personalizados deben tener adjunta una política basada en los recursos

Requisitos relacionados: NIST.800-53.r5 AC-2 NIST.800-53.r5 AC-2 (1), (15) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7),, NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-6 (3) NIST.800-53.r5 AC-5 NIST.800-53.r5 AC-6, PCI DSS v4.0. 1/103.3.1

Categoría: Proteger > Gestión del acceso seguro > Recurso no accesible públicamente

Gravedad: baja

Tipo de recurso: `AWS::Events::EventBus`

Regla de AWS Config: [custom-eventbus-policy-attached]

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un bus de eventos EventBridge personalizado de Amazon tiene adjunta una política basada en recursos. Este control falla si el bus de eventos personalizado no tiene una política basada en recursos.

De forma predeterminada, un bus de eventos EventBridge personalizado no incluye una política basada en recursos. Esto permite a los directores de la cuenta acceder al bus de eventos. Al adjuntar una política basada en recursos al bus de eventos, puede limitar el acceso al bus de eventos a cuentas específicas, así como conceder acceso intencionadamente a entidades de otra cuenta.

Corrección

Para adjuntar una política basada en recursos a un bus de eventos EventBridge personalizado, consulta Uso de políticas basadas en recursos para Amazon en EventBridge la Guía del usuario de Amazon. EventBridge

[EventBridge.4] los puntos finales EventBridge globales deberían tener habilitada la replicación de eventos

Requisitos relacionados: NIST.800-53.r5 CP-10 NIST.800-53.r5 CP-6 (2) NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoría: Recuperación > Resiliencia > Alta disponibilidad

Gravedad: media

Tipo de recurso: `AWS::Events::Endpoint`

Regla de AWS Config: `global-endpoint-event-replication-enabled`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si la replicación de eventos está habilitada para un punto final EventBridge global de Amazon. El control falla si la replicación de eventos no está habilitada para un punto de conexión global.

Los puntos de enlace globales ayudan a que su aplicación sea Regional-fault tolerante. Para empezar, debe asignar una comprobación de estado de Amazon Route 53 al punto de conexión. Cuando se inicia la conmutación por error, la comprobación de estado indica un estado “en mal estado”. A los pocos minutos del inicio de la conmutación por error, todos los eventos personalizados se enrutan a un bus de eventos en la región secundaria y son procesados por ese bus de eventos. Al utilizar puntos finales globales, puede habilitar la replicación de eventos. La replicación de eventos envía todos los eventos personalizados a los buses de eventos de las regiones principal y secundaria mediante reglas administradas. Recomendamos habilitar la replicación de eventos al configurar los puntos finales globales. La replicación de eventos le ayuda a comprobar que los puntos finales globales están configurados correctamente. La replicación de eventos es necesaria para recuperarse automáticamente de un evento de conmutación por error. Si no tiene habilitada la replicación de eventos, tendrá que restablecer manualmente la comprobación de estado de Route 53 a “en buen estado” antes de que los eventos se redirijan a la región principal.

> **Note**
>
> Si utilizas autobuses de eventos personalizados, necesitarás un autobús de eventos personalizado en cada región con el mismo nombre y en la misma cuenta para que la conmutación por error funcione correctamente. Habilitación de la replicación de eventos puede aumentar su costo mensual. Para obtener información sobre los precios, consulta los EventBridge precios de Amazon.

Corrección

Para habilitar la replicación de eventos para puntos de enlace EventBridge globales, consulte Crear un punto de enlace global en la Guía del EventBridge usuario de Amazon. Para la Replicación de eventos, seleccione Replicación de eventos habilitada.

Controles CSPM de Security Hub para Amazon Fraud Detector

Estos controles CSPM de Security Hub evalúan el servicio y los recursos de Amazon Fraud Detector.

Es posible que estos controles no estén disponibles en todos. Regiones de AWS Para obtener más información, consulte Disponibilidad de los controles por región.

[FraudDetector.1] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::FraudDetector::EntityType`

Regla de AWS Config: `frauddetector-entity-type-tagged`

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredKeyTags`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control verifica si un tipo de entidad de Amazon Fraud Detector tiene etiquetas con las claves específicas definidas en el parámetro `requiredKeyTags`. El control falla si el tipo de entidad no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredKeyTags`. Si el parámetro `requiredKeyTags` no está definido, el control solo verifica la existencia de una clave de etiqueta y falla si el tipo de entidad no tiene ninguna. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno

u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte Definición de permisos basados en atributos con autorización ABAC en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte las mejores prácticas y estrategias en los AWSrecursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para agregar etiquetas a un tipo de entidad de Amazon Fraud Detector (consola)

1. Abre la consola de Amazon Fraud Detector en https://console.aws.amazon.com/frauddetector.
2. En el panel de navegación, elija Entidades.
3. Seleccione un tipo de entidad en la lista.
4. En la sección etiquetas de tipos de entidad, seleccione Administrar etiquetas.
5. Elija Añadir nueva etiqueta. Escriba la clave y el valor de para la etiqueta. Repita la acción para pares de clave-valor adicionales.
6. Cuando haya terminado de agregar etiquetas, elija Save (Guardar).

[FraudDetector.2] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::FraudDetector::Label`

Regla de AWS Config: `frauddetector-label-tagged`

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredKeyTags`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control verifica si una etiqueta de categoría de Amazon Fraud Detector tiene etiquetas con las claves específicas definidas en el parámetro `requiredKeyTags`. El control falla si la etiqueta de categoría no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredKeyTags`. Si el parámetro `requiredKeyTags` no está definido, el control solo verifica la existencia de una clave de etiqueta y falla si la etiqueta de categoría no tiene ninguna. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan

operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte Definición de permisos basados en atributos con autorización ABAC en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte las mejores prácticas y estrategias en los AWSrecursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para agregar etiquetas a una etiqueta de categoría de Amazon Fraud Detector (consola)

1. Abre la consola de Amazon Fraud Detector en https://console.aws.amazon.com/frauddetector.
2. En el panel de navegación, elija Etiquetas de categoría.
3. Seleccione una etiqueta de categoría en la lista.
4. En la sección etiquetas de etiquetas de categorías, elija Administrar etiquetas.
5. Elija Añadir nueva etiqueta. Escriba la clave y el valor de para la etiqueta. Repita la acción para pares de clave-valor adicionales.
6. Cuando haya terminado de agregar etiquetas, elija Save (Guardar).

[FraudDetector.3] Los resultados de Amazon Fraud Detector deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::FraudDetector::Outcome`

Regla de AWS Config: `frauddetector-outcome-tagged`

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredKeyTags`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control verifica si una salida de Amazon Fraud Detector tiene etiquetas con las claves específicas definidas en el parámetro `requiredKeyTags`. El control falla si la salida no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredKeyTags`. Si el parámetro `requiredKeyTags` no está definido, el control solo verifica la existencia de una clave de etiqueta y falla si la salida no tiene ninguna. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte Definición de permisos basados en atributos con autorización ABAC en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte las mejores prácticas y estrategias en los AWSrecursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para agregar etiquetas a una salida de Amazon Fraud Detector (consola)

1. Abre la consola de Amazon Fraud Detector en https://console.aws.amazon.com/frauddetector.
2. En el panel de navegación, elija Salidas.
3. Seleccione una salida en la lista.
4. En la sección etiquetas de salidas, elija Administrar etiquetas.
5. Elija Añadir nueva etiqueta. Escriba la clave y el valor de para la etiqueta. Repita la acción para pares de clave-valor adicionales.
6. Cuando haya terminado de agregar etiquetas, elija Save (Guardar).

[FraudDetector.4] Las variables de Amazon Fraud Detector deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::FraudDetector::Variable`

Regla de AWS Config: `frauddetector-variable-tagged`

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredKeyTags`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si una variable de Amazon Fraud Detector tiene etiquetas con las claves específicas definidas en el parámetro `requiredKeyTags`. El control falla si la variable no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredKeyTags`. Si no se proporciona el parámetro `requiredKeyTags`, el control solo comprueba la existencia de una clave de etiqueta y falla si la variable no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte Definición de permisos basados en atributos con autorización ABAC en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte las mejores prácticas y estrategias en los AWSrecursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para agregar etiquetas a una variable de Amazon Fraud Detector (consola)

1. Abre la consola de Amazon Fraud Detector en https://console.aws.amazon.com/frauddetector.
2. En el panel de navegación, elija Variables.
3. Seleccione una variable de la lista.
4. En la sección etiquetas de variables, elija Administrar etiquetas.
5. Elija Añadir nueva etiqueta. Escriba la clave y el valor de para la etiqueta. Repita la acción para pares de clave-valor adicionales.
6. Cuando haya terminado de agregar etiquetas, elija Save (Guardar).

Controles CSPM de Security Hub para Amazon FSx

Estos AWS Security Hub CSPM controles evalúan el servicio y los recursos de Amazon FSx. Es posible que los controles no estén disponibles en todosRegiones de AWS. Para obtener más información, consulte Disponibilidad de los controles por región.

[FSx.1] FSx para sistemas de archivos OpenZFS debe configurarse para copiar etiquetas en copias de seguridad y volúmenes

Requisitos relacionados: NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::FSx::FileSystem`

Regla de AWS Config: fsx-openzfs-copy-tags-enabled

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si un sistema de archivos de Amazon FSx para OpenZFS está configurado para copiar etiquetas en las copias de seguridad y en los volúmenes. Se produce un error en el control si el sistema de archivos de OpenZFS no está configurado para copiar etiquetas en copias de seguridad y volúmenes.

La identificación y el inventario de sus activos de TI es un aspecto importante de gobernanza y seguridad. Las etiquetas le ayudan a clasificar AWS los recursos de diferentes maneras, por ejemplo, por propósito, propietario o entorno. Esto es útil cuando tiene muchos recursos del mismo tipo porque puede identificar rápidamente un recurso específico en función de las etiquetas que le haya asignado.

Corrección

Para obtener información sobre cómo configurar un sistema de archivos de FSx para OpenZFS para copiar etiquetas en las copias de seguridad y en los volúmenes, consulte Actualización de un sistema de archivos en la Guía del usuario de Amazon FSx para OpenZFS.

[FSx.2] Los sistemas de archivos FSx for Lustre deben configurarse para copiar etiquetas a las copias de seguridad

Requisitos relacionados:, NIST.800-53.r5 CP-9 NIST.800-53.r5 CM-8

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::FSx::FileSystem`

Regla de AWS Config: fsx-lustre-copy-tags-to-backups

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si un sistema de archivos de Amazon FSx para Lustre está configurado para copiar etiquetas en copias de seguridad y volúmenes. Se produce un error en el control si el sistema de archivos de Lustre no está configurado para copiar etiquetas en copias de seguridad y volúmenes.

La identificación y el inventario de sus activos de TI es un aspecto importante de gobernanza y seguridad. Las etiquetas le ayudan a clasificar AWS los recursos de diferentes maneras, por ejemplo, por propósito, propietario o entorno. Esto es útil cuando tiene muchos recursos del mismo tipo porque puede identificar rápidamente un recurso específico en función de las etiquetas que le haya asignado.

Corrección

Para obtener información sobre cómo configurar un sistema de archivos FSx para Lustre para copiar etiquetas en las copias de seguridad, consulte Cómo copiar copias de seguridad dentro de la misma Cuenta de AWS en la Guía del usuario de Amazon FSx para Lustre.

[FSx.3] FSx para sistemas de archivos OpenZFS debe configurarse para su implementación Multi-AZ

Categoría: Recuperación > Resiliencia > Alta disponibilidad

Gravedad: media

Tipo de recurso: `AWS::FSx::FileSystem`

Regla de AWS Config: fsx-openzfs-deployment-type-check

Tipo de programa: Periódico

Parámetros: `deploymentTypes: MULTI_AZ_1` (no personalizables)

Este control comprueba si un sistema de archivos Amazon FSx para OpenZFS está configurado para utilizar el tipo de despliegue de varias zonas de disponibilidad ()Multi-AZ. El control falla si el sistema de archivos no está configurado para usar el Multi-AZ tipo de implementación.

Amazon FSx para OpenZFS admite varios tipos de implementación para sistemas de archivos: Multi-AZ (HA), (HA) y Single-AZ Single-AZ (no HA). Los tipos de implementación ofrecen diferentes niveles de disponibilidad y durabilidad. Multi-AZ Los sistemas de archivos (HA) se componen de un par de servidores de archivos de alta disponibilidad (HA) que se distribuyen en dos zonas de disponibilidad (AZ). Recomendamos utilizar el tipo de implementación Multi-AZ (HA) para la mayoría de las cargas de trabajo de producción debido al modelo de alta disponibilidad y durabilidad que ofrece.

Corrección

Puede configurar un sistema de archivos Amazon FSx para OpenZFS para que utilice el tipo de Multi-AZ implementación al crear el sistema de archivos. No puede cambiar el tipo de implementación de un sistema de archivos FSx para OpenZFS ya existente.

Para obtener información sobre los tipos y las opciones de implementación para sistemas de archivos FSx para OpenZFS, consulte Disponibilidad y durabilidad para Amazon FSx para OpenZFS y Administración de recursos del sistema de archivos en la Guía del usuario de Amazon FSx para OpenZFS.

[FSx.4] FSx para sistemas de archivos NetApp ONTAP debe configurarse para su implementación Multi-AZ

Categoría: Recuperación > Resiliencia > Alta disponibilidad

Gravedad: media

Tipo de recurso: `AWS::FSx::FileSystem`

Regla de AWS Config: fsx-ontap-deployment-type-check

Tipo de programa: Periódico

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`deploymentTypes`	Una lista de tipos de implementación que se deben incluir en la evaluación. El control genera un resultado `FAILED` si un sistema de archivos no está configurado para usar un tipo de implementación especificado en la lista.	Enum	`MULTI_AZ_1` , `MULTI_AZ_2`	`MULTI_AZ_1` , `MULTI_AZ_2`

Este control comprueba si un sistema de archivos Amazon FSx para NetApp ONTAP está configurado para utilizar un tipo de despliegue de varias zonas de disponibilidad (Multi-AZ). El control

falla si el sistema de archivos no está configurado para usar un tipo de Multi-AZ implementación. Puede especificar opcionalmente una lista de tipos de implementación para incluir en la evaluación.

Amazon FSx para NetApp ONTAP admite varios tipos de implementación para sistemas de archivos: Single-AZ 1, Single-AZ 2, Multi-AZ 1 y 2. Multi-AZ Los tipos de implementación ofrecen distintos niveles de disponibilidad y durabilidad. Recomendamos utilizar un tipo de Multi-AZ implementación para la mayoría de las cargas de trabajo de producción debido al modelo de alta disponibilidad y durabilidad que ofrecen los tipos de Multi-AZ implementación. Multi-AZ los sistemas de archivos admiten todas las características de disponibilidad y durabilidad de los sistemas de Single-AZ archivos. Además, están diseñados para proporcionar disponibilidad continua a los datos aún cuando una zona de disponibilidad (AZ) no esté disponible.

Corrección

No puede cambiar el tipo de implementación de un sistema de archivos Amazon FSx for NetApp ONTAP existente. Sin embargo, puede hacer una copia de seguridad de los datos y, a continuación, restaurarlos en un nuevo sistema de archivos que utilice un tipo de Multi-AZ implementación.

Para obtener información sobre los tipos y las opciones de implementación para sistemas de archivos FSx para ONTAP, consulte Disponibilidad, durabilidad y opciones de implementación y Administración de los sistemas de archivos en la Guía del usuario de FSx para ONTAP.

[FSx.5] Los sistemas de archivos FSx for Windows File Server deben configurarse para Multi-AZ su implementación

Categoría: Recuperación > Resiliencia > Alta disponibilidad

Gravedad: media

Tipo de recurso: `AWS::FSx::FileSystem`

Regla de AWS Config: fsx-windows-deployment-type-check

Tipo de programa: Periódico

Parámetros: `deploymentTypes: MULTI_AZ_1` (no personalizables)

Este control comprueba si un sistema de archivos de Amazon FSx for Windows File Server está configurado para utilizar el tipo de despliegue de varias zonas de disponibilidad Multi-AZ (). El control falla si el sistema de archivos no está configurado para usar el tipo de Multi-AZ implementación.

Amazon FSx for Windows File Server admite dos tipos de implementación para sistemas de archivos Single-AZ: Multi-AZy. Los tipos de implementación ofrecen diferentes niveles de disponibilidad y durabilidad. Single-AZ los sistemas de archivos se componen de una única instancia de servidor de archivos de Windows y un conjunto de volúmenes de almacenamiento dentro de una única zona de disponibilidad (AZ). Multi-AZ los sistemas de archivos se componen de un clúster de servidores de archivos de Windows de alta disponibilidad repartidos en dos zonas de disponibilidad. Se recomienda utilizar el tipo de Multi-AZ implementación para la mayoría de las cargas de trabajo de producción debido al modelo de alta disponibilidad y durabilidad que ofrece.

Corrección

Puede configurar un sistema de archivos Amazon FSx for Windows File Server para que utilice Multi-AZ el tipo de implementación al crear el sistema de archivos. No es posible cambiar el tipo de implementación de un sistema de archivos FSx para Windows File Server ya existente.

Para obtener información sobre los tipos y las opciones de despliegue de los sistemas de archivos fSx para Windows File Server, consulte Disponibilidad y durabilidad Single-AZ : Multi-AZ y sistemas de archivos y Introducción a Amazon FSx para Windows File Server en la Guía del usuario de Amazon FSx para Windows File Server.

Controles CSPM de Security Hub para Global Accelerator

Estos AWS Security Hub CSPM controles evalúan el AWS Global Accelerator servicio y los recursos.

Es posible que estos controles no estén disponibles en todosRegiones de AWS. Para obtener más información, consulte Disponibilidad de los controles por región.

[GlobalAccelerator.1] Los aceleradores de Global Accelerator deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::GlobalAccelerator::Accelerator`

AWS Configregla: `tagged-globalaccelerator-accelerator` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	`No default value`

Este control comprueba si un AWS Global Accelerator acelerador tiene etiquetas con las teclas específicas definidas en el parámetro`requiredTagKeys`. El control lanza error si el acelerador no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si el acelerador no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte Etiquetar sus AWS recursos en el. Referencia general de AWS

Corrección

Para agregar etiquetas a un acelerador global de Global Accelerator, consulte Etiquetado en AWS Global Accelerator en la Guía para desarrolladores de AWS Global Accelerator.

Controles CSPM de Security Hub paraAWS Glue

Estos AWS Security Hub CSPM controles evalúan el AWS Glue servicio y los recursos. Es posible que los controles no estén disponibles en todosRegiones de AWS. Para obtener más información, consulte Disponibilidad de los controles por región.

[Glue.1]AWS Gluelos trabajos deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::Glue::Job`

AWS Configregla: `tagged-glue-job` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si un AWS Glue trabajo tiene etiquetas con las claves específicas definidas en el parámetro`requiredTagKeys`. El control falla si el trabajo no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si el trabajo no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre

ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte Etiquetar sus AWS recursos en el. Referencia general de AWS

Corrección

Para añadir etiquetas a un AWS Glue trabajo, consulte las AWSetiquetas AWS Glue en la Guía del AWS Glueusuario.

[Glue.3]AWS GlueLas transformaciones de aprendizaje automático deben cifrarse en reposo

Categoría: Proteger > Protección de datos > Cifrado de datos en reposo

Gravedad: media

Tipo de recurso: `AWS::Glue::MLTransform`

Regla de AWS Config: glue-ml-transform-encrypted-at-rest

Tipo de horario: provocado por un cambio

Parámetros: no

Este control comprueba si una transformación AWS Glue de aprendizaje automático está cifrada en reposo. El control falla si la transformación de machine learning no está cifrada en reposo.

Los datos en reposo hacen referencia a los datos que se almacenan en un almacenamiento persistente y no volátil durante cualquier periodo de tiempo. El cifrado de datos en reposo permite proteger la confidencialidad de los datos, lo que reduce el riesgo de que un usuario no autorizado pueda acceder a ellos.

Corrección

Para configurar el cifrado para las transformaciones de aprendizaje AWS Glue automático, consulte Trabajar con transformaciones de aprendizaje automático en la Guía del AWS Glue usuario.

[Glue.4]AWS GlueLos trabajos de Spark deberían ejecutarse en versiones compatibles deAWS Glue

Requisitos relacionados: NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2 NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2 (2), NIST.800-53.r5 SI-2 (4), NIST.800-53.r5 SI-2 (5)

Categoría: Identificar > Administración de vulnerabilidades, parches y versiones

Gravedad: media

Tipo de recurso: `AWS::Glue::Job`

Regla de AWS Config: glue-spark-job-supported-version

Tipo de horario: provocado por un cambio

Parámetros: `minimumSupportedGlueVersion`: `3.0` (no personalizables)

Este control comprueba si un AWS Glue trabajo de Spark está configurado para ejecutarse en una versión compatible deAWS Glue. El control falla si el trabajo de Spark está configurado para ejecutarse en una versión anterior a la versión mínima compatible. AWS Glue

> **Note**
>
> Este control también genera la `FAILED` búsqueda de un AWS Glue trabajo de Spark si la propiedad AWS Glue version (`GlueVersion`) no existe o es nula en el elemento de configuración (CI) del trabajo. En tales casos, el resultado incluye la anotación siguiente: `GlueVersion is null or missing in glueetl job configuration`. Para resolver este tipo de resultado `FAILED`, agregue la propiedad `GlueVersion` a la configuración del trabajo. Para obtener una lista de versiones compatibles y entornos de tiempo de ejecución, consulte Versiones de AWS Glue en la Guía del usuario de AWS Glue.

Ejecutar trabajos de AWS Glue Spark en las versiones actuales de AWS Glue puede optimizar el rendimiento, la seguridad y el acceso a las funciones más recientes deAWS Glue. También puede ayudar a proteger contra vulnerabilidades de seguridad. Por ejemplo, se puede publicar una versión nueva para ofrecer actualizaciones de seguridad, corregir problemas o incorporar características nuevas.

Corrección

Para obtener información sobre cómo migrar un trabajo de Spark a una versión compatible deAWS Glue, consulte Migración de trabajos AWS Glue de Spark en la Guía del AWS Glueusuario.

Controles CSPM de Security Hub para Amazon GuardDuty

Estos AWS Security Hub CSPM controles evalúan el GuardDuty servicio y los recursos de Amazon. Es posible que los controles no estén disponibles en todosRegiones de AWS. Para obtener más información, consulte Disponibilidad de los controles por región.

[GuardDuty.1] GuardDuty debería estar activado

Requisitos relacionados: NIST.800-53.r5 AC-2 (12), NIST.800-53.r5 AU-6 (1), NIST.800-53.r5 AU-6 (5) NIST.800-53.r5 CA-7, NIST.800-53.r5 CM-8 (3), NIST.800-53.r5 RA-3 (4), NIST.800-53.r5 SA-11 (1), NIST.800-53.r5 SA-11 (6), NIST.800-53.r5 SA-15 (2), NIST.800-53.r5 SA-15 (8), NIST.800-53.r5 SA-8 (19), NIST.800-53.r5 SA-8 (21), NIST.800-53.r5 SA-8 (25) NIST.800-53.r5 SC-5, NIST.800-53.r5 SC-5 (1), NIST.800-53.r5 SC-5 (3) NIST.800-53.r5 SI-20, NIST.800-53.r5 SI-3 (8) NIST.800-53.r5 SI-4, NIST.800-53.r5 SI-4(1), NIST.800-53.r5 SI-4 (13), NIST.800-53.r5 SI-4 (2), NIST.800-53.r5 SI-4 (22), NIST.800-53.r5 SI-4 (25), NIST.800-53.r5 SI-4 (4), NIST.800-53.r5 SI-4 (5), NIST.800-171.r2 3.4.2, NIST.800-171.r2 3.14.6, NIST.800-171.r2 3.14.7, PCI DSS v3.2. 1/112.4, PCI DSS v4.0. 1/11.5.1

Categoría: Detectar - Servicios de detección

Gravedad: alta

Tipo de recurso: `AWS::::Account`

Regla de AWS Config: guardduty-enabled-centralized

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si Amazon GuardDuty está activado en tu GuardDuty cuenta y región.

Se recomienda encarecidamente que lo habilites GuardDuty en todas las AWS regiones compatibles. Si lo hace, podrá GuardDuty obtener información sobre actividades no autorizadas o inusuales, incluso en las regiones que no utilice activamente. Esto también permite monitorear CloudTrail eventos GuardDuty a nivel mundialServicios de AWS, como la IAM.

Corrección

Para activarlo GuardDuty, consulta Cómo empezar con GuardDuty en la Guía del GuardDuty usuario de Amazon.

GuardDuty Los filtros [GuardDuty.2] deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::GuardDuty::Filter`

AWS Configregla: `tagged-guardduty-filter` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	`No default value`

Este control comprueba si un GuardDuty filtro de Amazon tiene etiquetas con las claves específicas definidas en el parámetro`requiredTagKeys`. El control falla si el filtro no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y falla si el filtro no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte Etiquetar sus AWS recursos en el. Referencia general de AWS

Corrección

Para añadir etiquetas a un GuardDuty filtro, consulta la referencia TagResourcede la GuardDuty API de Amazon.

[GuardDuty.3] Los GuardDuty IPSets deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::GuardDuty::IPSet`

AWS Configregla: `tagged-guardduty-ipset` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	`No default value`

Este control comprueba si un GuardDuty IPSet de Amazon tiene etiquetas con las claves específicas definidas en el parámetro`requiredTagKeys`. El control falla si el IPSet no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y falla si el IPSet no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte Etiquetar sus AWS recursos en el. Referencia general de AWS

Corrección

Para añadir etiquetas a un GuardDuty IPSet, consulte la referencia TagResourcede la GuardDuty API de Amazon.

[GuardDuty.4] GuardDuty los detectores deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::GuardDuty::Detector`

AWS Configregla: `tagged-guardduty-detector` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	`No default value`

Este control comprueba si un GuardDuty detector de Amazon tiene etiquetas con las claves específicas definidas en el parámetro`requiredTagKeys`. El control falla si el detector no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y falla si el detector no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan

operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte Etiquetar sus AWS recursos en el. Referencia general de AWS

Corrección

Para añadir etiquetas a un GuardDuty detector, consulta la referencia TagResourcede la GuardDuty API de Amazon.

[GuardDuty.5] La monitorización del registro de auditoría de GuardDuty EKS debe estar habilitada

Categoría: Detectar - Servicios de detección

Gravedad: alta

Tipo de recurso: `AWS::GuardDuty::Detector`

Regla de AWS Config: guardduty-eks-protection-audit-enabled

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si la supervisión del registro de auditoría de GuardDuty EKS está habilitada. En el caso de una cuenta independiente, el control falla si la supervisión del registro de auditoría de GuardDuty EKS está deshabilitada en la cuenta. En un entorno con varias cuentas, el control falla si la cuenta de GuardDuty administrador delegado y todas las cuentas de los miembros no tienen habilitada la monitorización de registros de auditoría de EKS.

En un entorno con varias cuentas, el control genera resultados únicamente en la cuenta del administrador delegado GuardDuty . Solo el administrador delegado puede activar o desactivar la función de supervisión del registro de auditoría de EKS para las cuentas de los miembros de la organización. GuardDuty las cuentas de los miembros no pueden modificar esta configuración desde sus cuentas. Este control genera `FAILED` resultados si el GuardDuty administrador delegado

tiene una cuenta de miembro suspendida que no tiene habilitada la monitorización del registro de auditoría de GuardDuty EKS. Para recibir una `PASSED` confirmación, el administrador delegado debe desvincular estas cuentas suspendidas. GuardDuty

GuardDuty La monitorización de registros de auditoría de EKS le ayuda a detectar actividades potencialmente sospechosas en sus clústeres de Amazon Elastic Kubernetes Service (Amazon EKS). La supervisión de registros de auditoría de EKS utiliza los registros de auditoría de Kubernetes para capturar las actividades cronológicas de los usuarios, las aplicaciones que utilizan la API de Kubernetes y el plano de control.

Corrección

Para habilitar la supervisión del registro de auditoría de GuardDuty EKS, consulte la supervisión del registro de auditoría de EKS en la Guía del GuardDuty usuario de Amazon.

[GuardDuty.6] GuardDuty La protección Lambda debe estar habilitada

Requisitos relacionados: PCI DSS v4.0. 1/115.5.1

Categoría: Detectar - Servicios de detección

Gravedad: alta

Tipo de recurso: `AWS::GuardDuty::Detector`

Regla de AWS Config: guardduty-lambda-protection-enabled

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si la Protección GuardDuty Lambda está habilitada. En el caso de una cuenta independiente, el control falla si GuardDuty Lambda Protection está deshabilitada en la cuenta. En un entorno de varias cuentas, el control falla si la cuenta de GuardDuty administrador delegado y todas las cuentas de los miembros no tienen habilitada la Protección Lambda.

En un entorno con varias cuentas, el control genera resultados únicamente en la cuenta de administrador delegado. GuardDuty Solo el administrador delegado puede activar o desactivar la función Lambda Protection para las cuentas de los miembros de la organización. GuardDuty las cuentas de los miembros no pueden modificar esta configuración desde sus cuentas. Este control genera `FAILED` resultados si el GuardDuty administrador delegado tiene una cuenta de

miembro suspendida que no tiene habilitada la Protección GuardDuty Lambda. Para recibir una confirmación`PASSED`, el administrador delegado debe desvincular estas cuentas suspendidas. GuardDuty

GuardDuty Lambda Protection le ayuda a identificar posibles amenazas de seguridad cuando se invoca una AWS Lambda función. Después de activar Lambda Protection, GuardDuty comienza a monitorear los registros de actividad de la red Lambda asociados a las funciones de Lambda en su. Cuenta de AWS Cuando se invoca una función Lambda e GuardDuty identifica tráfico de red sospechoso que indica la presencia de un fragmento de código potencialmente malicioso en la función Lambda, GuardDuty genera una detección.

Corrección

Para activar GuardDuty Lambda Protection, consulte Configuración de Lambda Protection en la Guía del usuario de Amazon. GuardDuty

[GuardDuty.7] La monitorización del tiempo de ejecución de GuardDuty EKS debe estar habilitada

Requisitos relacionados: PCI DSS v4.0. 1/115.5.1

Categoría: Detectar - Servicios de detección

Gravedad: alta

Tipo de recurso: `AWS::GuardDuty::Detector`

Regla de AWS Config: guardduty-eks-protection-runtime-enabled

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si la monitorización del tiempo de ejecución de GuardDuty EKS con administración automática de agentes está habilitada. En el caso de una cuenta independiente, el control falla si GuardDuty EKS Runtime Monitoring con administración automática de agentes está deshabilitado en la cuenta. En un entorno con varias cuentas, el control falla si la cuenta de GuardDuty administrador delegado y todas las cuentas de los miembros no tienen habilitada EKS Runtime Monitoring con la administración automática de agentes habilitada.

En un entorno con varias cuentas, el control genera resultados únicamente en la cuenta de administrador delegado GuardDuty . Solo el administrador delegado puede activar o desactivar la función EKS Runtime Monitoring, que permite gestionar automáticamente los agentes de las

cuentas de los miembros de la organización. GuardDuty las cuentas de los miembros no pueden modificar esta configuración desde sus cuentas. Este control genera `FAILED` resultados si el GuardDuty administrador delegado tiene una cuenta de miembro suspendida que no tiene habilitada la monitorización de tiempo de ejecución de GuardDuty EKS. Para recibir una `PASSED` confirmación, el administrador delegado debe desvincular estas cuentas suspendidas. GuardDuty

EKS Protection en Amazon GuardDuty ofrece cobertura de detección de amenazas para ayudarle a proteger los clústeres de Amazon EKS en su AWS entorno. La supervisión en tiempo de ejecución de EKS utiliza los eventos de nivel de sistema operativo para ayudarlo a detectar posibles amenazas en los nodos y contenedores de EKS de sus clústeres de EKS.

Corrección

Para habilitar EKS Runtime Monitoring con la administración automatizada de agentes, consulte Habilitar GuardDuty Runtime Monitoring en la Guía del GuardDuty usuario de Amazon.

[GuardDuty.8] La protección contra GuardDuty malware para EC2 debe estar habilitada

Categoría: Detectar - Servicios de detección

Gravedad: alta

Tipo de recurso: `AWS::GuardDuty::Detector`

Regla de AWS Config: guardduty-malware-protection-enabled

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si la protección contra GuardDuty malware está habilitada. En el caso de una cuenta independiente, el control falla si la protección contra GuardDuty malware está deshabilitada en la cuenta. En un entorno con varias cuentas, el control falla si la cuenta de GuardDuty administrador delegado y todas las cuentas de los miembros no tienen habilitada la protección contra malware.

En un entorno con varias cuentas, el control genera resultados únicamente en la cuenta de administrador delegado GuardDuty . Solo el administrador delegado puede activar o desactivar la función de protección contra malware para las cuentas de los miembros de la organización. GuardDuty las cuentas de los miembros no pueden modificar esta configuración desde sus cuentas. Este control genera `FAILED` resultados si el GuardDuty administrador delegado tiene una cuenta de

miembro suspendida que no tiene habilitada la protección contra GuardDuty malware. Para recibir una `PASSED` confirmación, el administrador delegado debe desvincular estas cuentas suspendidas. GuardDuty

GuardDuty Malware Protection for EC2 le ayuda a detectar la posible presencia de malware escaneando los volúmenes de Amazon Elastic Block Store (Amazon EBS) adjuntos a las instancias de Amazon Elastic Compute Cloud (Amazon EC2) y a las cargas de trabajo de contenedores. La protección contra malware ofrece opciones de análisis en las que puede decidir si desea incluir o excluir instancias y cargas de trabajo de contenedores específicas de EC2 en el momento del análisis. También ofrece la opción de conservar en sus cuentas las instantáneas de los volúmenes de EBS adjuntos a las instancias de EC2 o a las cargas de trabajo de los contenedores. GuardDuty Las instantáneas se conservan solo cuando se encuentra malware y se generan los resultados de la protección contra malware.

Corrección

Para activar la protección contra GuardDuty malware para EC2, consulte Configuración del análisis de GuardDuty-initiated malware en la Guía del GuardDuty usuario de Amazon.

[GuardDuty.9] La protección GuardDuty RDS debe estar habilitada

Requisitos relacionados: PCI DSS v4.0. 1/115.5.1

Categoría: Detectar - Servicios de detección

Gravedad: alta

Tipo de recurso: `AWS::GuardDuty::Detector`

Regla de AWS Config: guardduty-rds-protection-enabled

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si la protección GuardDuty RDS está habilitada. En el caso de una cuenta independiente, el control falla si la protección de GuardDuty RDS está deshabilitada en la cuenta. En un entorno con varias cuentas, el control falla si la cuenta de GuardDuty administrador delegado y todas las cuentas de los miembros no tienen habilitada la protección RDS.

En un entorno con varias cuentas, el control genera resultados únicamente en la cuenta de administrador delegado. GuardDuty Solo el administrador delegado puede activar o desactivar

la función de protección RDS para las cuentas de los miembros de la organización. GuardDuty las cuentas de los miembros no pueden modificar esta configuración desde sus cuentas. Este control genera `FAILED` resultados si el GuardDuty administrador delegado tiene una cuenta de miembro suspendida que no tiene habilitada la protección GuardDuty RDS. Para recibir una confirmación`PASSED`, el administrador delegado debe desvincular estas cuentas suspendidas. GuardDuty

RDS Protection GuardDuty analiza y perfila la actividad de inicio de sesión de RDS para detectar posibles amenazas de acceso a sus bases de datos de Amazon Aurora (Aurora MySQL-Compatible Edition y Aurora PostgreSQL-Compatible Edition). Esta característica le permite identificar comportamientos de inicio de sesión potencialmente sospechosos. La protección de RDS no requiere infraestructura adicional; está diseñada para no afectar al rendimiento de las instancias de bases de datos. Cuando RDS Protection detecta un intento de inicio de sesión potencialmente sospechoso o anómalo que indica una amenaza para su base de datos, GuardDuty genera un nuevo hallazgo con detalles sobre la base de datos potencialmente comprometida.

Corrección

Para activar la protección de GuardDuty RDS, consulte Protección de GuardDuty RDS en la Guía GuardDuty del usuario de Amazon.

[GuardDuty.10] La protección GuardDuty S3 debe estar habilitada

Requisitos relacionados: PCI DSS v4.0. 1/115.5.1

Categoría: Detectar - Servicios de detección

Gravedad: alta

Tipo de recurso: `AWS::GuardDuty::Detector`

Regla de AWS Config: guardduty-s3-protection-enabled

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si la protección GuardDuty S3 está habilitada. En el caso de una cuenta independiente, el control falla si GuardDuty S3 Protection está deshabilitada en la cuenta. En un entorno con varias cuentas, el control falla si la cuenta de GuardDuty administrador delegado y todas las cuentas de los miembros no tienen habilitada la protección S3.

En un entorno con varias cuentas, el control genera resultados únicamente en la cuenta del administrador delegado GuardDuty . Solo el administrador delegado puede activar o desactivar la función de protección S3 para las cuentas de los miembros de la organización. GuardDuty las cuentas de los miembros no pueden modificar esta configuración desde sus cuentas. Este control genera `FAILED` resultados si el GuardDuty administrador delegado tiene una cuenta de miembro suspendida que no tiene habilitada la protección GuardDuty S3. Para recibir una `PASSED` confirmación, el administrador delegado debe desvincular estas cuentas suspendidas. GuardDuty

S3 Protection permite supervisar las operaciones de las API GuardDuty a nivel de objeto para identificar posibles riesgos de seguridad para los datos contenidos en sus depósitos de Amazon Simple Storage Service (Amazon S3). GuardDuty monitorea las amenazas contra sus recursos de S3 mediante el análisis de los eventos AWS CloudTrail de administración y los eventos de datos de CloudTrail S3.

Corrección

Para activar la protección GuardDuty S3, consulte Amazon S3 Protection en Amazon GuardDuty en la Guía del GuardDuty usuario de Amazon.

[GuardDuty.11] La monitorización del GuardDuty tiempo de ejecución debe estar habilitada

Categoría: Detectar - Servicios de detección

Gravedad: alta

Tipo de recurso: `AWS::GuardDuty::Detector`

Regla de AWS Config: guardduty-runtime-monitoring-enabled

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si la monitorización del tiempo de ejecución está habilitada en Amazon GuardDuty. En el caso de una cuenta independiente, el control falla si GuardDuty Runtime Monitoring está deshabilitado para la cuenta. En un entorno con varias cuentas, el control falla si GuardDuty Runtime Monitoring está deshabilitado para la cuenta de GuardDuty administrador delegado y para todas las cuentas de los miembros.

En un entorno con varias cuentas, solo el GuardDuty administrador delegado puede activar o desactivar GuardDuty Runtime Monitoring para las cuentas de su organización. Además, solo el

GuardDuty administrador puede configurar y administrar los agentes de seguridad que GuardDuty utiliza para la supervisión en tiempo de ejecución de AWS las cargas de trabajo y los recursos de las cuentas de la organización. GuardDuty las cuentas de los miembros no pueden activar, configurar ni deshabilitar Runtime Monitoring para sus propias cuentas.

GuardDuty Runtime Monitoring observa y analiza los eventos a nivel del sistema operativo, las redes y los archivos para ayudarlo a detectar posibles amenazas en AWS cargas de trabajo específicas de su entorno. Utiliza agentes de GuardDuty seguridad que añaden visibilidad al comportamiento en tiempo de ejecución, como el acceso a los archivos, la ejecución de procesos, los argumentos de la línea de comandos y las conexiones de red. Puede habilitar y administrar el agente de seguridad para cada tipo de recurso que desee supervisar en busca de amenazas potenciales, como los clústeres de Amazon EKS y las instancias de Amazon EC2.

Corrección

Para obtener información sobre cómo configurar y habilitar GuardDuty Runtime Monitoring, consulte GuardDuty Runtime Monitoring y Enabling GuardDuty Runtime Monitoring en la Guía del GuardDuty usuario de Amazon.

[GuardDuty.12] La monitorización del tiempo de ejecución de GuardDuty ECS debe estar habilitada

Categoría: Detectar - Servicios de detección

Gravedad: media

Tipo de recurso: `AWS::GuardDuty::Detector`

Regla de AWS Config: guardduty-ecs-protection-runtime-enabled

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si el agente de seguridad GuardDuty automatizado de Amazon está activado para la supervisión en tiempo de ejecución de los clústeres de Amazon ECSAWS Fargate. En una cuenta independiente, el control falla si el agente de seguridad está desactivado para dicha cuenta. En un entorno con varias cuentas, el control falla si el agente de seguridad está deshabilitado en la cuenta de GuardDuty administrador delegado y en todas las cuentas de los miembros.

En un entorno con varias cuentas, este control solo genera resultados en la cuenta del administrador delegado GuardDuty . Esto se debe a que solo el GuardDuty administrador delegado puede activar

o desactivar la supervisión en tiempo de ejecución de ECS-Fargate los recursos de las cuentas de su organización. GuardDuty las cuentas de los miembros no pueden hacer esto para sus propias cuentas. Además, este control genera `FAILED` resultados si GuardDuty se suspende la cuenta de un miembro y si se desactiva la supervisión del tiempo de ejecución de ECS-Fargate los recursos de la cuenta de un miembro. Para recibir una confirmación`PASSED`, el GuardDuty administrador debe desvincular la cuenta de miembro suspendida de su cuenta de administrador mediante GuardDuty.

GuardDuty Runtime Monitoring observa y analiza los eventos a nivel del sistema operativo, las redes y los archivos para ayudarlo a detectar posibles amenazas en AWS cargas de trabajo específicas de su entorno. Utiliza agentes de GuardDuty seguridad que añaden visibilidad al comportamiento en tiempo de ejecución, como el acceso a los archivos, la ejecución de procesos, los argumentos de la línea de comandos y las conexiones de red. Puede habilitar y administrar el agente de seguridad para cada tipo de recurso que desee supervisar en busca de amenazas potenciales. Esto incluye los clústeres de Amazon ECS en AWS Fargate.

Corrección

Para habilitar y administrar el agente de seguridad para la supervisión de ECS-Fargate los recursos en tiempo de GuardDuty ejecución, debe usarlo GuardDuty directamente. No puede habilitarlo ni administrarlo manualmente para ECS-Fargate los recursos. Para obtener información sobre cómo habilitar y administrar el agente de seguridad, consulte Requisitos previos para el soporte AWS Fargate (solo para Amazon ECS) y Administración del agente de seguridad automatizado para AWS Fargate (solo Amazon ECS) en la Guía del GuardDuty usuario de Amazon.

[GuardDuty.13] La monitorización del tiempo de ejecución de GuardDuty EC2 debe estar habilitada

Categoría: Detectar - Servicios de detección

Gravedad: media

Tipo de recurso: `AWS::GuardDuty::Detector`

Regla de AWS Config: guardduty-ec2-protection-runtime-enabled

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si el agente de seguridad GuardDuty automatizado de Amazon está habilitado para la supervisión en tiempo de ejecución de las instancias de Amazon EC2. En una

cuenta independiente, el control falla si el agente de seguridad está desactivado para dicha cuenta. En un entorno con varias cuentas, el control falla si el agente de seguridad está deshabilitado en la cuenta de GuardDuty administrador delegado y en todas las cuentas de los miembros.

En un entorno con varias cuentas, este control solo genera resultados en la cuenta del administrador delegado GuardDuty . Esto se debe a que solo el GuardDuty administrador delegado puede habilitar o deshabilitar Runtime Monitoring de las instancias de Amazon EC2 para las cuentas de su organización. GuardDuty las cuentas de los miembros no pueden hacer esto para sus propias cuentas. Además, este control genera `FAILED` resultados si GuardDuty se suspende en una cuenta de miembro y se desactiva la supervisión del tiempo de ejecución de las instancias de EC2 para la cuenta de miembro. Para recibir una confirmación`PASSED`, el GuardDuty administrador debe desasociar la cuenta de miembro suspendida de su cuenta de administrador mediante. GuardDuty

GuardDuty Runtime Monitoring observa y analiza los eventos a nivel del sistema operativo, las redes y los archivos para ayudarlo a detectar posibles amenazas en AWS cargas de trabajo específicas de su entorno. Utiliza agentes de GuardDuty seguridad que añaden visibilidad al comportamiento en tiempo de ejecución, como el acceso a los archivos, la ejecución de procesos, los argumentos de la línea de comandos y las conexiones de red. Puede habilitar y administrar el agente de seguridad para cada tipo de recurso que desee supervisar en busca de amenazas potenciales. Esto incluye instancias de Amazon EC2.

Corrección

Para obtener información sobre la configuración y la administración del agente de seguridad automatizado para la supervisión en tiempo de GuardDuty ejecución de las instancias EC2, consulte Requisitos previos para el soporte de instancias de Amazon EC2 y Habilitación del agente de seguridad automatizado para instancias de Amazon EC2 en la Guía del usuario de Amazon. GuardDuty

Controles CSPM de Security Hub paraAWS Identity and Access Management

Estos AWS Security Hub CSPM controles evalúan el servicio y los recursos AWS Identity and Access Management (IAM). Es posible que los controles no estén disponibles en todosRegiones de AWS. Para obtener más información, consulte Disponibilidad de los controles por región.

[IAM.1] Las políticas de IAM no deberían permitir todos los privilegios administrativos «*»

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2. 0/12.2, Punto de referencia sobre los AWS fundamentos de la CEI v1.4. 0/1.16 NIST.800-53.r5 AC-2, NIST.800-53.r5 AC-2 (1), (15)

NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-3 (10) NIST.800-53.r5 AC-5 NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6 (2), NIST.800-53.r5 AC-6 NIST.800-53.r5 AC-6 (3), NIST.800-171.r2 3.1.4, PCI DSS v3.2. 1/72.2.1

Categoría: Proteger - Administración de acceso seguro

Gravedad: alta

Tipo de recurso: `AWS::IAM::Policy`

Regla de AWS Config: `iam-policy-no-statements-with-admin-access`

Tipo de horario: provocado por un cambio

Parámetros:

- `excludePermissionBoundaryPolicy: true` (no personalizable)

Este control comprueba si la versión predeterminada de las políticas de IAM (también conocidas como políticas administradas por el cliente) tiene acceso de administrador con una instrucción que tenga `"Effect": "Allow"` con `"Action": "*"` en `"Resource": "*"`. El control falla si tiene políticas de IAM con una declaración de este tipo.

El control solo comprueba las políticas administradas por el cliente que haya creado usted. No comprueba las políticas integradas y AWS gestionadas.

Las políticas de IAM definen un conjunto de privilegios concedidos a usuarios, grupos o roles. Siguiendo los consejos de seguridad estándar, se AWS recomienda conceder los privilegios mínimos, es decir, conceder únicamente los permisos necesarios para realizar una tarea. Cuando proporciona privilegios administrativos completos en lugar del conjunto mínimo de permisos que necesita el usuario, expone los recursos a acciones potencialmente no deseadas.

En lugar de concederles privilegios administrativos totales, determine las tareas que tienen que realizar los usuarios y elabore políticas al respecto para permitir a los usuarios realizar solo esas tareas. Es más seguro comenzar con un conjunto mínimo de permisos y conceder permisos adicionales según sea necesario. No comience con permisos demasiado indulgentes para luego restringirlos más adelante.

Debe quitar las políticas de IAM que tienen una instrucción con `"Effect": "Allow"` y `"Action": "*"` en `"Resource": "*"`.

> **Note**
>
> AWS Configdebe estar habilitado en todas las regiones en las que utilice Security Hub CSPM. Sin embargo, el registro de recursos globales se puede habilitar en una sola región. Si solo registra recursos globales en una única región, puede desactivar este control en todas las regiones salvo aquella en la que haya registrado los recursos globales.

Corrección

Para modificar sus políticas de IAM de manera que no permitan todos los privilegios administrativos "*", consulte Edición de políticas de IAM en la Guía del usuario de IAM.

[IAM.2] Los usuarios de IAM no deberían tener políticas de IAM adjuntas

Requisitos relacionados: CIS AWS Foundations Benchmark v5.0. 0/1.14, Criterio de referencia sobre los AWS fundamentos de la CEI v3.0. 0/1.15, Criterio de referencia sobre los AWS fundamentos de la CEI v1.2. 0/1.16, NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-2, (15) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-6 (3), NIST.800-171.r2 3.1.1 NIST.800-53.r5 AC-6, NIST.800-171.r2 3.1.2, NIST.800-171.r2 3.1.7, NIST.800-171.r2 3.3.9, 3.13.3, PCI DSS v3.2. NIST.800-171.r2 1/72.2.1

Categoría: Proteger - Administración de acceso seguro

Gravedad: baja

Tipo de recurso: `AWS::IAM::User`

Regla de AWS Config: `iam-user-no-policies-check`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si sus usuarios de IAM tienen políticas asociadas. El control falla si los usuarios de IAM tienen políticas asociadas. Los usuarios de IAM deben heredar los permisos de los grupos de IAM o asumir un rol.

De forma predeterminada, los usuarios, grupos y roles de IAM no tienen acceso a los AWS recursos. Las políticas de IAM conceden privilegios a los usuarios, grupos o roles. Recomendamos aplicar

políticas de IAM directamente a grupos y roles, pero no a los usuarios. La asignación de privilegios en el nivel de grupo o rol reduce la complejidad de la administración del acceso a medida que crece el número de usuarios. A su vez, la reducción de la complejidad de la administración del acceso podría reducir la oportunidad de que una entidad principal reciba o conserve accidentalmente excesivos privilegios.

> **Note**
>
> AWS Configdebe estar habilitado en todas las regiones en las que utilice Security Hub CSPM. Sin embargo, el registro de recursos globales se puede habilitar en una sola región. Si solo registra recursos globales en una única región, puede deshabilitar este control en todas las regiones salvo en la región en la que haya registrado los recursos globales.

Corrección

Para resolver este problema, cree un grupo de IAM y asocie la política al grupo. Luego, agregue los usuarios al grupo. La política se aplica a cada usuario del grupo. Para eliminar una política asociada directamente a un usuario, consulte Adición y eliminación de permisos de identidad de IAM en la Guía del usuario de IAM.

[IAM.3] Las claves de acceso de los usuarios de IAM deben rotarse cada 90 días o menos

Requisitos relacionados: CIS AWS Foundations Benchmark v5.0. 0/1.13, Criterio de referencia sobre los AWS fundamentos de la CEI v3.0. 0/1.14, Punto de referencia sobre los AWS fundamentos de la CEI v1.4. 0/1.14, Punto de referencia sobre los AWS fundamentos de la CEI v1.2. 0/1.4, NIST.800-53.r5 AC-2 (1), (3), NIST.800-53.r5 AC-2 NIST.800-53.r5 AC-3 (15), PCI DSS v4.0. 1/8.3.9, PCI DSS v4.0. 1/8.6.3

Categoría: Proteger - Administración de acceso seguro

Gravedad: media

Tipo de recurso: `AWS::IAM::User`

Regla de AWS Config: `access-keys-rotated`

Tipo de programa: Periódico

Parámetros:

- `maxAccessKeyAge: 90` (no personalizable)

Este control comprueba si las claves de acceso activas rotan en un plazo de 90 días.

Le recomendamos encarecidamente que no genere y elimine todas las claves de acceso de la cuenta. En su lugar, la mejor práctica recomendada es crear una o más funciones de IAM o utilizar la federación mediante la federación. AWS IAM Identity Center Puede utilizar estos métodos para permitir que sus usuarios accedan a Consola de administración de AWS yAWS CLI.

Cada enfoque tiene sus casos de uso. La federación es generalmente mejor para las empresas que tienen un directorio o plan central existente y prevén que van a necesitar más que el límite actual de usuarios de IAM. Las aplicaciones que se ejecutan fuera de un AWS entorno necesitan claves de acceso para acceder a AWS los recursos mediante programación.

Sin embargo, si los recursos que necesitan acceso programático se ejecutan internamenteAWS, la mejor práctica es utilizar las funciones de IAM. Los roles le permiten conceder acceso a un recurso sin codificar de forma rígida un ID de clave de acceso y una clave de acceso secreta en la configuración.

Para obtener más información sobre cómo proteger las claves de acceso y la cuenta, consulte las prácticas recomendadas para administrar las claves de AWS acceso en el. Referencia general de AWS Consulte también la entrada del blog Pautas para protegerse Cuenta de AWS mientras utiliza el acceso programático.

Si ya tiene una clave de acceso, Security Hub CSPM recomienda rotar las claves de acceso cada 90 días. La rotación de las claves de acceso reduce la posibilidad de que se utilice una clave de acceso asociada a una cuenta en peligro o cancelada. También garantiza que no se pueda acceder a los datos con una clave antigua que podría haberse perdido, revelado o robado. Actualice siempre sus aplicaciones después de rotar las claves de acceso.

Las claves de acceso constan de un ID de clave de acceso y de una clave de acceso secreta. Se utilizan para firmar las solicitudes programáticas que realiza a AWS. Los usuarios necesitan sus propias claves de acceso para realizar llamadas programáticas AWS desde las AWS CLI Herramientas para Windows PowerShell o los AWS SDK o realizar llamadas HTTP directas mediante las operaciones de la API de forma individual. Servicios de AWS

Si su organización utiliza AWS IAM Identity Center (IAM Identity Center), sus usuarios pueden iniciar sesión en Active Directory, en un directorio integrado del IAM Identity Center o en otro proveedor de identidad (IdP) conectado al IAM Identity Center. A continuación, pueden asignarse a una función de

IAM que les permita ejecutar AWS CLI comandos o realizar operaciones de AWS API sin necesidad de claves de acceso. Para obtener más información, consulte Configuración del AWS CLI uso AWS IAM Identity Center en la Guía del AWS Command Line Interfaceusuario.

> **Note**
>
> AWS Configdebe estar habilitado en todas las regiones en las que utilice Security Hub CSPM. Sin embargo, el registro de recursos globales se puede habilitar en una sola región. Si solo registra recursos globales en una única región, puede desactivar este control en todas las regiones salvo aquella en la que haya registrado los recursos globales.

Corrección

Para rotar las claves de acceso que tienen más de 90 días de antigüedad, consulte Rotación de las claves de acceso en la Guía del usuario de IAM. Siga las instrucciones para cualquier usuario cuya clave de acceso tenga más de 90 días de antigüedad.

[IAM.4] La clave de acceso del usuario raíz de IAM no debería existir

Requisitos relacionados: CIS AWS Foundations Benchmark v5.0. 0/1.3, Criterio de referencia sobre AWS los fundamentos de la CEI v3.0. 0/1.4, Punto de referencia sobre los AWS fundamentos de la CEI v1.4. 0/1.4, Criterio de referencia sobre los AWS fundamentos de la CEI v1.2. 0/1.12, PCI DSS v3.2. 1/2.1, PCI DSS v3.2. 1/2.2, PCI DSS v3.2. 1/7.2.1, NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), (10) NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6 (2) NIST.800-53.r5 AC-6

Categoría: Proteger - Administración de acceso seguro

Gravedad: crítica

Tipo de recurso: `AWS::::Account`

Regla de AWS Config: `iam-root-access-key-check`

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si está presente la clave de acceso del usuario raíz.

El usuario root es el usuario con más privilegios de unCuenta de AWS. AWSlas claves de acceso proporcionan acceso programático a una cuenta determinada.

Security Hub (CSPM) recomienda eliminar todas las claves de acceso asociadas al usuario root. Esto limita los vectores que se pueden utilizar para comprometer su cuenta. También fomenta la creación y el uso de cuentas basadas en roles, que tienen menos privilegios.

Corrección

Para eliminar la clave de acceso del usuario raíz, consulte Eliminar las claves de acceso del usuario raíz en la Guía del usuario de IAM. Para eliminar las claves de acceso del usuario raíz de una entrada Cuenta de AWSAWS GovCloud (US), consulte Eliminar las claves de acceso del usuario raíz de mi AWS GovCloud (US) cuenta en la Guía del AWS GovCloud (US)usuario.

[IAM.5] La MFA debe estar habilitada para todos los usuarios de IAM que tengan una contraseña de consola

Requisitos relacionados: CIS AWS Foundations Benchmark v5.0. 0/1.9, Criterio de referencia sobre los AWS fundamentos de la CEI v3.0. 0/1.10, punto de referencia sobre los AWS fundamentos de la CEI v1.4. 0/1.10, Criterio de referencia sobre los AWS fundamentos de la CEI v1.2. 0/1.2, NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 IA-2 (1), (2), NIST.800-53.r5 IA-2 (6), NIST.800-53.r5 IA-2 NIST.800-53.r5 IA-2 (8), PCI DSS v4.0. 1/82.4.2

Categoría: Proteger - Administración de acceso seguro

Gravedad: media

Tipo de recurso: `AWS::IAM::User`

Regla de AWS Config: `mfa-enabled-for-iam-console-access`

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si la autenticación AWS multifactor (MFA) está habilitada para todos los usuarios de IAM que utilizan una contraseña de consola.

Multi-factor la autenticación (MFA) añade una capa adicional de protección además del nombre de usuario y la contraseña. Con la MFA habilitada, cuando un usuario inicia sesión en un AWS sitio web, se le solicita su nombre de usuario y contraseña. Además, se les solicita un código de autenticación desde su dispositivo AWS MFA.

Recomendamos que habilite la MFA para todas las cuentas que tengan una contraseña de consola. MFA está diseñado para proporcionar una mayor seguridad para acceder a la consola. La entidad de autenticación debe poseer un dispositivo que emita una clave sujeta a limitación temporal y debe tener conocimiento de una credencial.

> **Note**
>
> AWS Configdebe estar habilitado en todas las regiones en las que utilice Security Hub CSPM. Sin embargo, el registro de recursos globales se puede habilitar en una sola región. Si solo registra recursos globales en una única región, puede desactivar este control en todas las regiones salvo aquella en la que haya registrado los recursos globales.

Corrección

Para agregar MFA a los usuarios de IAM, consulte Uso de la autenticación multifactor (MFA) en AWS en la Guía del usuario de IAM.

[IAM.6] La MFA de hardware debe estar habilitada para el usuario root

Requisitos relacionados: CIS AWS Foundations Benchmark v5.0. 0/1.5, Criterio de referencia sobre los AWS fundamentos de la CEI v3.0. 0/1.6, Punto de referencia sobre los AWS fundamentos de la CEI v1.4. 0/1.6, Criterio de referencia sobre los AWS fundamentos de la CEI v1.2. 0/1.14, PCI DSS v3.2. 1/8.3.1, NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), (1), NIST.800-53.r5 IA-2 (2), NIST.800-53.r5 IA-2 (6), NIST.800-53.r5 IA-2 NIST.800-53.r5 IA-2 (8), PCI DSS v4.0. 1/83.4.2

Categoría: Proteger - Administración de acceso seguro

Gravedad: crítica

Tipo de recurso: `AWS::::Account`

Regla de AWS Config: `root-account-hardware-mfa-enabled`

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si Cuenta de AWS está habilitado para usar un dispositivo de autenticación multifactor (MFA) de hardware para iniciar sesión con credenciales de usuario root. El control falla si no está habilitado MFA de hardware o si se permiten dispositivos MFA virtuales para iniciar sesión con las credenciales del usuario raíz.

Una aplicación de MFA virtual podría no proporcionar el mismo nivel de seguridad que un dispositivo MFA físico. Recomendamos que use un dispositivo MFA virtual solo mientras espera la aprobación de compra o la llegada del dispositivo de hardware. Para obtener más información, consulte Asignación de un dispositivo MFA virtual (consola) en la Guía del usuario de IAM.

> **Note**
>
> Security Hub CSPM evalúa este control en función de la presencia de credenciales de usuario raíz (perfil de inicio de sesión) en un. Cuenta de AWS El control arroja resultados `PASSED` en los siguientes casos:
>
> - Las credenciales del usuario raíz están presentes en la cuenta y MFA de hardware está habilitado para el usuario raíz.
> - Las credenciales del usuario raíz no están presentes en la cuenta.
>
> El control genera un resultado de `FAILED` si las credenciales del usuario raíz están presentes en la cuenta y MFA de hardware no está habilitado para el usuario raíz.

Corrección

Para obtener información sobre cómo habilitar la MFA de hardware para el usuario raíz, consulte la Multi-factor autenticación de un Usuario raíz de la cuenta de AWS en la Guía del usuario de IAM.

[IAM.7] Las políticas de contraseñas para los usuarios de IAM deben tener configuraciones sólidas

Requisitos relacionados: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-2 (3), (15), NIST.800-53.r5 AC-3 NIST.800-53.r5 IA-5 (1), NIST.800-171.r2 3.5.2, NIST.800-171.r2 3.5.7, NIST.800-171.r2 3.5.8, PCI DSS v4.0. 1/82.3.6, PCI DSS v4.0. 1/8.3.7, PCI DSS v4.0. 1/8.3.9, PCI DSS v4.0. 1/8.3.10.1, PCI DSS v4.0. 1/8.6.3

Categoría: Proteger - Administración de acceso seguro

Gravedad: media

Tipo de recurso: `AWS::::Account`

Regla de AWS Config: `iam-password-policy`

Tipo de programa: Periódico

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`RequireUppercaseCharacters`	Requiere que al menos haya un carácter en mayúscula en la contraseña	Booleano	`true` o `false`	`true`
`RequireLowercaseCharacters`	Requiere que al menos haya un carácter en minúscula en la contraseña	Booleano	`true` o `false`	`true`
`RequireSymbols`	Requiere que al menos haya un símbolo en la contraseña	Booleano	`true` o `false`	`true`
`RequireNumbers`	Requiere que al menos haya un número en la contraseña	Booleano	`true` o `false`	`true`
`MinimumPasswordLength`	Cantidad mínima de caracteres en la contraseña	Entero	De `8` a `128`	`8`
`PasswordReusePrevention`	Cantidad de rotaciones de contraseñas para poder reutilizar una contraseña anterior	Entero	De `12` a `24`	Sin valor predeterminado
`MaxPasswordAge`	Cantidad de días antes de que la contraseña expire	Entero	De `1` a `90`	Sin valor predeterminado

Este control comprueba si la política de contraseñas de cuenta para usuarios de IAM utiliza las siguientes configuraciones seguras. Se producirá un error en el control si la política de contraseñas no utiliza configuraciones seguras. A menos que proporcione valores de parámetros

personalizados, el CSPM de Security Hub utiliza los valores predeterminados mencionados en la tabla anterior. `MaxPasswordAge`Los parámetros `PasswordReusePrevention` y no tienen un valor predeterminado, por lo que si los excluye, Security Hub CSPM ignora el número de rotaciones de contraseñas y la antigüedad de la contraseña al evaluar este control.

Para acceder aConsola de administración de AWS, los usuarios de IAM necesitan contraseñas. Como práctica recomendada, Security Hub CSPM recomienda encarecidamente que, en lugar de crear usuarios de IAM, utilice la federación. La federación permite a los usuarios utilizar sus credenciales corporativas existentes para iniciar sesión en Consola de administración de AWS. Utilice AWS IAM Identity Center (IAM Identity Center) para crear o federar el usuario y, a continuación, asuma una función de IAM en una cuenta.

Para obtener más información sobre los proveedores de identidad y la federación, consulte Proveedores de identidad y federación en la Guía del usuario de IAM. Para obtener más información sobre IAM Identity Center, consulte la AWS IAM Identity Center Guía del usuario.

Si necesita utilizar usuarios de IAM, Security Hub CSPM recomienda que exija la creación de contraseñas de usuario seguras. Puede establecer una política de contraseñas Cuenta de AWS para especificar los requisitos de complejidad y los períodos de rotación obligatorios de las contraseñas. Al crear o cambiar una política de contraseñas, la mayoría de los ajustes de la política de contraseñas se aplican la siguiente vez que los usuarios cambien sus contraseñas. Algunos de los ajustes se aplican de forma inmediata.

Corrección

Para actualizar la política de contraseñas, consulte Configuración de una política de contraseñas de la cuenta para usuarios de IAM en la Guía del usuario de IAM.

[IAM.8] Se deben eliminar las credenciales de usuario de IAM no utilizadas

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2. 0/1.3 NIST.800-53.r5 AC-2, NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-2 (3), (15) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-3 (7), NIST.800-171.r2 3.1.2 NIST.800-53.r5 AC-6, PCI DSS v3.2. 1/81.1.4, PCI DSS v4.0. 1/8.2.6

Categoría: Proteger - Administración de acceso seguro

Gravedad: media

Tipo de recurso: `AWS::IAM::User`

Regla de AWS Config: `iam-user-unused-credentials-check`

Tipo de programa: Periódico

Parámetros:

- `maxCredentialUsageAge`: `90` (no personalizable)

Este control comprueba si los usuarios de IAM tienen contraseñas o claves de acceso activas que no se han utilizado durante 90 días.

Los usuarios de IAM pueden acceder a AWS los recursos mediante diferentes tipos de credenciales, como contraseñas o claves de acceso.

Security Hub CSPM recomienda eliminar o desactivar todas las credenciales que no se hayan utilizado durante 90 días o más. Al deshabilitar o eliminar credenciales innecesarias se reduce la oportunidad de que se utilicen credenciales asociadas a una cuenta en peligro o abandonada.

> **Note**
>
> AWS Configdebe estar habilitado en todas las regiones en las que utilice Security Hub CSPM. Sin embargo, el registro de recursos globales se puede habilitar en una sola región. Si solo registra recursos globales en una única región, puede desactivar este control en todas las regiones salvo aquella en la que haya registrado los recursos globales.

Corrección

Al ver la información del usuario en la consola de IAM, hay columnas para la antigüedad de la clave de acceso, la antigüedad de la Contraseña y la Última actividad. Si el valor en cualquiera de estas columnas es superior a 90 días, desactive las credenciales de esos usuarios.

También puede utilizar los informes de credenciales para monitorizar a los usuarios e identificar a aquellos que no tienen actividad durante 90 días o más. Puede descargar los informes de credenciales en formato `.csv` desde la consola de IAM.

Después de identificar las cuentas inactivas o las credenciales no utilizadas, desactívalas. Para obtener instrucciones, consulte Creación, cambio o eliminación de la contraseña de un usuario de IAM (consola) en la Guía del usuario de IAM.

[IAM.9] La MFA debe estar habilitada para el usuario root

Requisitos relacionados: CIS AWS Foundations Benchmark v5.0. 0/14.4, PCI DSS v3.2. 1/8.3.1, PCI DSS v4.0. 1/8.4.2, Criterio de referencia sobre los AWS fundamentos de la CEI v3.0. 0/1.5, Punto de referencia sobre los AWS fundamentos de la CEI v1.4. 0/1.5, Criterio de referencia sobre los AWS fundamentos de la CEI v1.2. 0/1.13, NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 IA-2 (1), NIST.800-53.r5 IA-2 (2), (6), NIST.800-53.r5 IA-2 (8) NIST.800-53.r5 IA-2

Categoría: Proteger - Administración de acceso seguro

Gravedad: crítica

Tipo de recurso: `AWS::::Account`

Regla de AWS Config: `root-account-mfa-enabled`

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si la autenticación multifactor (MFA) está habilitada para que el usuario raíz de IAM de Cuenta de AWS an inicie sesión en. Consola de administración de AWS El control falla si MFA no está habilitado para el usuario raíz de la cuenta.

El usuario raíz de IAM de an Cuenta de AWS tiene acceso completo a todos los servicios y recursos de la cuenta. Si la MFA está habilitada, el usuario debe introducir un nombre de usuario, una contraseña y un código de autenticación desde su dispositivo de AWS MFA para poder iniciar sesión en. Consola de administración de AWS MFA aporta una capa adicional de protección sobre el nombre de usuario y la contraseña.

Este control genera un resultado `PASSED` en los siguientes casos:

- Las credenciales del usuario raíz están presentes en la cuenta y MFA está habilitada para el usuario raíz.
- Las credenciales del usuario raíz no están presentes en la cuenta.

El control genera resultados `FAILED` si las credenciales del usuario raíz están presentes en la cuenta y MFA no está habilitada para el usuario raíz.

Corrección

Para obtener información sobre cómo habilitar la MFA para el usuario raíz de unaCuenta de AWS, consulte la Multi-factor autenticación Usuario raíz de la cuenta de AWS en la Guía del AWS Identity and Access Managementusuario.

[IAM.10] Las políticas de contraseñas para los usuarios de IAM deben tener configuraciones sólidas

Requisitos relacionados: NIST.800-171.r2 3.5.2, NIST.800-171.r2 3.5.7, NIST.800-171.r2 3.5.8, PCI DSS v3.2. 1/81.1.4, PCI DSS v3.2. 1/8.2.3, PCI DSS v3.2. 1/8.2.4, PCI DSS v3.2. 1/8.2.5

Categoría: Proteger - Administración de acceso seguro

Gravedad: media

Tipo de recurso: `AWS::::Account`

Regla de AWS Config: `iam-password-policy`

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si la política de contraseñas de cuenta para usuarios de IAM utiliza las siguientes configuraciones mínimas de PCI DSS.

- `RequireUppercaseCharacters`: requiere que al menos haya un carácter en mayúscula en la contraseña. (Valor predeterminado = `true`)
- `RequireLowercaseCharacters`: requiere que al menos haya un carácter en minúscula en la contraseña. (Valor predeterminado = `true`)
- `RequireNumbers`: requiere que al menos haya un número en la contraseña. (Valor predeterminado = `true`)
- `MinimumPasswordLength`: longitud mínima de la contraseña. (Predeterminado = 7 o más)
- `PasswordReusePrevention`: número de contraseñas antes de que se permita reutilizarlas. (Valor predeterminado = 4)
- `MaxPasswordAge`: número de días antes del vencimiento de la contraseña. (Valor predeterminado = 90)

> **Note**
>
> El 30 de mayo de 2025, Security Hub CSPM eliminó este control del estándar PCI DSS v4.0.1. La versión 4.0.1 de PCI DSS ahora requiere que las contraseñas tengan un mínimo de 8 caracteres. Este control aún se aplica al estándar PCI DSS v3.2.1, el cual tiene requisitos distintos para contraseñas.
> Para evaluar las políticas de contraseñas de las cuentas con respecto a los requisitos de la versión 4.0.1 de la PCI DSS, puede utilizar el control. IAM.7 Este control exige que las contraseñas tengan un mínimo de 8 caracteres. También admite valores personalizados para la longitud de las contraseñas y otros parámetros. El IAM.7 control forma parte del estándar PCI DSS v4.0.1 del Security Hub CSPM.

Corrección

Para actualizar su política de contraseñas y usar la configuración recomendada, consulte Establecer una política de contraseñas de cuentas para los usuarios de IAM en la Guía del usuario de IAM.

[IAM.11] Asegúrese de que la política de contraseñas de IAM requiera al menos una letra mayúscula

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2. 0/13.5, NIST.800-171.r2 3.5.7, PCI DSS v4.0. 1/8.3.6, PCI DSS v4.0. 1/8.6.3

Categoría: Proteger - Administración de acceso seguro

Gravedad: media

Tipo de recurso: `AWS::::Account`

Regla de AWS Config: `iam-password-policy`

Tipo de programa: Periódico

Parámetros: ninguno

Las políticas de contraseñas aplican, en parte, los requisitos de complejidad de las contraseñas. Utilice las políticas de contraseñas de IAM para garantizar que las contraseñas utilicen diferentes conjuntos de caracteres.

CIS recomienda que la política de contraseñas exija al menos una letra mayúscula. La configuración de una política de complejidad de contraseñas aumenta la resiliencia de la cuenta ante intentos de inicio de sesión por fuerza bruta.

Corrección

Para cambiar la política de contraseñas, consulte Configurar una política de contraseñas de cuentas para los usuarios de IAM en la Guía del usuario de IAM. Para lograr una Contraseña fuerte, seleccione Se requiere al menos una letra mayúscula del alfabeto latino (A-Z).

[IAM.12] Asegúrese de que la política de contraseñas de IAM requiera al menos una letra minúscula

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2. 0/13.6, NIST.800-171.r2 3.5.7, PCI DSS v4.0. 1/8.3.6, PCI DSS v4.0. 1/8.6.3

Categoría: Proteger - Administración de acceso seguro

Gravedad: media

Tipo de recurso: `AWS::::Account`

Regla de AWS Config: `iam-password-policy`

Tipo de programa: Periódico

Parámetros: ninguno

Las políticas de contraseñas aplican, en parte, los requisitos de complejidad de las contraseñas. Utilice las políticas de contraseñas de IAM para garantizar que las contraseñas utilicen diferentes conjuntos de caracteres. CIS recomienda que la política de contraseñas exija al menos una letra minúscula. La configuración de una política de complejidad de contraseñas aumenta la resiliencia de la cuenta ante intentos de inicio de sesión por fuerza bruta.

Corrección

Para cambiar la política de contraseñas, consulte Configurar una política de contraseñas de cuentas para los usuarios de IAM en la Guía del usuario de IAM. Para lograr una Contraseña fuerte, seleccione Se requiere al menos una letra minúscula del alfabeto latino (A-Z).

[IAM.13] Asegúrese de que la política de contraseñas de IAM requiera al menos un símbolo

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2. 0/1.7, 3.5.7 NIST.800-171.r2

Categoría: Proteger - Administración de acceso seguro

Gravedad: media

Tipo de recurso: `AWS::::Account`

Regla de AWS Config: `iam-password-policy`

Tipo de programa: Periódico

Parámetros: ninguno

Las políticas de contraseñas aplican, en parte, los requisitos de complejidad de las contraseñas. Utilice las políticas de contraseñas de IAM para garantizar que las contraseñas utilicen diferentes conjuntos de caracteres.

CIS recomienda que la política de contraseñas exija al menos un símbolo. La configuración de una política de complejidad de contraseñas aumenta la resiliencia de la cuenta ante intentos de inicio de sesión por fuerza bruta.

Corrección

Para cambiar la política de contraseñas, consulte Configurar una política de contraseñas de cuentas para los usuarios de IAM en la Guía del usuario de IAM. Para la Seguridad de la contraseña, seleccione Requerir al menos un carácter no alfanumérico.

[IAM.14] Asegúrese de que la política de contraseñas de IAM requiera al menos un número

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2. 0/14.8, NIST.800-171.r2 3.5.7, PCI DSS v4.0. 1/8.3.6, PCI DSS v4.0. 1/8.6.3

Categoría: Proteger - Administración de acceso seguro

Gravedad: media

Tipo de recurso: `AWS::::Account`

Regla de AWS Config: `iam-password-policy`

Tipo de programa: Periódico

Parámetros: ninguno

Las políticas de contraseñas aplican, en parte, los requisitos de complejidad de las contraseñas. Utilice las políticas de contraseñas de IAM para garantizar que las contraseñas utilicen diferentes conjuntos de caracteres.

CIS recomienda que la política de contraseñas exija al menos un número. La configuración de una política de complejidad de contraseñas aumenta la resiliencia de la cuenta ante intentos de inicio de sesión por fuerza bruta.

Corrección

Para cambiar la política de contraseñas, consulte Configurar una política de contraseñas de cuentas para los usuarios de IAM en la Guía del usuario de IAM. Para la Seguridad de la contraseña, seleccione Requerir al menos un número.

[IAM.15] Asegúrese de que la política de contraseñas de IAM exija una longitud de contraseña mínima de 14 o más

Requisitos relacionados: CIS AWS Foundations Benchmark v5.0. 0/1.7, Criterio de referencia sobre los AWS fundamentos de la CEI v3.0. 0/1.8, Punto de referencia sobre los AWS fundamentos de la CEI v1.4. 0/1.8, Criterio de referencia sobre los AWS fundamentos de la CEI v1.2. 0/1.9, 3.5.7 NIST.800-171.r2

Categoría: Proteger - Administración de acceso seguro

Gravedad: media

Tipo de recurso: `AWS::::Account`

Regla de AWS Config: `iam-password-policy`

Tipo de programa: Periódico

Parámetros: ninguno

Las políticas de contraseñas aplican, en parte, los requisitos de complejidad de las contraseñas. Utilice las políticas de contraseñas de IAM para garantizar que las contraseñas tengan como mínimo una determinada longitud.

CIS recomienda que la política de contraseñas exija al menos una longitud de contraseña de 14 caracteres. La configuración de una política de complejidad de contraseñas aumenta la resiliencia de la cuenta ante intentos de inicio de sesión por fuerza bruta.

Corrección

Para cambiar la política de contraseñas, consulte Configurar una política de contraseñas de cuentas para los usuarios de IAM en la Guía del usuario de IAM. Para la Longitud mínima de la contraseña, introduzca **14** o un número mayor.

[IAM.16] Asegúrese de que la política de contraseñas de IAM impida la reutilización de contraseñas

Requisitos relacionados: CIS AWS Foundations Benchmark v5.0. 0/1.8, Criterio de referencia sobre los AWS fundamentos de la CEI v3.0. 0/1.9, Punto de referencia sobre los AWS fundamentos de la CEI v1.4. 0/1.9, Criterio de referencia sobre los AWS fundamentos de la CEI v1.2. 0/1.10, NIST.800-171.r2 3.5.8, PCI DSS v4.0. 1/8.3.7

Categoría: Proteger - Administración de acceso seguro

Gravedad: baja

Tipo de recurso: `AWS::::Account`

Regla de AWS Config: `iam-password-policy`

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si el número de contraseñas que se deben recordar está establecido en 24. El control falla si el valor no es 24.

Las políticas de contraseñas de IAM pueden evitar la reutilización de una contraseña determinada por el mismo usuario.

CIS recomienda que la política de contraseñas evite la reutilización de contraseñas. Evitar la reutilización de contraseñas de aumenta la resiliencia de la cuenta frente a intentos de inicio de sesión por fuerza bruta.

Corrección

Para cambiar la política de contraseñas, consulte Configurar una política de contraseñas de cuentas para los usuarios de IAM en la Guía del usuario de IAM. Para Impedir la reutilización de la contraseña, introduzca **24**.

[IAM.17] Asegúrese de que la política de contraseñas de IAM haga caducar las contraseñas en un plazo de 90 días o menos

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2. 0/11.1, PCI DSS v4.0. 1/8.3.9, PCI DSS v4.0. 1/8.3.10.1

Categoría: Proteger - Administración de acceso seguro

Gravedad: baja

Tipo de recurso: `AWS::::Account`

Regla de AWS Config: `iam-password-policy`

Tipo de programa: Periódico

Parámetros: ninguno

Las políticas de contraseñas de IAM pueden requerir que las contraseñas se roten o que caduquen al cabo de un determinado número de días.

CIS recomienda que la política de contraseñas haga caducar las contraseñas al cabo de 90 días o menos. La reducción de la vida útil de la contraseña aumenta la resiliencia de la cuenta frente a intentos de inicio de sesión por fuerza bruta. Exigir cambios regulares de contraseña también es útil en los siguientes casos:

- Las contraseñas pueden ser robadas o estar en peligro sin que usted lo sepa. Esto puede ocurrir debido a un sistema amenazado, una vulnerabilidad de software o una amenaza interna.
- Algunos filtros web corporativas y gubernamentales o servidores proxy puede interceptar y registrar el tráfico incluso si está cifrado.
- Muchas personas utilizan la misma contraseña para muchos sistemas como, por ejemplo, trabajo, correo electrónico y personal.
- Algunas estaciones de trabajo de usuarios finales en peligro podrían tener un registrador de combinación de teclas.

Corrección

Para cambiar la política de contraseñas, consulte Configurar una política de contraseñas de cuentas para los usuarios de IAM en la Guía del usuario de IAM. Para Activar la caducidad de la contraseña, introduzca **`90`** o un número menor.

[IAM.18] Asegúrese de que se haya creado una función de soporte para gestionar los incidentes conAWS Support

Requisitos relacionados: CIS AWS Foundations Benchmark v5.0. 0/1.16, Criterio de referencia sobre los AWS fundamentos de la CEI v3.0. 0/1.17, Punto de referencia sobre los AWS fundamentos de la CEI v1.4. 0/1.17, Criterio de referencia sobre los AWS fundamentos de la CEI v1.2. 0/1.20, NIST.800-171.r2 3.1.2, PCI DSS v4.0. 1/122.10.3

Categoría: Proteger - Administración de acceso seguro

Gravedad: baja

Tipo de recurso: `AWS::::Account`

Regla de AWS Config: `iam-policy-in-use`

Tipo de programa: Periódico

Parámetros:

- `policyARN`: `arn:partition:iam::aws:policy/AWSSupportAccess` (no personalizable)
- `policyUsageType`: `ANY` (no personalizable)

AWSproporciona un centro de soporte que se puede utilizar para la notificación y respuesta a incidentes, así como para el soporte técnico y el servicio de atención al cliente.

Cree un rol de IAM para permitir que los usuarios autorizados administren incidentes con AWS Support. Al implementar los privilegios mínimos para el control de acceso, una función de IAM requerirá una política de IAM adecuada que permita el acceso al centro de soporte con el fin de gestionar los incidentes. Soporte

> **Note**
>
> AWS Configdebe estar habilitado en todas las regiones en las que utilice Security Hub CSPM. Sin embargo, el registro de recursos globales se puede habilitar en una sola región. Si solo registra recursos globales en una única región, puede desactivar este control en todas las regiones salvo aquella en la que haya registrado los recursos globales.

Corrección

Para solucionar este problema, cree un rol que permita a los usuarios autorizados administrar incidentes de Soporte.

Para crear el rol que se va a usar paraSoporteacceder

1. Abra la consola de IAM en https://console.aws.amazon.com/iam/.

2. En el panel de navegación de IAM, elija Roles y, a continuación, Crear rol.
3. En Tipo de rol, elija Otro Cuenta de AWS.
4. En el campo ID de cuenta, introduzca el Cuenta de AWS ID del usuario Cuenta de AWS al que desea conceder acceso a sus recursos.

   Si los usuarios o grupos que asumirán este rol están en la misma cuenta, introduzca el número de cuenta local.

   > **Note**
   >
   > El administrador de la cuenta especificada puede conceder permiso para asumir este rol a cualquier usuario de en esa cuenta. Para ello, el administrador asocia una política al usuario o grupo que concede permiso para la acción `sts:AssumeRole`. En esa política, el recurso debe ser el ARN del rol.

5. Elija Siguiente: permisos.
6. Busque la política administrada `AWSSupportAccess`.
7. Seleccione la casilla de verificación de la política administrada `AWSSupportAccess`.
8. Elija Siguiente: etiquetas.
9. (Opcional) Para agregar metadatos al rol, asocie etiquetas como pares clave-valor.

   Para obtener más información sobre el uso de etiquetas en IAM, consulte Etiquetado de usuarios y roles de IAM en la Guía del usuario de IAM.
10. Elija Siguiente: Revisar.
11. Escriba un nombre para el rol en Nombre de rol.

    Los nombres de los roles deben ser únicos dentro de suCuenta de AWS. No distinguen entre mayúsculas y minúsculas.
12. (Opcional) En Descripción del rol, introduzca una descripción para el nuevo rol.
13. Revise el rol y, a continuación, elija Create role (Crear rol).

[IAM.19] La MFA debe estar habilitada para todos los usuarios de IAM

Requisitos relacionados: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), (1), NIST.800-53.r5 IA-2 (2), NIST.800-53.r5 IA-2 (6), NIST.800-53.r5 IA-2 NIST.800-53.r5 IA-2 (8), NIST.800-171.r2

3.3.8, NIST.800-171.r2 3.5.3, NIST.800-171.r2 3.5.4, 3.7.5, PCI DSS v3.2 NIST.800-171.r2 . 1/83.3.1, PCI DSS v4.0. 1/8.4.2,

Categoría: Proteger - Administración de acceso seguro

Gravedad: media

Tipo de recurso: `AWS::IAM::User`

Regla de AWS Config: `iam-user-mfa-enabled`

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si los usuarios de IAM tienen habilitada la autenticación multifactor (MFA).

> **Note**
>
> AWS Configdebe estar habilitado en todas las regiones en las que utilice Security Hub CSPM. Sin embargo, el registro de recursos globales se puede habilitar en una sola región. Si solo registra recursos globales en una única región, puede desactivar este control en todas las regiones salvo aquella en la que haya registrado los recursos globales.

Corrección

Para añadir MFA a los usuarios de IAM, consulte Habilitar dispositivos de MFA para los usuarios AWS en la Guía del usuario de IAM.

[IAM.20] Evite el uso del usuario root

> **Important**
>
> Security Hub CSPM retiró este control en abril de 2024. Para obtener más información, consulte Registro de cambios de los controles del CSPM de Security Hub.

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2. 0/11.

Categoría: Proteger - Administración de acceso seguro

Gravedad: baja

Tipo de recurso: `AWS::IAM::User`

AWS Configregla: `use-of-root-account-test` (regla CSPM de Security Hub personalizada)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si hay restricciones en el uso del usuario root. Cuenta de AWS El control evalúa los siguientes recursos:

- Temas de Amazon Simple Notification Service (Amazon SNS)
- AWS CloudTrailsenderos
- Filtros métricos asociados a los CloudTrail senderos
- CloudWatch Alarmas de Amazon basadas en los filtros

Esta comprobación da como resultado `FAILED` si una o varias de las siguientes afirmaciones son verdaderas:

- No CloudTrail existe ningún rastro en la cuenta.
- Una CloudTrail ruta está habilitada, pero no configurada con al menos una ruta multirregional que incluya eventos de administración de lectura y escritura.
- Una CloudTrail ruta está habilitada, pero no está asociada a un grupo de CloudWatch registros.
- No se utiliza el filtro métrico exacto prescrito por el Center for Internet Security (CIS). El filtro métrico prescrito es `'{$.userIdentity.type="Root" && $.userIdentity.invokedBy NOT EXISTS && $.eventType !="AwsServiceEvent"}'`.
- No existe ninguna CloudWatch alarma basada en el filtro de métricas en la cuenta.
- CloudWatch las alarmas configuradas para enviar notificaciones al tema de SNS asociado no se activan en función del estado de la alarma.
- El tema de SNS no cumple con las restricciones para enviar un mensaje a un tema de SNS.
- El tema de SNS no tiene al menos un suscriptor.

Esta comprobación da como resultado `NO_DATA` si una o más de las siguientes afirmaciones son verdaderas:

- Una ruta multirregional se basa en una Región diferente. Security Hub CSPM solo puede generar hallazgos en la región en la que se encuentra el rastro.
- Una ruta multirregional pertenece a una cuenta diferente. Security Hub CSPM solo puede generar hallazgos para la cuenta propietaria del rastro.

Esta comprobación da como resultado `WARNING` si una o más de las siguientes afirmaciones son verdaderas:

- La cuenta corriente no es propietaria del tema de SNS al que se hace referencia en la alarma. CloudWatch
- La cuenta actual no tiene acceso al tema de SNS al invocar la API de SNS de `ListSubscriptionsByTopic`.

> **Note**
>
> Recomendamos utilizar los registros de la organización para registrar los eventos de varias cuentas de una organización. De forma predeterminada, los registros de la organización son registros multirregionales y solo los puede administrar la cuenta AWS Organizations de administración o la cuenta de CloudTrail administrador delegado. El uso de un registro de la organización da como resultado un estado de control de NO_DATA para los controles evaluados en las cuentas de los miembros de la organización. En las cuentas de los miembros, Security Hub CSPM solo genera hallazgos para los recursos propiedad de los miembros. Los resultados relacionados con los registros de la organización se generan en la cuenta del propietario del recurso. Puede ver estos resultados en su cuenta de administrador delegado de CSPM de Security Hub mediante la agregación entre regiones.

Como práctica recomendada, utilice sus credenciales de usuario raíz solo cuando sea necesario para realizar tareas de administración de cuentas y servicios. Aplique políticas de IAM directamente a los grupos y roles, pero no a los usuarios. Para ver las instrucciones sobre cómo configurar un administrador para el uso diario, consulte Creación del primer grupo y usuario administrador de IAM en la Guía de usuario de IAM.

Corrección

Los pasos para solucionar este problema incluyen la configuración de un tema de Amazon SNS, CloudTrail una ruta, un filtro de métricas y una alarma para el filtro de métricas.

Para crear un tema de Amazon SNS

1. Abra la consola de Amazon SNS en https://console.aws.amazon.com/sns/v3/home.
2. Cree un tema de Amazon SNS que reciba todas las alarmas de CIS.

   Cree al menos un suscriptor al tema. Para obtener más información, consulte Introducción a Amazon SNS en la Guía para desarrolladores de Amazon Simple Notification Service.

A continuación, configure un activo CloudTrail que se aplique a todas las regiones. Para ello, siga los pasos de corrección en the section called "[CloudTrail.1] CloudTrail debe estar habilitado y configurado con al menos un registro multirregional que incluya eventos de administración de lectura y escritura".

Anote el nombre del grupo de CloudWatch registros que asocie a la CloudTrail ruta. Cree el filtro de métricas en el grupo de registro.

Por último, cree el filtro métrico y la alarma.

Para crear un filtro de métricas y alarma

1. Abra la CloudWatch consola en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, seleccione Grupos de registro.
3. Seleccione la casilla de verificación del grupo de CloudWatch registros que está asociado a la CloudTrail ruta que ha creado.
4. En Acciones, elija Crear filtro de métricas.
5. En Definir patrón, haga lo siguiente:

   a. Copie el siguiente patrón y, a continuación, péguelo en el campo Filter Pattern (Patrón de filtros).

   ```
   {$.userIdentity.type="Root" && $.userIdentity.invokedBy NOT EXISTS &&
    $.eventType !="AwsServiceEvent"}
   ```

   b. Elija Siguiente.
6. En Asignar métrica, haga lo siguiente:

   a. En Nombre de filtro, escriba un nombre para el filtro de métricas.

   b. En Espacio de nombres de métrica, escriba **`LogMetrics`**.

Si usa el mismo espacio de nombres para todos los filtros de métricas de registro de CIS, todas las métricas de CIS Benchmark se agrupan.

c. Para Nombre de métrica, ingrese un nombre para la métrica. Recuerde el nombre de la métrica. Deberá seleccionar la métrica al crear la alarma.

d. En Metric Value (Valor de métrica), ingrese **1**.

e. Elija Siguiente.

7. En Revisar y crear, compruebe la información que proporcionó para el nuevo filtro de métricas. A continuación, elija Crear filtro de métrica.

8. En el panel de navegación, elija Grupos de registros y, a continuación, elija el filtro que creó en Filtros métricos.

9. Seleccione la casilla de verificación del filtro. Elija Crear alarma.

10. En Especificar métrica y condiciones, realice lo siguiente:

    a. En Condiciones, vaya a Tipo de umbral y escriba Estático.

    b. En Definir la condición de alarma, elija Greater/Equal.

    c. En Definir el valor umbral, introduzca **1**.

    d. Elija Siguiente.

11. En Configuración de acciones, haga lo siguiente:

    a. Para Desencadenador de estado de alarma, elija En alarma.

    b. En Select an SNS topic, elija Select an existing SNS topic.

    c. En Enviar notificación a, introduzca el nombre del tema de SNS que creó en el procedimiento anterior.

    d. Elija Siguiente.

12. En Añadir una descripción, escriba un nombre y la descripción de la alarma, como **`CIS-1.1-RootAccountUsage`**. A continuación, elija Siguiente.

13. En Vista previa y creación, revise la configuración de la alarma. A continuación, elija Create Alarm (Crear alarma).

[IAM.21] Las políticas de IAM gestionadas por el cliente que cree no deberían permitir acciones comodín en los servicios

Requisitos relacionados: NIST.800-53.r5 AC-2, NIST.800-53.r5 AC-2 (1), (15) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7),, NIST.800-53.r5 AC-3 (10) NIST.800-53.r5 AC-5, (2) NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6 NIST.800-53.r5 AC-6 (3), NIST.800-53.r5 AC-6 NIST.800-171.r2 3.1.1, NIST.800-171.r2 3.1.2, NIST.800-171.r2 3.1.5, NIST.800-171.r2 3.1.7, 3.3.8, 3.3.9, 3.13.3, NIST.800-171.r2 3.13.4 NIST.800-171.r2 NIST.800-171.r2 NIST.800-171.r2

Categoría: Detectar > Gestión de acceso seguro

Gravedad: baja

Tipo de recurso: `AWS::IAM::Policy`

Regla de AWS Config: `iam-policy-no-statements-with-full-access`

Tipo de horario: provocado por un cambio

Parámetros:

- `excludePermissionBoundaryPolicy`: `True` (no personalizable)

Este control comprueba si las políticas de IAM basadas en la identidad que cree incluyen instrucciones de permiso que utilizan el comodín * para conceder permisos para todas las acciones de cualquier servicio. El control falla si alguna declaración de política incluye `"Effect": "Allow"` con `"Action": "Service:*"`.

Por ejemplo, la siguiente afirmación de una política da como resultado una conclusión fallida.

```
"Statement": [
{
  "Sid": "EC2-Wildcard",
  "Effect": "Allow",
  "Action": "ec2:*",
  "Resource": "*"
}
```

El control también falla si se usa `"Effect": "Allow"` con `"NotAction": "service:*"`. En ese caso, el `NotAction` elemento proporciona acceso a todas las acciones de una, excepto a las acciones especificadas en. Servicio de AWS `NotAction`

Este control solo se aplica a las políticas de IAM administradas por el cliente. No se aplica a las políticas de IAM gestionadas por AWS.

Al asignar permisos aServicios de AWS, es importante incluir las acciones de IAM permitidas en sus políticas de IAM. Debe restringir las acciones de IAM solo a las acciones que sean necesarias. Esto le ayuda a proporcionar permisos con privilegios mínimos. Las políticas demasiado permisivas pueden provocar una escalada de privilegios si las políticas están vinculadas a un director de IAM que podría no requerir el permiso.

En algunos casos, es posible que desee permitir acciones de IAM que tienen un prefijo similar, como `DescribeFlowLogs` y `DescribeAvailabilityZones`. En estos casos autorizados, puede añadir un comodín con sufijo al prefijo común. Por ejemplo, `ec2:Describe*`.

Este control se activa si utiliza una acción de IAM con un prefijo con un comodín con sufijo. Por ejemplo, la siguiente declaración de una política da como resultado que se aprueba una conclusión.

```
"Statement": [
{
  "Sid": "EC2-Wildcard",
  "Effect": "Allow",
  "Action": "ec2:Describe*",
  "Resource": "*"
}
```

Si agrupa las acciones de IAM relacionadas de esta manera, también puede evitar superar los límites de tamaño de las políticas de IAM.

> **Note**
>
> AWS Configdebe estar habilitado en todas las regiones en las que utilice Security Hub CSPM. Sin embargo, el registro de recursos globales se puede habilitar en una sola región. Si solo registra recursos globales en una única región, puede desactivar este control en todas las regiones salvo aquella en la que haya registrado los recursos globales.

Corrección

Para solucionar este problema, actualice sus políticas de IAM para que no permitan todos los privilegios administrativos “*”. Para conocer los detalles acerca de cómo editar una política de IAM, consulte Edición de políticas de IAM en la Guía del usuario de IAM.

[IAM.22] Se deben eliminar las credenciales de usuario de IAM que no se hayan utilizado durante 45 días

Requisitos relacionados: CIS AWS Foundations Benchmark v5.0. 0/1.11, Criterio de referencia sobre los AWS fundamentos de la CEI v3.0. 0/1.12, Punto de referencia sobre los AWS fundamentos de la CEI v1.4. 0/1.12, 3.1.2 NIST.800-171.r2

Categoría: Proteger - Administración de acceso seguro

Gravedad: media

Tipo de recurso: `AWS::IAM::User`

AWS Configregla: **`iam-user-unused-credentials-check`**

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si los usuarios de IAM tienen contraseñas o claves de acceso activas que no se han utilizado durante 45 días o más. Para ello, comprueba si el `maxCredentialUsageAge` parámetro de la AWS Config regla es igual o superior a 45.

Los usuarios pueden acceder a AWS los recursos mediante diferentes tipos de credenciales, como contraseñas o claves de acceso.

CIS recomienda que elimine o desactive todas las credenciales que han dejado de utilizarse durante 45 días o más. Al deshabilitar o eliminar credenciales innecesarias se reduce la oportunidad de que se utilicen credenciales asociadas a una cuenta en peligro o abandonada.

La AWS Config regla para este control utiliza las operaciones `GetCredentialReport`y la `GenerateCredentialReport`API, que solo se actualizan cada cuatro horas. Los cambios en los usuarios de IAM pueden tardar hasta cuatro horas en ser visibles para este control.

> **Note**
>
> AWS Configdebe estar habilitado en todas las regiones en las que utilice Security Hub CSPM. Sin embargo, puede habilitar el registro de los recursos globales en una sola región. Si solo registra recursos globales en una única región, puede desactivar este control en todas las regiones salvo aquella en la que haya registrado los recursos globales.

Corrección

Al ver la información del usuario en la consola de IAM, hay columnas para la antigüedad de la clave de acceso, la antigüedad de la Contraseña y la Última actividad. Si el valor en cualquiera de estas columnas es superior a 45 días, desactive las credenciales de esos usuarios.

También puede utilizar los informes de credenciales para monitorizar a los usuarios e identificar a aquellos que no tienen actividad durante 45 días o más. Puede descargar los informes de credenciales en formato `.csv` desde la consola de IAM.

Después de identificar las cuentas inactivas o las credenciales no utilizadas, desactívalas. Para obtener instrucciones, consulte Creación, cambio o eliminación de la contraseña de un usuario de IAM (consola) en la Guía del usuario de IAM.

[IAM.23] Los analizadores de IAM Access Analyzer deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::AccessAnalyzer::Analyzer`

AWS Configregla: `tagged-accessanalyzer-analyzer` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	`No default value`

Este control comprueba si un analizador gestionado por AWS Identity and Access Management Access Analyzer (IAM Access Analyzer) tiene etiquetas con las claves específicas definidas en el parámetro. `requiredTagKeys` El control lanza error si el analizador no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si el analizador no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte Etiquetar sus AWS recursos en el. Referencia general de AWS

Corrección

Para agregar etiquetas a un analizador, consulte TagResource en la Referencia de la API del Analizador de acceso de AWS IAM.

[IAM.24] Las funciones de IAM deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::IAM::Role`

AWS Configregla: `tagged-iam-role` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	`No default value`

Este control comprueba si un rol AWS Identity and Access Management (de IAM) tiene etiquetas con las claves específicas definidas en el parámetro`requiredTagKeys`. El control lanza error si el rol no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si el rol no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan

operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte Etiquetar sus AWS recursos en el. Referencia general de AWS

Corrección

Para agregar etiquetas a un rol de IAM, consulte Etiquetado de recursos de IAM en la Guía del usuario de IAM.

[IAM.25] Los usuarios de IAM deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::IAM::User`

AWS Configregla: `tagged-iam-user` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que	`No default value`

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
	recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.		cumplan los requisitos de AWS.	

Este control comprueba si un usuario AWS Identity and Access Management (de IAM) tiene etiquetas con las claves específicas definidas en el parámetro`requiredTagKeys`. El control lanza error si el usuario no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si el usuario no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte Etiquetar sus AWS recursos en el. Referencia general de AWS

Corrección

Para agregar etiquetas a un usuario de IAM, consulte Etiquetado de recursos de IAM en la Guía del usuario de IAM.

[IAM.26] SSL/TLS Los certificados caducados gestionados en IAM deben eliminarse

Requisitos relacionados: CIS AWS Foundations Benchmark v5.0. 0/1.18, Criterio de referencia sobre los AWS fundamentos de la CEI v3.0. 0/1.19

Categoría: Identificar > Cumplimiento

Gravedad: media

Tipo de recurso: `AWS::IAM::ServerCertificate`

AWS Configregla: **`iam-server-certificate-expiration-check`**

Tipo de programa: Periódico

Parámetros: ninguno

Esto controla si un certificado de SSL/TLS servidor activo que se administra en IAM ha caducado. El control produce un error si no se elimina el certificado de SSL/TLS servidor caducado.

Para habilitar las conexiones HTTPS a tu sitio web o aplicaciónAWS, necesitas un certificado de SSL/TLS servidor. Puede usar IAM o AWS Gestor de certificados (ACM) para almacenar e implementar certificados de servidor. Utilice IAM como administrador de certificados solo cuando deba admitir conexiones HTTPS en un entorno Región de AWS que no sea compatible con ACM. IAM cifra de forma segura sus claves privadas y almacena la versión cifrada en el almacenamiento de certificados SSL de IAM. IAM admite el despliegue de certificados de servidor en todas las regiones, pero debe obtener su certificado de un proveedor externo para poder utilizarlo con ellos. AWS No se puede cargar un certificado de ACM en IAM. Además, no se puede administrar los certificados desde la consola de IAM. Al eliminar SSL/TLS los certificados caducados, se elimina el riesgo de que un certificado no válido se distribuya accidentalmente en un recurso, lo que puede dañar la credibilidad de la aplicación o el sitio web subyacentes.

Corrección

Para eliminar un certificado de servidor de IAM, consulte Administración de los certificados de servidor en IAM en la Guía del usuario de IAM.

[IAM.27] Las identidades de IAM no deberían tener la AWSCloudShellFullAccess política adjunta

Requisitos relacionados: CIS AWS Foundations Benchmark v5.0. 0/1.21, Criterio de referencia sobre los AWS fundamentos de la CEI v3.0. 0/12.2

Categoría: Proteger > Administración de acceso seguro > Políticas de IAM seguras

Gravedad: media

Tipo de recurso: `AWS::IAM::Role`, `AWS::IAM::User`, `AWS::IAM::Group`

AWS Configregla: **`iam-policy-blacklisted-check`**

Tipo de horario: provocado por un cambio

Parámetros:

- «PolicYarns»: «arn:aws:iam: :aws:, arn:aws-cn:iam: :aws:, arn:aws-us-gov:iam: :awspolicy/AWSCloudShellFullAccess:» policy/AWSCloudShellFullAccess policy/AWSCloudShellFullAccess

Este control comprueba si una identidad de IAM (usuario, función o grupo) tiene asociada la política gestionadaAWS. `AWSCloudShellFullAccess` El control lanza error si una identidad de IAM tiene la política `AWSCloudShellFullAccess` adjunta.

AWS CloudShellproporciona una forma cómoda de ejecutar comandos CLI contraServicios de AWS. La política AWS gestionada `AWSCloudShellFullAccess` proporciona acceso total a CloudShell, lo que permite cargar y descargar archivos entre el sistema local del usuario y el CloudShell entorno. Dentro del CloudShell entorno, un usuario tiene permisos de sudo y puede acceder a Internet. Como resultado, adjuntar esta política gestionada a una identidad de IAM les permite instalar software de transferencia de archivos y mover datos desde CloudShell servidores de Internet externos. Recomendamos seguir el principio de privilegio mínimo y adjuntar permisos más limitados a las identidades de IAM.

Corrección

Para desasociar la política `AWSCloudShellFullAccess` de una identidad de IAM, consulte Cómo agregar y eliminar permisos de identidad de IAM en la Guía del usuario de IAM.

[IAM.28] El analizador de acceso externo de IAM Access Analyzer debe estar habilitado

Requisitos relacionados: CIS AWS Foundations Benchmark v5.0. 0/1.19, Criterio de referencia sobre los AWS fundamentos de la CEI v3.0. 0/1.20

Categoría: Detectar > Servicios de detección > Supervisión de uso con privilegios

Gravedad: alta

Tipo de recurso: `AWS::AccessAnalyzer::Analyzer`

AWS Configregla: **`iam-external-access-analyzer-enabled`**

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si un Cuenta de AWS analizador de acceso externo de IAM Access Analyzer está activado. El control lanza error si la cuenta no tiene un analizador de acceso externo habilitado en la Región de AWS seleccionada.

Los analizadores de acceso externo del Analizador de acceso de IAM ayudan a identificar recursos, como buckets de Amazon Simple Storage Service (Amazon S3) o roles de IAM, que se comparten con una entidad externa. De esta manera, se evita el acceso no deseado a los recursos y los datos. El Analizador de acceso de IAM es regional y debe estar habilitado en cada región. Para identificar los recursos que se comparten con entidades externas, un analizador de acceso utiliza un razonamiento basado en la lógica para analizar las políticas basadas en los recursos de su entorno. AWS Cuando crea un analizador de acceso externo, puede crearlo y habilitarlo para toda la organización o para cuentas individuales.

> **Note**
>
> Si una cuenta forma parte de una organizaciónAWS Organizations, este control no tiene en cuenta los analizadores de acceso externos que especifican la organización como zona de confianza y están habilitados para la organización en la región actual. Si la organización usa este tipo de configuración, considere desactivar este control para las cuentas de miembro individuales en la organización en la región.

Corrección

Para obtener información sobre cómo habilitar un analizador de acceso externo en una región específica, consulte tag Introducción al Analizador de acceso de IAM en la Guía del usuario de IAM. Debe habilitar un analizador en cada región en la que desee supervisar el acceso a sus recursos.

Controles CSPM de Security Hub para Amazon Inspector

Estos AWS Security Hub CSPM controles evalúan el servicio y los recursos de Amazon Inspector.

Es posible que estos controles no estén disponibles en todosRegiones de AWS. Para obtener más información, consulte Disponibilidad de los controles por región.

[Inspector.1] El escaneo EC2 de Amazon Inspector debe estar activado

Requisitos relacionados: PCI DSS v4.0. 1/113.3.1

Categoría: Detectar - Servicios de detección

Gravedad: alta

Tipo de recurso: `AWS::::Account`

Regla de AWS Config: `inspector-ec2-scan-enabled`

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si está habilitado el análisis de EC2 en Amazon Inspector. En el caso de una cuenta independiente, el control lanza un error si el análisis de EC2 en Amazon Inspector está desactivado en la cuenta. En un entorno con varias cuentas, el control lanza un error si ni la cuenta de administrador delegado de Amazon Inspector ni ninguna de las cuentas de los miembros tienen habilitado el análisis de EC2.

En un entorno con varias cuentas, el control genera resultados solo en la cuenta de administrador delegado de Amazon Inspector. Solo el administrador delegado puede activar o desactivar la característica de análisis de EC2 para las cuentas de los miembros en la organización. Los miembros de Amazon Inspector no pueden modificar esta configuración desde sus cuentas. Este control genera resultados `FAILED` si el administrador delegado tiene una cuenta de miembro suspendida que no tiene habilitado el análisis de EC2 en Amazon Inspector. Para recibir un resultado `PASSED`, el administrador delegado debe desvincular estas cuentas suspendidas en Amazon Inspector.

El análisis de EC2 en Amazon Inspector extrae metadatos de su instancia de Amazon Elastic Compute Cloud (Amazon EC2) y, a continuación, los compara con las reglas recopiladas en los avisos de seguridad para generar resultados. Amazon Inspector analiza las instancias en busca de vulnerabilidades en los paquetes y problemas de accesibilidad a la red. Para obtener información

sobre los sistemas operativos compatibles, incluido el sistema operativo que se puede analizar sin un agente SSM, consulte Sistemas operativos compatibles: análisis de Amazon EC2.

Corrección

Para activar el análisis de EC2 en Amazon Inspector, consulte Activación de análisis en la Guía del usuario de Amazon Inspector.

[Inspector.2] El escaneo ECR de Amazon Inspector debe estar activado

Requisitos relacionados: PCI DSS v4.0. 1/113.3.1

Categoría: Detectar - Servicios de detección

Gravedad: alta

Tipo de recurso: `AWS::::Account`

Regla de AWS Config: `inspector-ecr-scan-enabled`

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si está habilitado el análisis de ECR en Amazon Inspector. En el caso de una cuenta independiente, el control lanza un error si el análisis de ECR en Amazon Inspector está desactivado en la cuenta. En un entorno con varias cuentas, el control lanza un error si ni la cuenta de administrador delegado de Amazon Inspector ni ninguna de las cuentas de los miembros tienen habilitado el análisis de ECR.

En un entorno con varias cuentas, el control genera resultados solo en la cuenta de administrador delegado de Amazon Inspector. Solo el administrador delegado puede activar o desactivar la característica de análisis de ECR para las cuentas de los miembros en la organización. Los miembros de Amazon Inspector no pueden modificar esta configuración desde sus cuentas. Este control genera resultados `FAILED` si el administrador delegado tiene una cuenta de miembro suspendida que no tiene habilitado el análisis de ECR en Amazon Inspector. Para recibir un resultado `PASSED`, el administrador delegado debe desvincular estas cuentas suspendidas en Amazon Inspector.

Amazon Inspector analiza las imágenes de contenedores almacenadas en Amazon Elastic Container Registry (Amazon ECR) en busca de vulnerabilidades en el software para generar resultados de vulnerabilidades de paquetes. Al activar los análisis de Amazon Inspector para Amazon ECR, se

configura Amazon Inspector como servicio de análisis preferido para su registro privado. Amazon Inspector reemplaza los análisis básicos, que se ofrecen de forma gratuita en Amazon ECR, por análisis mejorados, que se ofrecen y facturan a través de Amazon Inspector. Los análisis mejorados le ofrecen la ventaja de analizar vulnerabilidades tanto de sistemas operativos como de paquetes de lenguajes de programación en el nivel de registro. Puede revisar los resultados descubiertos a partir de análisis mejorados en el nivel de imagen, para cada capa de la imagen, en la consola de Amazon ECR. Además, puedes revisar estos resultados y trabajar con ellos en otros servicios que no están disponibles para los resultados de digitalización básicos, como AWS Security Hub CSPM Amazon EventBridge.

Corrección

Para habilitar el análisis de ECR en Amazon Inspector, consulte Activating scans en la Guía del usuario de Amazon Inspector.

[Inspector.3] El escaneo de código Lambda de Amazon Inspector Lambda debe estar activado

Requisitos relacionados: PCI DSS v4.0. 1/62.2.4, PCI DSS v4.0. 1/63.3.1

Categoría: Detectar - Servicios de detección

Gravedad: alta

Tipo de recurso: `AWS::::Account`

Regla de AWS Config: `inspector-lambda-code-scan-enabled`

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si está habilitado el análisis de código de Lambda en Amazon Inspector. En el caso de una cuenta independiente, el control lanza un error si el análisis de código de Lambda en Amazon Inspector está desactivado en la cuenta. En un entorno de varias cuentas, el control lanza un error si ni la cuenta de administrador delegado de Amazon Inspector ni ninguna de las cuentas de los miembros tienen habilitado el análisis de código de Lambda.

En un entorno con varias cuentas, el control genera resultados solo en la cuenta de administrador delegado de Amazon Inspector. Solo el administrador delegado puede activar o desactivar la característica de análisis de código de Lambda para las cuentas de los miembros en la organización. Los miembros de Amazon Inspector no pueden modificar esta configuración desde sus cuentas. Este control genera resultados `FAILED` si el administrador delegado tiene una cuenta de miembro

suspendida que no tiene habilitado el análisis de códigos de Lambda en Amazon Inspector. Para recibir un resultado `PASSED`, el administrador delegado debe desvincular estas cuentas suspendidas en Amazon Inspector.

El escaneo de código Lambda de Amazon Inspector analiza el código de la aplicación personalizada dentro de una AWS Lambda función para detectar vulnerabilidades en el código según las prácticas recomendadas AWS de seguridad. El análisis de código de Lambda puede detectar fallos de inyección, fugas de datos, errores de criptografía débil o una falta de cifrado en el código. Esta función Regiones de AWSsolo está disponible de forma específica. Puede activar el análisis de código de Lambda junto al análisis estándar de Lambda (consulte [Inspector.4] El escaneo estándar de Amazon Inspector Lambda debe estar activado).

Corrección

Para habilitar el análisis de código de Lambda en Amazon Inspector, consulte Activación de análisis en la Guía del usuario de Amazon Inspector.

[Inspector.4] El escaneo estándar de Amazon Inspector Lambda debe estar activado

Requisitos relacionados: PCI DSS v4.0. 1/62.2.4, PCI DSS v4.0. 1/63.3.1

Categoría: Detectar - Servicios de detección

Gravedad: alta

Tipo de recurso: `AWS::::Account`

Regla de AWS Config: `inspector-lambda-standard-scan-enabled`

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si está habilitado el análisis estándar de Lambda en Amazon Inspector. En el caso de una cuenta independiente, el control lanza un error si el análisis estándar de Lambda en Amazon Inspector está desactivado en la cuenta. En un entorno de varias cuentas, el control lanza un error si ni la cuenta de administrador delegado de Amazon Inspector ni ninguna de las cuentas de los miembros tienen habilitado el análisis estándar de Lambda.

En un entorno con varias cuentas, el control genera resultados solo en la cuenta de administrador delegado de Amazon Inspector. Solo el administrador delegado puede activar o desactivar la característica de análisis estándar de Lambda para las cuentas de los miembros en la organización.

Los miembros de Amazon Inspector no pueden modificar esta configuración desde sus cuentas. Este control genera resultados `FAILED` si el administrador delegado tiene una cuenta de miembro suspendida que no tiene habilitado el análisis estándar de Lambda en Amazon Inspector. Para recibir un resultado `PASSED`, el administrador delegado debe desvincular estas cuentas suspendidas en Amazon Inspector.

El escaneo estándar de Amazon Inspector Lambda identifica las vulnerabilidades de software en las dependencias del paquete de aplicaciones que añada al código y las capas de AWS Lambda función. Si Amazon Inspector detecta una vulnerabilidad en las dependencias del paquete de la aplicación de la función de Lambda, Amazon Inspector genera un resultado detallado del tipo `Package Vulnerability`. Puede activar el análisis de código de Lambda junto al análisis estándar de Lambda (consulte [Inspector.3] El escaneo de código Lambda de Amazon Inspector Lambda debe estar activado).

Corrección

Para habilitar el análisis estándar de Lambda en Amazon Inspector, consulte Activación de análisis en la Guía del usuario de Amazon Inspector.

Controles CSPM de Security Hub paraAWS IoT

Estos AWS Security Hub CSPM controles evalúan el AWS IoT servicio y los recursos.

Es posible que estos controles no estén disponibles en todosRegiones de AWS. Para obtener más información, consulte Disponibilidad de los controles por región.

[IoT.1]AWS IoT Device Defenderlos perfiles de seguridad deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::IoT::SecurityProfile`

AWS Configregla: `tagged-iot-securityprofile` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	`No default value`

Este control comprueba si un perfil de AWS IoT Device Defender seguridad tiene etiquetas con las claves específicas definidas en el parámetro`requiredTagKeys`. El control lanza un error si el perfil de seguridad no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si el perfil de seguridad no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte Etiquetar sus AWS recursos en el. Referencia general de AWS

Corrección

Para añadir etiquetas a un perfil AWS IoT Device Defender de seguridad, consulte Etiquetar AWS IoT los recursos en la AWS IoT Guía para desarrolladores.

[IoT.2]AWS IoT Corelas acciones de mitigación deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::IoT::MitigationAction`

AWS Configregla: `tagged-iot-mitigationaction` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	`No default value`

Este control comprueba si una acción de AWS IoT Core mitigación tiene etiquetas con las claves específicas definidas en el parámetro`requiredTagKeys`. El control lanza un error si la acción de mitigación no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si la acción de mitigación no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte Etiquetar sus AWS recursos en el. Referencia general de AWS

Corrección

Para añadir etiquetas a una acción de AWS IoT Core mitigación, consulta Cómo etiquetar tus AWS IoT recursos en la AWS IoT Guía para desarrolladores.

[IoT.3]AWS IoT Corelas dimensiones deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::IoT::Dimension`

AWS Configregla: `tagged-iot-dimension` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	`No default value`

Este control comprueba si una AWS IoT Core dimensión tiene etiquetas con las claves específicas definidas en el parámetro`requiredTagKeys`. El control lanza un error si la dimensión no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si la dimensión no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan

operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte Etiquetar sus AWS recursos en el. Referencia general de AWS

Corrección

Para añadir etiquetas a una AWS IoT Core dimensión, consulta Cómo etiquetar tus AWS IoT recursos en la AWS IoT Guía para desarrolladores.

[IoT.4]AWS IoT Corelos autorizadores deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::IoT::Authorizer`

AWS Configregla: `tagged-iot-authorizer` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que	`No default value`

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
	recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.		cumplan los requisitos de AWS.	

Este control comprueba si un AWS IoT Core autorizador tiene etiquetas con las claves específicas definidas en el parámetro`requiredTagKeys`. El control lanza un error si el autorizador no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si el autorizador no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte Etiquetar sus AWS recursos en el. Referencia general de AWS

Corrección

Para añadir etiquetas a un AWS IoT Core autorizador, consulta Cómo etiquetar tus AWS IoT recursos en la Guía para desarrolladores. AWS IoT

[IoT.5]AWS IoT CoreLos alias de los roles deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::IoT::RoleAlias`

AWS Configregla: `tagged-iot-rolealias` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	`No default value`

Este control comprueba si el alias de un AWS IoT Core rol tiene etiquetas con las claves específicas definidas en el parámetro`requiredTagKeys`. El control lanza un error si el alias de un rol no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si el alias de un rol no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte Etiquetar sus AWS recursos en el. Referencia general de AWS

Corrección

Para añadir etiquetas a un alias de AWS IoT Core rol, consulta Cómo etiquetar tus AWS IoT recursos en la AWS IoT Guía para desarrolladores.

[IoT.6]AWS IoT Corelas políticas deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::IoT::Policy`

AWS Configregla: `tagged-iot-policy` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	`No default value`

Este control comprueba si una AWS IoT Core política tiene etiquetas con las claves específicas definidas en el parámetro`requiredTagKeys`. El control lanza un error si la política no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si la política no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre

ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte Etiquetar sus AWS recursos en el. Referencia general de AWS

Corrección

Para añadir etiquetas a una AWS IoT Core política, consulta Cómo etiquetar tus AWS IoT recursos en la AWS IoT Guía para desarrolladores.

Controles CSPM de Security Hub paraAWSIoT SiteWise

Estos AWS Security Hub CSPM controles evalúan el SiteWise servicio y los recursos de AWS IoT.

Es posible que estos controles no estén disponibles en todosRegiones de AWS. Para obtener más información, consulte Disponibilidad de los controles por región.

[IoTSiteWise.1]AWSLos modelos SiteWise de activos de IoT deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::IoTSiteWise::AssetModel`

Regla de AWS Config: `iotsitewise-asset-model-tagged`

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredKeyTags`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los	Sin valor predeterminado

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
	de etiquetas distinguen entre mayúsculas y minúsculas.		requisitos de AWS.	

Este control comprueba si un modelo de SiteWise activos de AWS IoT tiene etiquetas con las claves específicas definidas en el parámetro`requiredKeyTags`. El control falla si el modelo de activos no tiene ninguna clave de etiqueta o si no incluye todas las claves especificadas en el parámetro `requiredKeyTags`. Si no se especifica el parámetro `requiredKeyTags`, el control solo verifica la existencia de una clave de etiqueta y falla si el modelo de activos no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte Definición de permisos basados en atributos con autorización ABAC en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado,

consulte las mejores prácticas y estrategias en los AWSrecursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para añadir etiquetas a un modelo de SiteWise activos de AWS IoT, consulte Etiquete sus AWS IoT SiteWise recursos en la Guía del AWS IoT SiteWise usuario.

[IoTSiteWise.2]AWS SiteWise Los paneles de IoT deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::IoTSiteWise::Dashboard`

Regla de AWS Config: `iotsitewise-dashboard-tagged`

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredKeyTags`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si un SiteWise panel de AWS IoT tiene etiquetas con las claves específicas definidas en el parámetro`requiredKeyTags`. El control falla si el panel no tiene ninguna clave de etiqueta o si no incluye todas las claves especificadas en el parámetro `requiredKeyTags`. Si no se

proporciona el parámetro `requiredKeyTags`, el control solo verifica la existencia de una clave de etiqueta y falla si el panel no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte Definición de permisos basados en atributos con autorización ABAC en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte las mejores prácticas y estrategias en los AWSrecursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para añadir etiquetas a un SiteWise panel de AWS IoT, consulta Cómo etiquetar tus AWS IoT SiteWise recursos en la Guía del AWS IoT SiteWise usuario.

[IoTSiteWise.3]AWS SiteWise Las pasarelas de IoT deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::IoTSiteWise::Gateway`

Regla de AWS Config: `iotsitewise-gateway-tagged`

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredKeyTags`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si una SiteWise pasarela de AWS IoT tiene etiquetas con las claves específicas definidas en el parámetro`requiredKeyTags`. El control lanza error si la puerta de enlace no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredKeyTags`. Si no se proporciona el parámetro `requiredKeyTags`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si la puerta de enlace no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte Definición de permisos basados en atributos con autorización ABAC en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte las mejores prácticas y estrategias en los AWSrecursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para agregar etiquetas a una SiteWise puerta de enlace de AWS IoT, consulte Etiquete sus AWS IoT SiteWise recursos en la Guía del AWS IoT SiteWise usuario.

[IoTSiteWise.4]AWS SiteWise Los portales de IoT deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::IoTSiteWise::Portal`

Regla de AWS Config: `iotsitewise-portal-tagged`

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredKeyTags`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si un SiteWise portal de AWS IoT tiene etiquetas con las claves específicas definidas en el parámetro`requiredKeyTags`. El control falla si el portal no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredKeyTags`. Si no se proporciona el parámetro `requiredKeyTags`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si el portal no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte Definición de permisos basados en atributos con autorización ABAC en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte las mejores prácticas y estrategias en los AWSrecursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para añadir etiquetas a un SiteWise portal de AWS IoT, consulte Etiquete sus AWS IoT SiteWise recursos en la Guía del AWS IoT SiteWise usuario.

[IoTSiteWise.5]AWS SiteWise Los proyectos de IoT deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::IoTSiteWise::Project`

Regla de AWS Config: `iotsitewise-project-tagged`

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredKeyTags`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si un SiteWise proyecto de AWS IoT tiene etiquetas con las claves específicas definidas en el parámetro`requiredKeyTags`. El control falla si el proyecto no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredKeyTags`. Si no se proporciona el parámetro `requiredKeyTags`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si el proyecto no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para

sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte Definición de permisos basados en atributos con autorización ABAC en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte las mejores prácticas y estrategias en los AWSrecursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para añadir etiquetas a un SiteWise proyecto de AWS IoT, consulte Etiquetar sus AWS IoT SiteWise recursos en la Guía del AWS IoT SiteWise usuario.

Controles CSPM de Security Hub paraAWSIoT TwinMaker

Estos AWS Security Hub CSPM controles evalúan el TwinMaker servicio y los recursos de AWS IoT.

Es posible que estos controles no estén disponibles en todosRegiones de AWS. Para obtener más información, consulte Disponibilidad de los controles por región.

[IoTTwinMaker.1]AWSLos trabajos de TwinMaker sincronización de IoT deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::IoTTwinMaker::SyncJob`

Regla de AWS Config: `iottwinmaker-sync-job-tagged`

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredKeyTags`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si un trabajo de TwinMaker sincronización de AWS IoT tiene etiquetas con las claves específicas definidas en el parámetro`requiredKeyTags`. El control falla si el trabajo de sincronización no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredKeyTags`. Si no se proporciona el parámetro `requiredKeyTags`, el control solo comprueba la existencia de una clave de etiqueta y falla si el trabajo de sincronización no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte Definición de permisos basados en atributos con autorización ABAC en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte las mejores prácticas y estrategias en los AWSrecursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para añadir etiquetas a un trabajo de TwinMaker sincronización de AWS IoT, consulte TagResourcela Guía del AWS IoT TwinMaker usuario.

[IoTTwinMaker.2]AWS TwinMaker Los espacios de trabajo de IoT deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::IoTTwinMaker::Workspace`

Regla de AWS Config: `iottwinmaker-workspace-tagged`

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredKeyTags`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si un TwinMaker espacio de trabajo de AWS IoT tiene etiquetas con las claves específicas definidas en el parámetro`requiredKeyTags`. El control lanza error si el espacio de trabajo no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredKeyTags`. Si no se proporciona el parámetro `requiredKeyTags`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si el espacio de trabajo no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte Definición de permisos basados en atributos con autorización ABAC en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte las mejores prácticas y estrategias en los AWSrecursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para añadir etiquetas a un espacio de TwinMaker trabajo de AWS IoT, consulte TagResourcela Guía del AWS IoT TwinMaker usuario.

[IoTTwinMaker.3]AWS TwinMaker Las escenas de IoT deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::IoTTwinMaker::Scene`

Regla de AWS Config: `iottwinmaker-scene-tagged`

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredKeyTags`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si una TwinMaker escena de AWS IoT tiene etiquetas con las claves específicas definidas en el parámetro`requiredKeyTags`. El control falla si la escena no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredKeyTags`. Si no se proporciona el parámetro `requiredKeyTags`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si la escena no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS

los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte Definición de permisos basados en atributos con autorización ABAC en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte las mejores prácticas y estrategias en los AWSrecursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para añadir etiquetas a una TwinMaker escena de AWS IoT, consulte TagResourcela Guía del AWS IoT TwinMaker usuario.

[IoTTwinMaker.4]AWS TwinMaker Las entidades de IoT deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::IoTTwinMaker::Entity`

Regla de AWS Config: `iottwinmaker-entity-tagged`

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredKeyTags`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si una TwinMaker entidad de AWS IoT tiene etiquetas con las claves específicas definidas en el parámetro`requiredKeyTags`. El control falla si la entidad no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredKeyTags`. Si el parámetro `requiredKeyTags` no está definido, el control solo verifica la existencia de una clave de etiqueta y falla si la entidad no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte Definición de permisos basados en atributos con autorización ABAC en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte las mejores prácticas y estrategias en los AWSrecursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para añadir etiquetas a una TwinMaker entidad de AWS IoT, consulte TagResourcela Guía del AWS IoT TwinMaker usuario.

Controles CSPM de Security Hub paraAWSIoT Wireless

Estos AWS Security Hub CSPM controles evalúan el servicio y los recursos de AWS IoT Wireless.

Es posible que estos controles no estén disponibles en todosRegiones de AWS. Para obtener más información, consulte Disponibilidad de los controles por región.

[IoTWireless.1]AWSLos grupos de multidifusión de IoT Wireless deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::IoTWireless::MulticastGroup`

Regla de AWS Config: `iotwireless-multicast-group-tagged`

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredKeyTags`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si un grupo de multidifusión de AWS IoT Wireless tiene etiquetas con las claves específicas definidas en el parámetro`requiredKeyTags`. El control lanza un error si el grupo de multidifusión no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredKeyTags`. Si no se proporciona el parámetro `requiredKeyTags`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si el grupo de multidifusión no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte Definición de permisos basados en atributos con autorización ABAC en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte las mejores prácticas y estrategias en los AWSrecursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para agregar etiquetas a un grupo de multidifusión de AWS IoT Wireless, consulte Etiquetar sus AWS IoT Wireless recursos en la Guía para AWS IoT Wireless desarrolladores.

[IoTWireless.2]AWSLos perfiles de servicio de IoT Wireless deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::IoTWireless::ServiceProfile`

Regla de AWS Config: `iotwireless-service-profile-tagged`

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredKeyTags`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si un perfil de servicio AWS IoT Wireless tiene etiquetas con las claves específicas definidas en el parámetro`requiredKeyTags`. El control falla si el perfil de servicio no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredKeyTags`. Si no se proporciona el parámetro `requiredKeyTags`, el control solo comprueba la existencia de una clave de etiqueta y falla si el perfil de servicio no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte Definición de permisos basados en atributos con autorización ABAC en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte las mejores prácticas y estrategias en los AWSrecursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para añadir etiquetas a un perfil de servicio de AWS IoT Wireless, consulte Etiquetar sus AWS IoT Wireless recursos en la Guía para AWS IoT Wireless desarrolladores.

[IoTWireless.3]AWSLas tareas de IoT FUOTA deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::IoTWireless::FuotaTask`

Regla de AWS Config: `iotwireless-fuota-task-tagged`

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredKeyTags`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si una tarea de actualización inalámbrica del firmware de AWS IoT Wireless (FUOTA) tiene etiquetas con las claves específicas definidas en el parámetro. `requiredKeyTags` El control falla si la tarea FUOTA no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredKeyTags`. Si no se proporciona el parámetro `requiredKeyTags`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si la tarea FUOTA no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS

los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte Definición de permisos basados en atributos con autorización ABAC en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte las mejores prácticas y estrategias en los AWSrecursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para añadir etiquetas a una tarea FUOTA de AWS IoT Wireless, consulta Cómo etiquetar tus AWS IoT Wireless recursos en la Guía para AWS IoT Wireless desarrolladores.

Controles CSPM de Security Hub para Amazon IVS

Estos AWS Security Hub CSPM controles evalúan el servicio y los recursos de Amazon Interactive Video Service (IVS).

Es posible que estos controles no estén disponibles en todosRegiones de AWS. Para obtener más información, consulte Disponibilidad de los controles por región.

[IVS.1] Los pares de teclas de reproducción IVS deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::IVS::PlaybackKeyPair`

Regla de AWS Config: `ivs-playback-key-pair-tagged`

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredKeyTags`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si un par de claves de reproducción de Amazon IVS tiene etiquetas con las claves específicas definidas en el parámetro `requiredKeyTags`. El control falla si el par de claves de reproducción no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredKeyTags`. Si no se proporciona el parámetro `requiredKeyTags`, el control solo comprueba la existencia de una clave de etiqueta y falla si el par de claves de reproducción no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte Definición de permisos basados en atributos con autorización ABAC en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte las mejores prácticas y estrategias en los AWSrecursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para añadir etiquetas a un par de claves de reproducción de IVS, consulte la referencia TagResourcede la API de Real-Time streaming de Amazon IVS.

[IVS.2] Las configuraciones de grabación de IVS deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::IVS::RecordingConfiguration`

Regla de AWS Config: `ivs-recording configuration-tagged`

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredKeyTags`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si una configuración de grabación de Amazon IVS tiene etiquetas con claves específicas definidas en el parámetro `requiredKeyTags`. El control falla si la configuración de grabación no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredKeyTags`. Si no se proporciona el parámetro `requiredKeyTags`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si la configuración de grabación no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte Definición de permisos basados en atributos con autorización ABAC en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte las mejores prácticas y estrategias en los AWSrecursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para añadir etiquetas a una configuración de grabación de IVS, consulte la referencia de TagResourcela API de Real-Time streaming de Amazon IVS.

[IVS.3] Los canales IVS deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::IVS::Channel`

Regla de AWS Config: `ivs-channel-tagged`

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredKeyTags`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si un canal de Amazon IVS tiene etiquetas con las claves específicas definidas en el parámetro `requiredKeyTags`. El control falla si el canal no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredKeyTags`. Si no se proporciona el parámetro `requiredKeyTags`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si el canal no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS

los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte Definición de permisos basados en atributos con autorización ABAC en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte las mejores prácticas y estrategias en los AWSrecursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para añadir etiquetas a un canal de IVS, consulte la referencia de TagResourcela API de Real-Time streaming de Amazon IVS.

Controles CSPM de Security Hub para Amazon Keyspaces

Estos AWS Security Hub CSPM controles evalúan el servicio y los recursos de Amazon Keyspaces.

Es posible que estos controles no estén disponibles en todosRegiones de AWS. Para obtener más información, consulte Disponibilidad de los controles por región.

[Keyspaces.1] Los espacios clave de Amazon Keyspaces deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::Cassandra::Keyspace`

Regla de AWS Config: `cassandra-keyspace-tagged`

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredKeyTags`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si un espacio de claves de Amazon Keyspaces tiene etiquetas con las claves específicas definidas en el parámetro `requiredKeyTags`. El control falla si el espacio de claves no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredKeyTags`. Si no se proporciona el parámetro `requiredKeyTags`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si el espacio de claves no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte Definición de permisos basados en atributos con autorización ABAC en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte las mejores prácticas y estrategias en los AWSrecursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para agregar etiquetas a un espacio de claves de Amazon Keyspaces, consulte Cómo agregar etiquetas a un espacio de claves en la Guía para desarrolladores de Amazon Keyspaces.

Controles CSPM de Security Hub para Kinesis

Estos AWS Security Hub CSPM controles evalúan el servicio y los recursos de Amazon Kinesis.

Es posible que estos controles no estén disponibles en todosRegiones de AWS. Para obtener más información, consulte Disponibilidad de los controles por región.

[Kinesis.1] Las transmisiones de Kinesis deben cifrarse en reposo

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6)

Categoría: Proteger > Protección de datos > Cifrado de datos en reposo

Gravedad: media

Tipo de recurso: `AWS::Kinesis::Stream`

Regla de AWS Config: kinesis-stream-encrypted

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si Kinesis Data Streams está cifrada en reposo con el cifrado del servidor. Este control falla si una transmisión de Kinesis no se cifra en reposo con el cifrado del servidor.

Server-side el cifrado es una función de Amazon Kinesis Data Streams que cifra automáticamente los datos antes de que estén en reposo mediante un. AWS KMS key Los datos se cifran antes de

escribirlos en la capa de almacenamiento del flujo de Kinesis y se descifran después de recuperarlos del almacenamiento. Como resultado, sus datos se cifran en reposo dentro del servicio de Amazon Kinesis Data Streams.

Corrección

Para obtener información sobre cómo habilitar el cifrado del servidor para las transmisiones de Kinesis, consulte ¿Cómo puedo empezar con el cifrado del servidor? en la Guía para desarrolladores de Amazon Kinesis.

[Kinesis.2] Las transmisiones de Kinesis deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::Kinesis::Stream`

AWS Configregla: `tagged-kinesis-stream` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si un flujo de datos de Amazon Kinesis tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza un error si el flujo de datos no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el

parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si el flujo de datos no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte Etiquetar sus AWS recursos en el. Referencia general de AWS

Corrección

Para agregar etiquetas a un flujo de datos de Kinesis, consulte Etiquetado de flujos de Amazon Kinesis Data Streams en la Guía para desarrolladores de Amazon Kinesis.

[Kinesis.3] Las transmisiones de Kinesis deben tener un período de retención de datos adecuado

Gravedad: media

Tipo de recurso: `AWS::Kinesis::Stream`

Regla de AWS Config: kinesis-stream-backup-retention-check

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`minimumBackupRetentionPeriod`	Cantidad mínima de horas que deben conservarse los datos.	Cadena	24 a 8760	168

Este control comprueba si un flujo de datos de Amazon Kinesis tiene un periodo de retención de datos más largo o igual de largo que el periodo especificado. El control lanza un error si el periodo de retención de datos es más corto que el periodo especificado. A menos que proporciones un valor de parámetro personalizado para el período de retención de datos, Security Hub CSPM utiliza un valor predeterminado de 168 horas.

En Kinesis Data Streams, un flujo de datos es una secuencia ordenada de registros de datos que se puede escribir y leer en tiempo real. Los registros de datos se almacenan temporalmente en particiones de su flujo. El periodo de tiempo desde que se agrega un registro hasta que ya no se puede obtener acceso a él se denomina periodo de retención. Kinesis Data Streams hace que los registros más antiguos que el nuevo periodo de retención sean inaccesibles casi inmediatamente después de reducir el periodo de retención. Por ejemplo, cambiar el periodo de retención de 24 horas a 48 horas implica que los registros añadidos a la secuencia 23 horas y 55 minutos antes seguirán estando disponibles después de que hayan transcurrido 24 horas.

Corrección

Para cambiar el periodo de retención de las copias de seguridad de sus flujos de Kinesis Data Streams, consulte Change the data retention period en la Guía para desarrolladores de Amazon Kinesis Data Streams.

Controles CSPM de Security Hub paraAWS KMS

Estos AWS Security Hub CSPM controles evalúan el AWS Key Management Service (AWS KMS) servicio y los recursos. Es posible que los controles no estén disponibles en todosRegiones de AWS. Para obtener más información, consulte Disponibilidad de los controles por región.

[KMS.1] Las políticas gestionadas por los clientes de IAM no deberían permitir acciones de descifrado en todas las claves de KMS

Requisitos relacionados: NIST.800-53.r5 AC-2 NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7),, NIST.800-53.r5 AC-5 NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6 (3)

Categoría: Proteger - Administración de acceso seguro

Gravedad: media

Tipo de recurso: `AWS::IAM::Policy`

Regla de AWS Config: iam-customer-policy-blocked-kms-actions

Tipo de horario: provocado por un cambio

Parámetros:

- `blockedActionsPatterns: kms:ReEncryptFrom, kms:Decrypt` (no personalizable)
- `excludePermissionBoundaryPolicy`: `True` (no personalizable)

Comprueba si la versión predeterminada de las políticas gestionadas por los clientes de IAM permite a los directores utilizar las acciones de AWS KMS descifrado en todos los recursos. El control falla si la política está lo suficientemente abierta como para permitir realizar acciones de `kms:Decrypt` o `kms:ReEncryptFrom` en todas las claves de KMS.

El control solo comprueba las claves de KMS en el elemento Recurso y no tiene en cuenta ningún condicional del elemento Condición de una política. Además, el control evalúa las políticas administradas por el cliente asociadas y no asociadas. No comprueba las políticas integradas ni las políticas gestionadas. AWS

Con AWS KMS ella, usted controla quién puede usar sus claves KMS y acceder a sus datos cifrados. Las políticas de IAM definen qué acciones puede realizar una identidad (usuario, grupo o rol) en qué recursos. Siguiendo las prácticas recomendadas de seguridad, se AWS recomienda conceder los privilegios mínimos. En otras palabras, debe conceder a las identidades únicamente los permisos `kms:Decrypt` o `kms:ReEncryptFrom` y únicamente para las claves que se requieren para realizar una tarea. De lo contrario, es posible que el usuario utilice claves que no sean adecuadas para sus datos.

En lugar de conceder permisos para todas las claves, determine el conjunto mínimo de claves que los usuarios necesitan para acceder a los datos cifrados. Luego, diseñe políticas que permitan a los usuarios usar solo esas claves. Por ejemplo, no permita permisos de `kms:Decrypt` en todas las claves KMS. En su lugar, permita únicamente `kms:Decrypt` las claves de su cuenta en una región determinada. Al adoptar el principio del privilegio mínimo, puede reducir el riesgo de que sus datos se divulguen de forma no intencionada.

Corrección

Para modificar una política de IAM administrada por el cliente, consulte Edición de políticas gestionadas por el cliente en la Guía del usuario de IAM. Al editar su política, proporcione para el campo `Resource` el nombre de recurso de Amazon (ARN) de la clave o claves específicas en las que desea permitir acciones de descifrado.

[KMS.2] Los directores de IAM no deberían tener políticas integradas de IAM que permitan realizar acciones de descifrado en todas las claves de KMS

Requisitos relacionados: NIST.800-53.r5 AC-2, NIST.800-53.r5 AC-2 (1), (15) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7),,, NIST.800-53.r5 AC-3 (3) NIST.800-53.r5 AC-5 NIST.800-53.r5 AC-6 NIST.800-53.r5 AC-6

Categoría: Proteger - Administración de acceso seguro

Gravedad: media

Tipo de recurso:

- `AWS::IAM::Group`
- `AWS::IAM::Role`
- `AWS::IAM::User`

Regla de AWS Config: iam-inline-policy-blocked-kms-actions

Tipo de horario: provocado por un cambio

Parámetros:

- `blockedActionsPatterns: kms:ReEncryptFrom, kms:Decrypt` (no personalizable)

Este control comprueba si las políticas integradas en sus identidades de IAM (rol, usuario o grupo) permiten las acciones de AWS KMS descifrado y recrifrado de todas las claves de KMS. El control falla si la política está lo suficientemente abierta como para permitir realizar acciones de `kms:Decrypt` o `kms:ReEncryptFrom` en todas las claves de KMS.

El control solo comprueba las claves de KMS en el elemento Recurso y no tiene en cuenta ningún condicional del elemento Condición de una política.

Con élAWS KMS, usted controla quién puede usar sus claves KMS y acceder a sus datos cifrados. Las políticas de IAM definen qué acciones puede realizar una identidad (usuario, grupo o rol) en qué recursos. Siguiendo las prácticas recomendadas de seguridad, se AWS recomienda conceder los privilegios mínimos. En otras palabras, debe conceder a las identidades únicamente los permisos que necesitan y únicamente para las claves que se requieren para realizar una tarea. De lo contrario, es posible que el usuario utilice claves que no sean adecuadas para sus datos.

En lugar de conceder permisos para todas las claves, determine el conjunto mínimo de claves que los usuarios necesitan para acceder a los datos cifrados. Luego, diseñe políticas que permitan a los usuarios usar solo esas claves. Por ejemplo, no permita permisos de `kms:Decrypt` en todas las claves KMS. En su lugar, conceda el permiso solo a claves específicas de una región específica de su cuenta. Al adoptar el principio del privilegio mínimo, puede reducir el riesgo de que sus datos se divulguen de forma no intencionada.

Corrección

Para modificar una política en línea de IAM, consulte Edición de políticas en línea en la Guía del usuario de IAM. Al editar su política, proporcione para el campo `Resource` el nombre de recurso de Amazon (ARN) de la clave o claves específicas en las que desea permitir acciones de descifrado.

[KMS.3]AWS KMS keysno se debe eliminar involuntariamente

Requisitos relacionados: NIST.800-53.r5 SC-12 NIST.800-53.r5 SC-12 (2)

Categoría: Proteger > Protección de datos > Protección contra la eliminación de datos

Gravedad: crítica

Tipo de recurso: `AWS::KMS::Key`

AWS Configregla: `kms-cmk-not-scheduled-for-deletion-2` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si la eliminación de las claves de KMS está programada. El control falla si está programada la eliminación de una clave KMS.

Las claves KMS no se pueden recuperar una vez eliminadas. Los datos cifrados con una clave KMS tampoco se pueden recuperar permanentemente si se elimina la clave KMS. Si los datos significativos se han cifrado con una clave de KMS cuya eliminación está programada, considere la posibilidad de descifrar los datos o volver a cifrarlos con una nueva clave de KMS, a menos que esté realizando un borrado criptográfico de forma intencionada.

Cuando se programa la eliminación de una clave de KMS, se aplica un período de espera obligatorio para dar tiempo a revertir la eliminación, en caso de que se haya programado por error. El período de espera predeterminado es de 30 días, pero se puede reducir a tan solo 7 días si está programada la eliminación de la clave KMS. Durante el período de espera, se puede cancelar la eliminación programada y no se eliminará la clave KMS.

Para obtener información adicional sobre la eliminación de claves de KMS, consulte Eliminar claves de KMS en la Guía para desarrolladores de AWS Key Management Service.

Corrección

Para cancelar una eliminación de claves de KMS programada, consulte Para cancelar la eliminación de claves en Programación y cancelación de la eliminación de claves (consola) de la Guía para desarrolladores de AWS Key Management Service.

[KMS.4]AWS KMSla rotación de claves debe estar habilitada

Requisitos relacionados: CIS AWS Foundations Benchmark v5.0. 0/3.6, Criterio de referencia sobre los AWS fundamentos de la CEI v3.0. 0/3.6, Punto de referencia sobre los AWS fundamentos de la CEI v1.4. 0/3.8, Criterio de referencia sobre los AWS fundamentos de la CEI v1.2. 0/2.8, NIST.800-53.r5 SC-12 (2) NIST.800-53.r5 SC-12, NIST.800-53.r5 SC-28 (3), PCI DSS v3.2. 1/3.6.4, PCI DSS v4.0. 1/34.7.4

Categoría: Proteger > Protección de datos > Cifrado de datos en reposo

Gravedad: media

Tipo de recurso: `AWS::KMS::Key`

Regla de AWS Config: cmk-backing-key-rotation-enabled

Tipo de programa: Periódico

Parámetros: ninguno

AWS KMSpermite a los clientes girar la clave de respaldo, que es el material clave almacenado AWS KMS y vinculado al identificador de clave de la clave KMS. Es la clave de backup que se utiliza para realizar operaciones criptográficas como, por ejemplo, cifrado y descifrado. Actualmente, la rotación de claves automática retiene todas las claves de backup anteriores, por lo que el descifrado de los datos cifrado se puede realizar de forma transparente.

CIS recomienda que habilite la rotación de claves de KMS. La rotación de claves de cifrado ayuda a reducir el impacto potencial de una clave en peligro porque los datos cifrados con una nueva clave no son accesibles con un clave anterior que se haya visto expuesta.

Corrección

Para habilitar la rotación de claves de KMS, consulte Cómo habilitar y deshabilitar la rotación automática de claves en la Guía para desarrolladores de AWS Key Management Service.

[KMS.5] Las claves KMS no deben ser de acceso público

Categoría: Proteger > Configuración de red segura > Recursos no accesibles públicamente

Gravedad: crítica

Tipo de recurso: `AWS::KMS::Key`

Regla de AWS Config: kms-key-policy-no-public-access

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una AWS KMS key es de acceso público. El control falla si se puede acceder de manera pública a la clave de KMS.

La implementación del acceso con privilegios mínimos es esencial a la hora de reducir los riesgos de seguridad y el impacto de los errores o intentos malintencionados. Si la política de claves de a AWS KMS key permite el acceso desde cuentas externas, es posible que terceros puedan cifrar y descifrar los datos con la clave. Esto podría provocar que una amenaza interna o externa extraiga datos del usuario Servicios de AWS que utilice la clave.

> **Note**
>
> Este control también devuelve un `FAILED` resultado AWS KMS key si sus configuraciones AWS Config impiden registrar la política clave en el elemento de configuración (CI) de la clave KMS. AWS ConfigPara completar la política clave en el CI para la clave de KMS, el AWS Configrol debe tener acceso para leer la política clave mediante la llamada a la GetKeyPolicyAPI. Para resolver este tipo de problema`FAILED`, compruebe las políticas que pueden impedir que el AWS Config rol tenga acceso de lectura a la política clave de la clave de KMS. Por ejemplo, revise lo siguiente:
>
> - La política de claves de la clave de KMS.
> - Las políticas de control de servicios (SCP) y las políticas de control de recursos (RCP) AWS Organizations que se aplican a tu cuenta.
> - Permisos para el AWS Config rol, si no usa el rol vinculado al AWS Configservicio.
>
> Además, este control no evalúa condiciones de políticas que utilicen caracteres comodín o variables. Para producir un resultado `PASSED`, las condiciones en la política de claves deben usar únicamente valores fijos, que son valores que no contienen caracteres comodín ni variables de políticas. Para obtener información sobre variables de políticas, consulte Variables y etiquetas en la Guía del usuario de AWS Identity and Access Management.

Corrección

Para obtener información sobre cómo actualizar la política clave de un usuarioAWS KMS key, consulte las políticas clave AWS KMS en la Guía para AWS Key Management Servicedesarrolladores.

Controles CSPM de Security Hub para AWS Lambda

Estos AWS Security Hub CSPM controles evalúan el AWS Lambda servicio y los recursos. Es posible que los controles no estén disponibles en todos los casos Regiones de AWS. Para obtener más información, consulte Disponibilidad de los controles por región.

[Lambda.1] Las políticas de las funciones de Lambda deberían prohibir el acceso público

Requisitos relacionados: NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21),, NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7 (11)

NIST.800-53.r5 SC-7, (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), PCI DSS v3.2. 1/1.2.1, PCI DSS v3.2. 1/11.3.1, PCI DSS v3.2. 1/13.3.2, PCI DSS v3.2. 1/13.3.4, PCI DSS v3.2. 1/71.2.1, PCI DSS versión 4.0. 1/72.2.1

Categoría: Proteger - Configuración de red segura

Gravedad: crítica

Tipo de recurso: `AWS::Lambda::Function`

Regla de AWS Config : lambda-function-public-access-prohibited

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si la política basada en recursos de la función de Lambda prohíbe el acceso público a la cuenta. El control falla si se permite el acceso público. El control también falla si se invoca una función de Lambda desde Amazon S3 y la política no incluye una condición para limitar el acceso público, como por ejemplo `AWS:SourceAccount`. Le recomendamos que utilice otras condiciones de S3 junto con `AWS:SourceAccount` en su política de bucket para obtener un acceso más preciso.

> **Note**
>
> Este control no evalúa condiciones de políticas que utilicen caracteres comodín o variables. Para producir un resultado `PASSED`, las condiciones en la política de la función de Lambda deben usar únicamente valores fijos, que son valores que no contienen caracteres comodín ni variables de políticas. Para obtener información sobre variables de políticas, consulte Variables y etiquetas en la Guía del usuario de AWS Identity and Access Management .

La función de Lambda no debe ser accesible públicamente, ya que puede permitir el acceso involuntario al código que tenga almacenado en la característica.

Corrección

Para solucionar este problema, debe actualizar la política basada en los recursos de su característica para eliminar los permisos o añadir la condición de `AWS:SourceAccount`. Solo puede actualizar la política basada en recursos desde la API de Lambda o. AWS CLI

Para empezar, revise la política basada en recursos de la consola Lambda. Identifique la declaración de política que tiene valores de campo `Principal` que hacen que la política sea pública, como `"*"` o `{ "AWS": "*" }`.

No puede editar la política desde la consola. Para eliminar los permisos de la característica, ejecute el comando remove-permission desde AWS CLI.

```
$ aws lambda remove-permission --function-name <function-name> --statement-
id <statement-id>
```

Sustituya *`<function-name>`* por el nombre de la función de Lambda y *`<statement-id>`* con el identificador de la sentencia (`Sid`) que desee eliminar.

[Lambda.2] Las funciones de Lambda deben usar los tiempos de ejecución compatibles

Requisitos relacionados: NIST.800-53.r5 CA-9 (1),, NIST.800-53.r5 CM-2 NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2 (2), (4), NIST.800-53.r5 SI-2 NIST.800-53.r5 SI-2 (5), PCI DSS v4.0. 1/12.3.4

Categoría: Proteger - Desarrollo seguro

Gravedad: media

Tipo de recurso: `AWS::Lambda::Function`

Regla de AWS Config : lambda-function-settings-check

Tipo de horario: provocado por un cambio

Parámetros:

- `runtime`: `dotnet10, dotnet8, java25, java21, java17, java11, java8.al2, java17.al2023, java11.al2023, java8.al2023, nodejs24.x, nodejs22.x, python3.14, python3.13, python3.12, python3.11, python3.10, ruby4.0, ruby3.4, ruby3.3` (no personalizable)

Este control comprueba si la configuración del tiempo de ejecución de las AWS Lambda funciones coincide con los valores esperados establecidos para los tiempos de ejecución compatibles en cada idioma. El control falla si la función de Lambda no utiliza un tiempo de ejecución compatible, tal como se indicó en la sección Parámetros. Security Hub CSPM ignora las funciones que tienen un tipo de paquete de. `Image`

Los Tiempos de ejecución de Lambda se crean a partir de una combinación de sistema operativo, lenguaje de programación y bibliotecas de software, todos ellos sujetos a operaciones de mantenimiento y actualizaciones de seguridad. Cuando un componente de un tiempo de ejecución deja de recibir actualizaciones de seguridad, Lambda descarta el tiempo de ejecución. Aunque no puede crear funciones que utilicen el tiempo de ejecución obsoleto, la función sigue estando disponible para procesar eventos de invocación. Recomendamos comprobar que sus funciones de Lambda sean actuales y que no utilicen entornos de tiempo de ejecución obsoletos. Para obtener una lista de los tiempos de ejecución compatibles, consulte los tiempos de ejecución de Lambda en la Guía para desarrolladores de AWS Lambda .

Corrección

Para obtener más información sobre los tiempos de ejecución compatibles y los programas de obsolescencia, consulte la Política de obsolescencia del tiempo de ejecución en la Guía para desarrolladores de AWS Lambda . Cuando migre los tiempos de ejecución a la versión más reciente, siga la sintaxis y las instrucciones de los editores del lenguaje. También recomendamos implementar actualizaciones del tiempo de ejecución para ayudar a reducir el riesgo de que las cargas de trabajo se vean afectadas en el caso de que se produzca una incompatibilidad entre las versiones en el tiempo de ejecución.

[Lambda.3] Las funciones de Lambda deben estar en una VPC

Requisitos relacionados: PCI DSS v3.2. 1/11.2.1, PCI DSS v3.2. 1/11.3.1, PCI DSS v3.2. 1/13.3.2, PCI DSS v3.2. 1/1.3.4 NIST.800-53.r5 AC-21 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), (21) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (11) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9) NIST.800-53.r5 SC-7

Categoría: Proteger - Configuración de red segura

Gravedad: baja

Tipo de recurso: `AWS::Lambda::Function`

AWS Config regla: lambda-inside-vpc

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si se implementó una función de Lambda en una nube privada virtual (VPC). El control falla si no se implementa la función de Lambda en una VPC. El CSPM de Security Hub

no evalúa la configuración de enrutamiento de subred de la VPC para determinar la accesibilidad pública. Es posible que vea resultados erróneos en los recursos de Lambda @Edge.

La implementación de recursos en una VPC refuerza la seguridad y el control de las configuraciones de red. Estas implementaciones también ofrecen escalabilidad y una alta tolerancia a los errores en varias zonas de disponibilidad. Puede personalizar las implementaciones de VPC para cumplir con los diversos requisitos de las aplicaciones.

Corrección

Para configurar una característica existente para conectarse a subredes privadas de su VPC, consulte Configuración del acceso a la VPC en la Guía para desarrolladores de AWS Lambda . Recomendamos elegir al menos dos subredes privadas para una alta disponibilidad y al menos un grupo de seguridad que cumpla con los requisitos de conectividad de la característica.

[Lambda.5] Las funciones de VPC Lambda deben funcionar en varias zonas de disponibilidad

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2) NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoría: Recuperación > Resiliencia > Alta disponibilidad

Gravedad: media

Tipo de recurso: `AWS::Lambda::Function`

Regla de AWS Config : lambda-vpc-multi-az-check

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub CSPM
`availabilityZones`	Cantidad mínima de zonas de disponibilidad	Enum	`2, 3, 4, 5, 6`	2

Este control comprueba si una AWS Lambda función que se conecta a una nube privada virtual (VPC) funciona al menos en el número especificado de zonas de disponibilidad (AZ). Se produce un error en el control si la función no funciona en al menos la cantidad especificada de AZ. A menos que proporcione un valor de parámetro personalizado para la cantidad mínima de zonas de disponibilidad, Security Hub CSPM utiliza un valor predeterminado de dos zonas de disponibilidad.

La implementación de recursos en varias zonas de disponibilidad es una práctica AWS recomendada para garantizar una alta disponibilidad en su arquitectura. La disponibilidad es un pilar fundamental del modelo de seguridad de la tríada de confidencialidad, integridad y disponibilidad. Todas las funciones de Lambda que se conectan a una VPC deben tener una implementación multi-AZ para garantizar que una sola zona de error no provoque una interrupción total de las operaciones.

Corrección

Si configura la característica para conectarse a una nube privada virtual (VPC) en su cuenta, especifique subredes en varias zonas de disponibilidad para garantizar una alta disponibilidad. Para obtener instrucciones, consulte Configuración del acceso a la VPC en la Guía para desarrolladores de AWS Lambda .

Alta disponibilidad: Lambda ejecuta la característica en varias zonas de disponibilidad para asegurarse de que está disponible para procesar eventos en caso de una interrupción del servicio en una sola zona.

[Lambda.6] Las funciones de Lambda deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::Lambda::Function`

AWS Config regla: `tagged-lambda-function` (regla CSPM personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub CSPM
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	`No default value`

Este control comprueba si una AWS Lambda función tiene etiquetas con las claves específicas definidas en el parámetro`requiredTagKeys`. El control falla si la función no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y falla si la función no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y se compone de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWSen la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Las etiquetas son accesibles para muchos Servicios de AWS, incluso AWS

Billing. Para conocer más prácticas recomendadas para el etiquetado, consulte Etiquetado de recursos de AWS en la Referencia general de AWS.

Corrección

Para agregar etiquetas a una función de Lambda, consulte Uso de etiquetas en funciones de Lambda en la Guía para desarrolladores de AWS Lambda .

[Lambda.7] Las funciones de Lambda deberían tener AWS X-Ray el rastreo activo está habilitado

Requisitos relacionados: NIST.800-53.r5 CA-7

Categoría: Identificar - Registro

Gravedad: baja

Tipo de recurso: `AWS::Lambda::Function`

Regla de AWS Config : lambda-function-xray-enabled

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si el rastreo activo con AWS X-Ray está activado para una AWS Lambda función. El control falla si el seguimiento activo con X-Ray está deshabilitado para la función Lambda.

AWS X-Ray puede proporcionar funciones de seguimiento y supervisión para las AWS Lambda funciones, lo que permite ahorrar tiempo y esfuerzo al depurar y operar las funciones de Lambda. Puede ayudar a diagnosticar errores e identificar cuellos de botella de rendimiento, ralentizaciones y tiempos de espera mediante un desglose detallado de la latencia de las funciones de Lambda. También puede contribuir al cumplimiento de los requisitos de privacidad y protección de los datos. Si habilita el rastreo activo para una función de Lambda, X-Ray proporciona una visión holística del flujo y el procesamiento de datos dentro de la función de Lambda, lo que puede ayudarlo a identificar posibles vulnerabilidades de seguridad o prácticas de manejo de datos que no cumplan con las normas. Esta visibilidad contribuye a mantener la integridad y la confidencialidad de los datos, así como el cumplimiento de las normas pertinentes.

> **Note**
>
> AWS X-Ray Actualmente, el rastreo no es compatible con las funciones de Lambda con Amazon Managed Streaming para Apache Kafka (Amazon MSK), Apache Kafka autogestionado, Amazon MQ con ActiveMQ y RabbitMQ ni con las asignaciones de fuentes de eventos de Amazon DocumentDB.

Corrección

Para obtener información sobre cómo habilitar el rastreo activo de una función, consulte Visualizar las invocaciones a funciones de Lambda en la Guía para desarrolladores. AWS Lambda AWS X-Ray AWS Lambda

Controles CSPM de Security Hub para Macie

Estos AWS Security Hub CSPM controles evalúan el servicio Amazon Macie.

Es posible que estos controles no estén disponibles en todosRegiones de AWS. Para obtener más información, consulte Disponibilidad de los controles por región.

[Macie.1] Amazon Macie debería estar activado

Requisitos relacionados: NIST.800-53.r5 CA-7, NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 RA-5, NIST.800-53.r5 SA-8 (19), NIST.800-53.r5 SI-4

Categoría: Detectar - Servicios de detección

Gravedad: media

Tipo de recurso: `AWS::::Account`

Regla de AWS Config: `macie-status-check`

Tipo de programa: Periódico

Este control comprueba si Amazon Macie está habilitado para una cuenta. Se produce un error en el control si Macie no está habilitado para la cuenta.

Amazon Macie detecta datos confidenciales mediante el machine learning y la coincidencia de patrones, proporciona visibilidad de los riesgos de seguridad de los datos y permite establecer una

protección automatizada contra esos riesgos. Macie evalúa de manera automática y continua los buckets de Amazon Simple Storage Service (Amazon S3) para garantizar la seguridad y el control de acceso, y genera resultados para notificarle posibles problemas con la seguridad o la privacidad de los datos de Amazon S3. Macie también detecta y notifica de manera automática los datos confidenciales, como información de identificación personal (PII), para proporcionarle una mejor comprensión de los datos que almacena en Amazon S3. Para más información, consulte la Guía del usuario de Amazon Macie.

Corrección

Para habilitar Macie, consulte Habilitación de Macie en la Guía del usuario de Amazon Macie.

[Macie.2] La detección automática de datos confidenciales por parte de Macie debería estar habilitada

Requisitos relacionados: NIST.800-53.r5 CA-7 NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 RA-5, NIST.800-53.r5 SA-8 (19), NIST.800-53.r5 SI-4

Categoría: Detectar - Servicios de detección

Gravedad: alta

Tipo de recurso: `AWS::::Account`

Regla de AWS Config: `macie-auto-sensitive-data-discovery-check`

Tipo de programa: Periódico

Este control comprueba si la detección automática de datos confidenciales está habilitada en una cuenta de administrador de Amazon Macie. Se produce un error en el control si la detección automática de datos confidenciales no está habilitada en una cuenta de administrador de Macie. Este control solo se aplica a las cuentas de administrador.

Macie detecta y notifica de manera automática los datos confidenciales, como información de identificación personal (PII), en buckets de Amazon Simple Storage Service (Amazon S3). Gracias a la detección automática de datos confidenciales, Macie evalúa continuamente su inventario de buckets y utiliza técnicas de muestreo para identificar y seleccionar los objetos de S3 representativos de sus buckets. A continuación, Macie analiza los objetos seleccionados en busca de datos confidenciales. A medida que el análisis avanza, Macie actualiza las estadísticas, los datos de inventario y demás información que proporciona sobre sus datos en S3. Macie también genera resultados para informar sobre los datos confidenciales que encuentra.

Corrección

Para crear y configurar trabajos automáticos de descubrimiento de datos confidenciales para analizar objetos en buckets de S3, consulte Configuring automated sensitive data discovery for your account en la Guía del usuario de Amazon Macie.

Controles de CSPM de Security Hub para Amazon MSK

Estos AWS Security Hub CSPM controles evalúan el servicio y los recursos de Amazon Managed Streaming for Apache Kafka (Amazon MSK). Es posible que los controles no estén disponibles en todos. Regiones de AWS Para obtener más información, consulte Disponibilidad de los controles por región.

[MSK.1] Los clústeres de MSK deben cifrarse en tránsito entre los nodos de intermediación

Requisitos relacionados: NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (3), NIST.800-53.r5 SC-7 (4), (1) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 NIST.800-53.r5 SC-8 (2), PCI DSS v4.0. 1/42.2.1

Categoría: Proteger > Protección de datos > Cifrado de datos en tránsito

Gravedad: media

Tipo de recurso: `AWS::MSK::Cluster`

Regla de AWS Config: msk-in-cluster-node-require-tls

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un clúster de Amazon MSK está cifrado en tránsito con HTTPS (TLS) entre los nodos intermediarios del clúster. El control falla si la comunicación de texto sin formato está habilitada para una conexión de nodo intermediario del clúster.

HTTPS ofrece un nivel de seguridad adicional, ya que utiliza TLS para mover datos y se puede utilizar para ayudar a evitar posibles ataques de “persona en medio” o similares para espiar o manipular el tráfico de red. De forma predeterminada, Amazon MSK cifra los datos en tránsito con TLS. Sin embardo, puede anular este valor predeterminado en el momento en que cree el clúster. Recomendamos utilizar conexiones cifradas a través de HTTPS (TLS) para las conexiones de nodos intermediarios.

Corrección

Para obtener información sobre cómo actualizar la configuración de cifrado de un clúster de Amazon MSK, consulte Actualización de la configuración de seguridad de un clúster en la Guía para desarrolladores de Amazon Managed Streaming para Apache Kafka.

[MSK.2] Los clústeres de MSK deberían tener configurada una supervisión mejorada

Requisitos relacionados: NIST.800-53.r5 CA-7 NIST.800-53.r5 SI-2

Categoría: Detectar - Servicios de detección

Gravedad: baja

Tipo de recurso: `AWS::MSK::Cluster`

Regla de AWS Config: msk-enhanced-monitoring-enabled

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un clúster de Amazon MSK tiene configurada la supervisión mejorada, especificada mediante un nivel de supervisión de al menos `PER_TOPIC_PER_BROKER`. Se produce un error en el control si el nivel de supervisión del clúster está establecido en `DEFAULT` o `PER_BROKER`.

El nivel de supervisión `PER_TOPIC_PER_BROKER` proporciona información más detallada sobre el rendimiento del clúster de MSK y también proporciona métricas relacionadas con el uso de los recursos, como el uso de la CPU y la memoria. Esto ayuda a identificar los cuellos de botella en el rendimiento y los patrones de uso de los recursos para temas y agentes individuales. Esta visibilidad, a su vez, puede optimizar el rendimiento de sus agentes de Kafka.

Corrección

Para configurar la supervisión mejorada para un clúster de MSK, haga lo siguiente:

1. Abra la consola Amazon MSK en? https://console.aws.amazon.com/msk/home region=us-east-1#/home/.
2. En el panel de navegación, seleccione Clusters (Clústeres). A continuación, elija una etiqueta de clúster.
3. En Acción, seleccione Editar supervisión.

4. Seleccione la opción Supervisión mejorada a nivel de tema.
5. Seleccione Save changes (Guardar cambios).

Para obtener más información sobre los niveles de monitoreo, consulte las métricas de Amazon MSK para monitorear a los corredores estándar CloudWatch en la Guía para desarrolladores de Amazon Managed Streaming for Apache Kafka.

[MSK.3] Los conectores MSK Connect deben estar cifrados en tránsito

Requisitos relacionados: PCI DSS v4.0. 1/42.2.1

Categoría: Proteger > Protección de datos > Cifrado de datos en tránsito

Gravedad: media

Tipo de recurso: `AWS::KafkaConnect::Connector`

AWS Configregla: `msk-connect-connector-encrypted` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un conector Amazon MSK Connect está cifrado en tránsito. Este control falla si el conector no está cifrado en tránsito.

Los datos en tránsito hacen referencia a los datos que se mueven de una ubicación a otra, por ejemplo, entre los nodos del clúster o entre el clúster y la aplicación. Los datos pueden moverse a través de Internet o dentro de una red privada. El cifrado de los datos en tránsito reduce el riesgo de que un usuario no autorizado pueda espiar el tráfico de la red.

Corrección

Puede habilitar el cifrado en tránsito cuando crea un conector MSK Connect. No puede cambiar la configuración de cifrado después de crear un conector. Para obtener más información, consulte Crear un conector en la Guía para desarrolladores de Amazon Managed Streaming para Apache Kafka.

[MSK.4] Los clústeres de MSK deben tener el acceso público deshabilitado

Categoría: Proteger > Gestión del acceso seguro > Recurso no accesible públicamente

Gravedad: crítica

Tipo de recurso: `AWS::MSK::Cluster`

Regla de AWS Config: msk-cluster-public-access-disabled

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control verifica que el acceso público esté desactivado para un clúster de Amazon MSK. El control falla si el acceso público está habilitado para el clúster de MSK.

De forma predeterminada, los clientes solo pueden acceder a un clúster de Amazon MSK cuando se encuentran en la misma VPC que el clúster. Toda la comunicación entre clientes de Kafka y un clúster de MSK es privada de forma predeterminada, y los datos de streaming no atraviesan Internet. Sin embargo, si un clúster de MSK está configurado para permitir acceso público, cualquier persona en Internet puede establecer una conexión con los agentes de Apache Kafka que se ejecutan dentro del clúster. Esto puede provocar problemas como acceso no autorizado, filtraciones de datos o explotación de vulnerabilidades. Si restringe el acceso a un clúster mediante medidas de autenticación y autorización, puede ayudar a proteger información confidencial y mantener la integridad de los recursos.

Corrección

Para obtener información sobre cómo administrar el acceso público a un clúster de Amazon MSK, consulte Activación del acceso público para un clúster aprovisionado de MSK en la Guía del desarrollador de Amazon Managed Streaming para Apache Kafka.

[MSK.5] Los conectores MSK deben tener el registro activado

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: `AWS::KafkaConnect::Connector`

Regla de AWS Config: msk-connect-connector-logging-enabled

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control verifica si el registro está habilitado para un conector de Amazon MSK. El control falla si el registro está desactivado para el conector de MSK.

Los conectores de Amazon MSK integran sistemas externos y servicios de Amazon con Apache Kafka mediante la copia continua de datos en streaming desde un origen de datos a un clúster de Apache Kafka, o mediante la copia continua de datos desde un clúster hacia un receptor de datos. MSK Connect puede generar eventos de registro que ayudan a depurar un conector. Al crear un conector, puede especificar cero o más de los siguientes destinos de registro: Amazon CloudWatch Logs, Amazon S3 y Amazon Data Firehose.

> **Note**
>
> Los valores de configuración confidenciales pueden aparecer en los registros de los conectores si un complemento no los define como secretos. Kafka Connect trata los valores de configuración indefinidos de la misma manera que cualquier otro valor de texto sin formato.

Corrección

Para habilitar el registro en un conector de Amazon MSK existente, debe volver a crear el conector con la configuración de registro correspondiente. Para obtener información sobre las opciones de configuración, consulte Registro para MSK Connect en la Guía del desarrollador de Amazon Managed Streaming para Apache Kafka.

[MSK.6] Los clústeres de MSK deberían deshabilitar el acceso no autenticado

Categoría: Proteger > Gestión del acceso seguro > Autenticación sin contraseña

Gravedad: media

Tipo de recurso: `AWS::MSK::Cluster`

Regla de AWS Config: msk-unrestricted-access-check

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si el acceso sin autenticación está desactivado para un clúster de Amazon MSK. El control falla si el acceso sin autenticación está habilitado para el clúster de MSK.

Amazon MSK admite mecanismos de autenticación y autorización para controlar el acceso a un clúster. Estos mecanismos verifican la identidad de los clientes que se conectan al clúster y determinan qué acciones pueden realizar. Un clúster de MSK se puede configurar para permitir acceso sin autenticación, lo que posibilita que cualquier cliente con conectividad de red publique y se suscriba a temas de Kafka sin proporcionar credenciales. Ejecutar un clúster de MSK sin exigir autenticación infringe el principio de privilegio mínimo y puede exponer el clúster a accesos no autorizados. Esto permite que cualquier cliente acceda, modifique o elimine datos en los temas de Kafka, lo que puede provocar filtraciones de datos, modificaciones no autorizadas o interrupciones del servicio. Recomendamos habilitar los mecanismos de autenticación, como la autenticación de IAM o el TLS mutuo SASL/SCRAM, para garantizar un control de acceso adecuado y mantener el cumplimiento de las normas de seguridad.

Corrección

Para obtener información sobre cómo cambiar la configuración de autenticación de un clúster de Amazon MSK, consulte las siguientes secciones de la Guía para desarrolladores de Amazon Managed Streaming para Apache Kafka: Actualización de la configuración de seguridad de un clúster de Amazon MSK y Autenticación y autorización para las API de Apache Kafka.

Controles CSPM de Security Hub para Amazon MQ

Estos AWS Security Hub CSPM controles evalúan el servicio y los recursos de Amazon MQ. Es posible que los controles no estén disponibles en todosRegiones de AWS. Para obtener más información, consulte Disponibilidad de los controles por región.

[MQ.2] Los corredores de ActiveMQ deben transmitir los registros de auditoría a CloudWatch

Requisitos relacionados: NIST.800-53.r5 AU-2,, NIST.800-53.r5 AU-3 NIST.800-53.r5 AU-12 NIST.800-53.r5 SI-4, PCI DSS v4.0. 1/10.3.3

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: `AWS::AmazonMQ::Broker`

Regla de AWS Config: `mq-cloudwatch-audit-log-enabled`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un bróker ActiveMQ de Amazon MQ transmite los registros de auditoría a Amazon Logs. CloudWatch El control falla si el agente no transmite los registros de auditoría a Logs. CloudWatch

Al publicar los registros de ActiveMQ Broker en Logs CloudWatch , puede CloudWatch crear alarmas y métricas que aumenten la visibilidad de la información relacionada con la seguridad.

Corrección

Para transmitir los registros de los corredores de ActiveMQ CloudWatch a los registros, consulte Configuración de Amazon MQ para los registros de ActiveMQ en la Guía para desarrolladores de Amazon MQ.

[MQ.4] Los corredores de Amazon MQ deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::AmazonMQ::Broker`

AWS Configregla: `tagged-amazonmq-broker` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	`No default value`

Este control comprueba si un agente de Amazon MQ tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control falla si el agente no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y falla si el agente no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte Etiquetar sus AWS recursos en el. Referencia general de AWS

Corrección

Para agregar etiquetas a un agente de Amazon MQ, consulte Etiquetado de recursos en la Guía para desarrolladores de Amazon MQ.

[MQ.5] Los corredores de ActiveMQ deberían usar el modo de implementación active/standby

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2) NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoría: Recuperación > Resiliencia > Alta disponibilidad

Gravedad: baja

Tipo de recurso: `AWS::AmazonMQ::Broker`

Regla de AWS Config: `mq-active-deployment-mode`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si el modo de implementación de un broker ActiveMQ de Amazon MQ está configurado en. active/standby El control falla si se establece un corredor de instancia única (habilitado de forma predeterminada) como modo de implementación.

Active/standby la implementación proporciona una alta disponibilidad para sus corredores ActiveMQ de Amazon MQ en un. Región de AWS El modo active/standby de implementación incluye dos instancias de broker en dos zonas de disponibilidad diferentes, configuradas en un par redundante. Estos agentes se comunican de forma sincrónica con la aplicación, lo que puede reducir el tiempo de inactividad y la pérdida de datos en caso de que se produzca un error.

Corrección

Para crear un agente ActiveMQ nuevo active/standby con modo de despliegue, consulte Creación y configuración de un agente ActiveMQ en la Guía para desarrolladores de Amazon MQ. Para el modo de implementación, elija un agente. Active/standby No se puede cambiar el modo de implementación de un broker ya existente. En su lugar, debe crear un nuevo corredor y copiar la configuración del corredor anterior.

[MQ.6] Los corredores de RabbitMQ deberían usar el modo de despliegue de clústeres

Requisitos relacionados: NIST.800-53.r5 CP-6 (2) NIST.800-53.r5 CP-10, (2) NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (5) NIST.800-53.r5 SI-13

Categoría: Recuperación > Resiliencia > Alta disponibilidad

Gravedad: baja

Tipo de recurso: `AWS::AmazonMQ::Broker`

Regla de AWS Config: `mq-rabbit-deployment-mode`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si el modo de implementación de un bróker RabbitMQ de Amazon MQ está configurado para la implementación en clúster. El control falla si se establece un corredor de instancia única (habilitado de forma predeterminada) como modo de implementación.

La implementación de clústeres proporciona una alta disponibilidad para sus corredores de Amazon MQ RabbitMQ en una Región de AWS. La implementación del clúster es una agrupación lógica de tres nodos de agente de RabbitMQ, cada uno con su propio volumen de Amazon Elastic Block Store (Amazon EBS) y un estado compartido. La implementación del clúster garantiza que los datos se repliquen en todos los nodos del clúster, lo que puede reducir el tiempo de inactividad y la pérdida de datos en caso de error.

Corrección

Para crear un nuevo bróker de RabbitMQ con el modo de implementación de clústeres, consulte Creación y conexión a un bróker de RabbitMQ en la Guía para desarrolladores de Amazon MQ. Para el Modo de implementación, elija Implementación en clúster. No se puede cambiar el modo de implementación de un broker ya existente. En su lugar, debe crear un nuevo corredor y copiar la configuración del corredor anterior.

Controles CSPM de Security Hub para Neptune

Estos AWS Security Hub CSPM controles evalúan el servicio y los recursos de Amazon Neptune.

Es posible que estos controles no estén disponibles en todosRegiones de AWS. Para obtener más información, consulte Disponibilidad de los controles por región.

[Neptune.1] Los clústeres de bases de datos de Neptune deben cifrarse en reposo

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6)

Categoría: Proteger > Protección de datos > Cifrado de datos en reposo

Gravedad: media

Tipo de recurso: `AWS::RDS::DBCluster`

Regla de AWS Config: `neptune-cluster-encrypted`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un clúster de base de datos de Neptune está cifrado en reposo. El control falla si un clúster de base de datos de Neptune no está cifrado en reposo.

Los datos en reposo se refieren a cualquier dato que se almacene en un almacenamiento persistente y no volátil durante cualquier período de tiempo. El cifrado le ayuda a proteger la confidencialidad de dichos datos, reduciendo el riesgo de que un usuario no autorizado pueda acceder a ellos. El cifrado de sus clústeres de bases de datos de Neptune protege sus datos y metadatos contra el acceso no autorizado. También cumple con los requisitos de conformidad para el cifrado de datos en reposo de los sistemas de archivos de producción.

Corrección

Puede habilitar el cifrado en reposo al crear un clúster de base de datos de Neptune. No se puede cambiar la configuración de cifrado después de crear un clúster. Para obtener más información, consulte Cifrar los recursos inactivos de Neptuno en la Guía del usuario de Neptuno.

[Neptune.2] Los clústeres de bases de datos de Neptune deberían publicar registros de auditoría en Logs CloudWatch

Requisitos relacionados: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (1), NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 AU-6 (5), NIST.800-53.r5 AU-7 (1), NIST.800-53.r5 AU-9 (7) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9) NIST.800-53.r5 SI-20, NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (5), NIST.800-53.r5 SI-7(8), PCI DSS v4.0. 1/10.3.3

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: `AWS::RDS::DBCluster`

Regla de AWS Config: `neptune-cluster-cloudwatch-log-export-enabled`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un clúster de base de datos de Neptune publica registros de auditoría en Amazon CloudWatch Logs. El control falla si un clúster de base de datos de Neptune no publica los registros de auditoría en Logs. CloudWatch `EnableCloudWatchLogsExport`debe estar configurado en. `Audit`

Amazon Neptune y Amazon CloudWatch están integrados para que pueda recopilar y analizar métricas de rendimiento. Neptune envía automáticamente las métricas a las alarmas CloudWatch y también las admite CloudWatch . Los registros de auditoría son altamente personalizables. Al auditar una base de datos, cada operación realizada con los datos se puede supervisar y registrar en un registro de auditoría que incluye información sobre el clúster de base de datos al que se accede y cómo se accede. Le recomendamos que envíe estos registros para ayudarle CloudWatch a supervisar sus clústeres de base de datos de Neptune.

Corrección

Para publicar registros de auditoría de Neptune en Logs, consulte Publicar CloudWatch registros de Neptuno CloudWatch en Amazon Logs en la Guía del usuario de Neptune. En la sección Exportaciones de registros, elija Auditar.

[Neptune.3] Las instantáneas del clúster de base de datos de Neptune no deben ser públicas

Requisitos relacionados: NIST.800-53.r5 AC-21 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), (21) NIST.800-53.r5 AC-4,, NIST.800-53.r5 AC-4 (11) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), PCI DSS v4.0. 1/14.4.4

Categoría: Proteger > Configuración de red segura > Recursos no accesibles públicamente

Gravedad: crítica

Tipo de recurso: `AWS::RDS::DBClusterSnapshot`

Regla de AWS Config: `neptune-cluster-snapshot-public-prohibited`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una instantánea de un clúster de base de datos manual de Neptune es pública. El control falla si una instantánea manual del clúster de base de datos de Neptune es pública.

Una instantánea manual de un clúster de base de datos de Neptune no debe ser pública a menos que se pretenda. Si comparte una instantánea manual sin cifrar públicamente, la instantánea estará

disponible para todo Cuentas de AWS. Las instantáneas públicas pueden provocar una exposición no intencionada de los datos.

Corrección

Para eliminar el acceso público a las instantáneas de clústeres de bases de datos manuales de Neptuno, consulte Compartir una instantánea de clúster de base de datos en la Guía del usuario de Neptune.

[Neptune.4] Los clústeres de base de datos de Neptune deben tener habilitada la protección contra eliminación

Requisitos relacionados: NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2) NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2)

Categoría: Proteger > Protección de datos > Protección contra la eliminación de datos

Gravedad: baja

Tipo de recurso: `AWS::RDS::DBCluster`

Regla de AWS Config: `neptune-cluster-deletion-protection-enabled`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un clúster de base de datos de Neptune tiene habilitada la protección contra eliminación. El control falla si un clúster de base de datos de Neptune no tiene habilitada la protección contra eliminación.

La activación de la protección contra la eliminación de clústeres ofrece un nivel adicional de protección contra la eliminación accidental de la base de datos o la eliminación por parte de un usuario no autorizado. Un clúster de Neptune DB no se puede eliminar mientras está habilitada la protección contra eliminación. Primero debe deshabilitar la protección contra la eliminación para que la solicitud de eliminación se pueda realizar correctamente.

Corrección

Para habilitar la protección contra la eliminación de un clúster de base de datos de Neptune existente, consulte Modificación del clúster de base de datos mediante la consola, la CLI y la API en la Guía del usuario de Amazon Aurora.

[Neptune.5] Los clústeres de Neptune DB deberían tener habilitadas las copias de seguridad automatizadas

Requisitos relacionados: NIST.800-53.r5 SI-12

Categoría: Recuperación > Resiliencia > Respaldos habilitados

Gravedad: media

Tipo de recurso: `AWS::RDS::DBCluster`

Regla de AWS Config: `neptune-cluster-backup-retention-check`

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`minimumBackupRetentionPeriod`	El periodo mínimo de retención de copias de seguridad en días	Entero	De 7 a 35	7

Este control comprueba si un clúster de base de datos de Neptune tiene las copias de seguridad automáticas habilitadas y un periodo de retención de las copias de seguridad superior o igual al periodo especificado. Se produce un error en el control si las copias de seguridad no están habilitadas para el clúster de base de datos de Neptune o si el periodo de retención es inferior al periodo especificado. A menos que proporcione un valor de parámetro personalizado para el período de retención de la copia de seguridad, Security Hub CSPM utiliza un valor predeterminado de 7 días.

Las copias de seguridad le ayudan a recuperarse más rápidamente de un incidente de seguridad y a reforzar la resiliencia de sus sistemas. Al automatizar las copias de seguridad de sus clústeres

de bases de datos de Neptune, podrá restaurar sus sistemas a un punto en el tiempo y minimizar el tiempo de inactividad y la pérdida de datos.

Corrección

Para habilitar las copias de seguridad automatizadas y establecer un periodo de retención de copias de seguridad para los clústeres de bases de datos de Neptune, consulte Habilitación de las copias de seguridad automatizadas en la Guía del usuario de Amazon RDS. Para el período de retención de la copia de seguridad, elija un valor mayor o igual a 7.

[Neptune.6] Las instantáneas del clúster de base de datos de Neptune deben cifrarse en reposo

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SC-7 (18)

Categoría: Proteger > Protección de datos > Cifrado de datos en reposo

Gravedad: media

Tipo de recurso: `AWS::RDS::DBClusterSnapshot`

Regla de AWS Config: `neptune-cluster-snapshot-encrypted`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una instantánea de un clúster de base de datos de Neptune está cifrada en reposo. El control falla si un clúster de base de datos de Neptune no está cifrado en reposo.

Los datos en reposo se refieren a cualquier dato que se almacene en un almacenamiento persistente y no volátil durante cualquier período de tiempo. El cifrado le ayuda a proteger la confidencialidad de dichos datos, reduciendo el riesgo de que un usuario no autorizado acceda a ellos. Los datos de las instantáneas de los clústeres de base de datos de Neptune deben cifrarse en reposo para ofrecer un nivel de seguridad adicional.

Corrección

No puede cifrar una instantánea de un clúster de base de datos de Neptune existente. En su lugar, debe restaurar la instantánea en un nuevo clúster de base de datos y habilitar el cifrado en el clúster.

Puede crear una instantánea cifrada desde el clúster cifrado. Para obtener instrucciones, consulte Restauración desde una instantánea de clúster de base de datos y Creación de una instantánea de clúster de base de datos en Neptuno en la Guía del usuario de Neptuno.

[Neptune.7] Los clústeres de base de datos de Neptune deben tener habilitada la autenticación de bases de datos de IAM

Requisitos relacionados: NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-6

Categoría: Proteger > Gestión del acceso seguro > Autenticación sin contraseña

Gravedad: media

Tipo de recurso: `AWS::RDS::DBCluster`

Regla de AWS Config: `neptune-cluster-iam-database-authentication`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un clúster de base de datos de Neptune tiene habilitada la autenticación de bases de datos de IAM. El control falla si la autenticación de la base de datos de IAM no está habilitada para un clúster de base de datos de Neptune.

La autenticación de base de datos de IAM para los clústeres de base de datos de Amazon Neptune elimina la necesidad de almacenar credenciales de usuario en la configuración de base de datos, ya que la autenticación se administra externamente mediante IAM. Cuando la autenticación de bases de datos de IAM está habilitada, cada solicitud debe firmarse con la versión 4 de AWS Signature.

Corrección

De forma predeterminada, la autenticación de bases de datos de IAM está deshabilitada al crear un clúster de Neptune DB. Para habilitarlo, consulte Habilitar la autenticación de bases de datos de IAM en Neptuno en la Guía del usuario de Neptuno.

[Neptune.8] Los clústeres de bases de datos de Neptune deben configurarse para copiar etiquetas a las instantáneas

Requisitos relacionados: NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::RDS::DBCluster`

Regla de AWS Config: `neptune-cluster-copy-tags-to-snapshot-enabled`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un clúster de base de datos de Neptune está configurado para copiar todas las etiquetas en las instantáneas cuando se crean las instantáneas. El control falla si un clúster de base de datos de Neptune no está configurado para copiar etiquetas a las instantáneas.

La identificación y el inventario de sus activos de TI es un aspecto fundamental de seguridad y control. Debe etiquetar instantáneas del mismo modo que los clústeres de base de datos de Amazon RDS principales. La copia de las etiquetas garantiza que los metadatos para las instantáneas de base de datos coincidan con los clústeres de base de datos principales y que cualquier política de acceso para la instantánea de base de datos también coincida con la de la instancia de base de datos principal.

Corrección

Para copiar etiquetas en instantáneas de clústeres de bases de datos de Neptuno, consulte Copiar etiquetas en Neptuno en la Guía del usuario de Neptuno.

[Neptune.9] Los clústeres de base de datos Neptune deben implementarse en varias zonas de disponibilidad

Requisitos relacionados: NIST.800-53.r5 CP-10 NIST.800-53.r5 CP-6 (2) NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoría: Recuperación > Resiliencia > Alta disponibilidad

Gravedad: media

Tipo de recurso: `AWS::RDS::DBCluster`

Regla de AWS Config: `neptune-cluster-multi-az-enabled`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un clúster de base de datos de Amazon Neptune tiene instancias de réplica de lectura en varias zonas de disponibilidad (AZ). Se produce un error en el control si el clúster se implementa en una sola AZ.

Si una AZ no está disponible y durante los eventos de mantenimiento habituales, las réplicas de lectura sirven como destinos de conmutación por error para la instancia principal. Es decir, si la instancia principal falla, Neptune promueve una instancia de réplica de lectura para convertirla en la instancia primaria. Por el contrario, si su clúster de base de datos no incluye ninguna instancia de lectura y réplica, su clúster de base de datos no estará disponible cuando se produzca un error en la instancia principal hasta que se vuelva a crear. Re-creating la instancia principal lleva mucho más tiempo que la promoción de una réplica de lectura. Para garantizar una alta disponibilidad, recomendamos crear una o varias instancias de réplica de lectura que tengan la misma clase de instancia de base de datos que la instancia principal y que estén ubicadas en AZ distintas de las de la instancia principal.

Corrección

Para implementar un clúster de base de datos Neptune en varias zonas de disponibilidad, consulte las instancias de Read-replica base de datos en un clúster de base de datos Neptune en la Guía del usuario de Neptune.

Controles CSPM de Security Hub paraAWS Network Firewall

Estos AWS Security Hub CSPM controles evalúan el AWS Network Firewall servicio y los recursos. Es posible que los controles no estén disponibles en todosRegiones de AWS. Para obtener más información, consulte Disponibilidad de los controles por región.

[NetworkFirewall.1] Los firewalls de Network Firewall deben implementarse en varias zonas de disponibilidad

Requisitos relacionados: NIST.800-53.r5 CP-10 NIST.800-53.r5 CP-6 (2) NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoría: Recuperación > Resiliencia > Alta disponibilidad

Gravedad: media

Tipo de recurso: `AWS::NetworkFirewall::Firewall`

Regla de AWS Config: netfw-multi-az-enabled

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control evalúa si un firewall gestionado a través de él AWS Network Firewall está desplegado en varias zonas de disponibilidad (AZ). Se produce un error en el control si un firewall se implementa en una sola AZ.

AWSla infraestructura global incluye múltiplesRegiones de AWS. Las AZ son ubicaciones físicamente independientes y aisladas de cada región que se encuentran conectadas mediante redes con un alto nivel de rendimiento y redundancia, además de baja latencia. Al implementar un firewall de Network Firewall en varias AZ, puede equilibrar y desviar el tráfico entre las AZ, lo que ayuda a diseñar soluciones de alta disponibilidad.

Corrección

Implementación de un firewall de Network Firewall en varias zonas de disponibilidad

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, en Firewall de red, elija Firewalls.
3. En la página Firewalls, seleccione el nombre del firewall que quiere editar.
4. En la página de detalles del firewall, elija la pestaña Detalles del firewall.
5. En la sección Política asociada y VPC, elija Editar
6. Para agregar una nueva AZ, elija Agregar nueva subred. Seleccione la AZ y la subred que quiere utilizar. Seleccione al menos dos AZ.
7. Seleccione Save.

[NetworkFirewall.2] El registro de Network Firewall debe estar habilitado

Requisitos relacionados: NIST.800-53.r5 AC-2 (12), NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2 NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 AU-9 (7), (9) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (8), NIST.800-53.r5 SI-3 (20) NIST.800-53.r5 SI-4, NIST.800-53.r5 SI-4 NIST.800-53.r5 SI-7 (8), NIST.800-171.r2 3.1.20, 3.13.1 NIST.800-171.r2

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: `AWS::NetworkFirewall::LoggingConfiguration`

Regla de AWS Config: netfw-logging-enabled

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si el registro está activado en un firewall. AWS Network Firewall Se produce un error en el control si el registro no está habilitado para al menos un tipo de registro o si el destino del registro no existe.

El registro ayuda a mantener la fiabilidad, la disponibilidad y el rendimiento de los firewalls. En Network Firewall, el registro proporciona información detallada sobre el tráfico de red, incluida la hora en la que el motor con estado recibió un flujo de paquetes, información detallada acerca del flujo de paquetes y las medidas de regla de estado adoptadas respecto del flujo de paquetes.

Corrección

Para habilitar el registro en un firewall, consulte Updating a firewall's logging configuration en la Guía para desarrolladores de AWS Network Firewall.

[NetworkFirewall.3] Las políticas de Network Firewall deben tener asociado al menos un grupo de reglas

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-171.r2 3.1.3 NIST.800-53.r5 CM-2, NIST.800-171.r2 3.13.1

Categoría: Proteger > Configuración de red segura

Gravedad: media

Tipo de recurso: `AWS::NetworkFirewall::FirewallPolicy`

Regla de AWS Config: netfw-policy-rule-group-associated

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una política de Network Firewall tiene asociados grupos de reglas con estado o sin estado. El control falla si no se asignan grupos de reglas sin estado o con estado.

Una política de firewall define la forma en que su firewall supervisa y gestiona el tráfico en Amazon Virtual Private Cloud (Amazon VPC). La configuración de grupos de reglas con estado y sin estado ayuda a filtrar los paquetes y los flujos de tráfico, y define el manejo del tráfico predeterminado.

Corrección

Para añadir un grupo de reglas a una política de Network Firewall, consulte Actualización de una política de firewall en la Guía para desarrolladores de AWS Network Firewall. Para obtener información sobre cómo crear y administrar grupos de reglas, consulte Grupos de reglas enAWS Network Firewall.

[NetworkFirewall.4] La acción sin estado predeterminada para las políticas de Network Firewall debe ser eliminar o reenviar paquetes completos

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Categoría: Proteger > Configuración de red segura

Gravedad: media

Tipo de recurso: `AWS::NetworkFirewall::FirewallPolicy`

Regla de AWS Config: netfw-policy-default-action-full-packets

Tipo de horario: provocado por un cambio

Parámetros:

- `statelessDefaultActions: aws:drop,aws:forward_to_sfe` (no personalizable)

Este control comprueba si la acción sin estado predeterminada para los paquetes completos de una política de Network Firewall es eliminar o reenviar. El control se activa si se selecciona `Drop` o `Forward`, y da error si se selecciona `Pass`.

Una política de firewall define la forma en que su firewall supervisa y gestiona el tráfico en Amazon VPC. Puede configurar grupos de reglas sin estado y con estado para filtrar los paquetes y los flujos de tráfico. Si se establece de forma predeterminada a `Pass` se puede permitir el tráfico no deseado.

Corrección

Para cambiar la política de firewall, consulte Actualización de una política de firewall en la Guía para desarrolladores de AWS Network Firewall. Para las Acciones predeterminadas Sin estado, seleccione Editar. A continuación, seleccione Soltar o Reenviar a grupos de reglas con estado como Acción.

[NetworkFirewall.5] La acción sin estado predeterminada para las políticas de Network Firewall debe ser eliminar o reenviar paquetes fragmentados

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-171.r2 3.1.3, NIST.800-53.r5 CM-2 3.1.14, 3.13.1, NIST.800-171.r2 3.13.6 NIST.800-171.r2 NIST.800-171.r2

Categoría: Proteger > Configuración de red segura

Gravedad: media

Tipo de recurso: `AWS::NetworkFirewall::FirewallPolicy`

Regla de AWS Config: netfw-policy-default-action-fragment-packets

Tipo de horario: provocado por un cambio

Parámetros:

- `statelessFragDefaultActions (Required) : aws:drop, aws:forward_to_sfe` (no personalizable)

Este control comprueba si la acción sin estado predeterminada para los paquetes fragmentados de una política de Network Firewall es eliminar o reenviar. El control se activa si se selecciona `Drop` o `Forward`, y da error si se selecciona `Pass`.

Una política de firewall define la forma en que su firewall supervisa y gestiona el tráfico en Amazon VPC. Puede configurar grupos de reglas sin estado y con estado para filtrar los paquetes y los flujos de tráfico. Si se establece de forma predeterminada a `Pass` se puede permitir el tráfico no deseado.

Corrección

Para cambiar la política de firewall, consulte Actualización de una política de firewall en la Guía para desarrolladores de AWS Network Firewall. Para las Acciones predeterminadas Sin estado,

seleccione Editar. A continuación, seleccione Soltar o Reenviar a grupos de reglas con estado como Acción.

[NetworkFirewall.6] El grupo de reglas de Stateless Network Firewall no debe estar vacío

Requisitos relacionados: NIST.800-53.r5 AC-4 (21), (11) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (5), NIST.800-171.r2 3.1.3, NIST.800-171.r2 3.1.14, 3.13.1, 3.13.6 NIST.800-171.r2 NIST.800-171.r2

Categoría: Proteger > Configuración de red segura

Gravedad: media

Tipo de recurso: `AWS::NetworkFirewall::RuleGroup`

Regla de AWS Config: netfw-stateless-rule-group-not-empty

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un grupo de reglas sin estado contiene reglas. AWS Network Firewall El control falla si no hay reglas en el grupo de reglas.

Un grupo de reglas contiene reglas que definen cómo el firewall procesa el tráfico en la VPC. Un grupo de reglas sin estado vacío, cuando está presente en una política de cortafuegos, puede dar la impresión de que el grupo de reglas procesará tráfico. Sin embargo, cuando el grupo de reglas sin estado está vacío, no procesa el tráfico.

Corrección

Para agregar reglas a su grupo de reglas de Network Firewall, consulte Actualización de un grupo de reglas con estado en la Guía para desarrolladores de AWS Network Firewall. En la página de detalles del firewall, en el Grupo de reglas sin estado, seleccione Editar para añadir reglas.

[NetworkFirewall.7] Los firewalls de Network Firewall deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::NetworkFirewall::Firewall`

AWS Configregla: `tagged-networkfirewall-firewall` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	`No default value`

Este control comprueba si un AWS Network Firewall firewall tiene etiquetas con las claves específicas definidas en el parámetro`requiredTagKeys`. El control falla si el firewall no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si el firewall no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan

operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte Etiquetar sus AWS recursos en el. Referencia general de AWS

Corrección

Para añadir etiquetas a un firewall de Network Firewall, consulte Etiquetado de AWS Network Firewall recursos en la Guía para AWS Network Firewall desarrolladores.

[NetworkFirewall.8] Las políticas de firewall de Network Firewall deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::NetworkFirewall::FirewallPolicy`

AWS Configregla: `tagged-networkfirewall-firewallpolicy` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que	`No default value`

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
	recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.		cumplan los requisitos de AWS.	

Este control comprueba si una política de AWS Network Firewall firewall tiene etiquetas con las claves específicas definidas en el parámetro`requiredTagKeys`. El control falla si la política de firewall no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si la política de firewall no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte Etiquetar sus AWS recursos en el. Referencia general de AWS

Corrección

Para añadir etiquetas a una política de Network Firewall, consulte Etiquetado de AWS Network Firewall recursos en la Guía para AWS Network Firewall desarrolladores.

[NetworkFirewall.9] Los firewalls de Network Firewall deben tener habilitada la protección de eliminación

Requisitos relacionados: NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2) NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2)

Categoría: Proteger > Seguridad de red

Gravedad: media

Tipo de recurso: `AWS::NetworkFirewall::Firewall`

Regla de AWS Config: netfw-deletion-protection-enabled

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un AWS Network Firewall firewall tiene habilitada la protección contra la eliminación. El control falla si la protección contra la eliminación no está habilitada en un firewall.

AWS Network Firewalles un servicio de detección de intrusiones y firewall de red gestionado y con estado que le permite inspeccionar y filtrar el tráfico hacia, desde o entre sus nubes privadas virtuales (VPC). La configuración de protección contra la eliminación protege contra la eliminación accidental del firewall.

Corrección

Para habilitar la protección contra eliminación en un firewall de Network Firewall existente, consulte Actualización de un firewall en la Guía para desarrolladores de AWS Network Firewall. Para Cambiar las protecciones, seleccione Habilitar. También puede activar la protección contra la eliminación invocando la UpdateFirewallDeleteProtectionAPI y configurando el campo en. `DeleteProtection` `true`

[NetworkFirewall.10] Los firewalls de Network Firewall deben tener habilitada la protección contra cambios de subred

Requisitos relacionados: NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2) NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2)

Categoría: Proteger > Seguridad de red

Gravedad: media

Tipo de recurso: `AWS::NetworkFirewall::Firewall`

Regla de AWS Config: netfw-subnet-change-protection-enabled

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control verifica si la protección contra cambios de subred está habilitada para un firewall de AWS Network Firewall. El control falla si la protección contra cambios de subred no está habilitada para el firewall.

AWS Network Firewalles un servicio de detección de intrusiones y firewall de red gestionado y con estado que puede utilizar para inspeccionar y filtrar el tráfico hacia, desde o entre sus nubes privadas virtuales (VPC). Si habilita la protección contra cambios de subred para un firewall de Network Firewall, puede proteger el firewall contra cambios accidentales en las asociaciones de subred.

Corrección

Para obtener información sobre cómo habilitar la protección contra cambios de subred en un firewall existente de Network Firewall, consulte Actualización de un firewall en la Guía del desarrollador de AWS Network Firewall.

Controles CSPM de Security Hub para Amazon Service OpenSearch

Estos AWS Security Hub CSPM controles evalúan el OpenSearch servicio y los recursos de Amazon OpenSearch Service (Servicio). Es posible que los controles no estén disponibles en todosRegiones de AWS. Para obtener más información, consulte Disponibilidad de los controles por región.

[Opensearch.1] OpenSearch los dominios deben tener activado el cifrado en reposo

Requisitos relacionados: PCI DSS v3.2. 1/12.2.1, PCI DSS v3.2. 1/1.3.1, PCI DSS v3.2. 1/1.3.4, PCI DSS v3.2. 1/7.2.1, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6),, (1) NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (6) NIST.800-53.r5 SI-7

Categoría: Proteger > Protección de datos > Cifrado de datos en reposo

Gravedad: media

Tipo de recurso: `AWS::OpenSearch::Domain`

Regla de AWS Config: `opensearch-encrypted-at-rest`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si los OpenSearch dominios tienen habilitada la configuración de cifrado en reposo. La comprobación falla si el cifrado en reposo no está habilitado.

Para aumentar la seguridad de los datos confidenciales, debe configurar su dominio de OpenSearch servicio para que esté cifrado en reposo. Al configurar el cifrado de datos en reposo, AWS KMS almacena y administra las claves de cifrado. Para realizar el cifrado, AWS KMS utiliza el algoritmo del estándar de cifrado avanzado con claves de 256 bits ()AES-256.

Para obtener más información sobre el cifrado de OpenSearch servicios en reposo, consulte Cifrado de datos en reposo para Amazon OpenSearch Service en la Guía para desarrolladores de Amazon OpenSearch Service.

Corrección

Para habilitar el cifrado en reposo para OpenSearch dominios nuevos y existentes, consulta Cómo habilitar el cifrado de datos en reposo en la Guía para desarrolladores de Amazon OpenSearch Service.

[Opensearch.2] OpenSearch los dominios no deben ser de acceso público

Requisitos relacionados: PCI DSS v3.2. 1/12.2.1, PCI DSS v3.2. 1/1.3.1, PCI DSS v3.2. 1/1.3.2, PCI DSS v3.2. 1/1.3.4, PCI DSS v3.2. 1/1.3.6, NIST.800-53.r5 AC-21 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 AC-4,, (11) NIST.800-53.r5 AC-6

NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9) NIST.800-53.r5 SC-7

Categoría: Proteger > Configuración de red segura > Recursos dentro de VPC

Gravedad: crítica

Tipo de recurso: `AWS::OpenSearch::Domain`

Regla de AWS Config: `opensearch-in-vpc-only`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si OpenSearch los dominios están en una VPC. No evalúa la configuración de direccionamiento de subred de VPC para determinar el acceso público.

Debe asegurarse de que OpenSearch los dominios no estén conectados a subredes públicas. Consulta Resource-based las políticas en la Guía para desarrolladores OpenSearch de Amazon Service. También debe asegurarse de que la VPC esté configurada de acuerdo con las prácticas recomendadas. Consulte Prácticas recomendadas de seguridad para su VPC en la Guía del usuario de Amazon VPC.

OpenSearch los dominios implementados en una VPC pueden comunicarse con los recursos de la VPC a través de la AWS red privada, sin necesidad de atravesar la Internet pública. Esta configuración aumenta la posición de seguridad al limitar el acceso a los datos en tránsito. Las VPC proporcionan una serie de controles de red para proteger el acceso a los OpenSearch dominios, incluidas las ACL de red y los grupos de seguridad. Security Hub recomienda migrar OpenSearch los dominios públicos a las VPC para aprovechar estos controles.

Corrección

Si crea un dominio con un punto de enlace público, no podrá colocarlo posteriormente en una VPC. En lugar de ello, se debe crear un dominio nuevo y migrar los datos. y viceversa. Si crea un dominio dentro de una VPC, no puede tener un punto de enlace público. En su lugar, debe crear otro dominio o deshabilitar este control.

Para obtener instrucciones, consulta Cómo lanzar tus dominios de Amazon OpenSearch Service dentro de una VPC en la Guía para desarrolladores de Amazon OpenSearch Service.

[Opensearch.3] OpenSearch los dominios deben cifrar los datos enviados entre nodos

Requisitos relacionados: NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (3), NIST.800-53.r5 SC-7 (4) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (2)

Categoría: Proteger > Protección de datos > Cifrado de datos en tránsito

Gravedad: media

Tipo de recurso: `AWS::OpenSearch::Domain`

Regla de AWS Config: `opensearch-node-to-node-encryption-check`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si los OpenSearch dominios tienen activado el cifrado de nodo a nodo. Este control falla si el cifrado de nodo a nodo está deshabilitado en el dominio.

HTTPS (TLS) puede utilizarse para ayudar a evitar posibles ataques de espionaje o de manipulación del tráfico de red con ataques de «persona en medio» o similares. Solo se deben permitir las conexiones cifradas a través de HTTPS (TLS). Al habilitar el cifrado de nodo a nodo para los OpenSearch dominios, se garantiza que las comunicaciones dentro del clúster estén cifradas en tránsito.

Puede haber una penalización en el rendimiento asociada a esta configuración. Debe conocer y probar la compensación de rendimiento antes de activar esta opción.

Corrección

Para habilitar el cifrado de nodo a nodo en un OpenSearch dominio, consulta Cómo habilitar el cifrado de nodo a nodo en la Guía para desarrolladores de Amazon Service. OpenSearch

[Opensearch.4] El registro de errores de OpenSearch dominio en Logs debe estar habilitado CloudWatch

Requisitos relacionados: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8)

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: `AWS::OpenSearch::Domain`

Regla de AWS Config: `opensearch-logs-to-cloudwatch`

Tipo de horario: provocado por un cambio

Parámetros:

- `logtype = 'error'` (no personalizable)

Este control comprueba si OpenSearch los dominios están configurados para enviar registros de errores a CloudWatch Logs. Este control falla si el registro de errores no CloudWatch está habilitado para un dominio.

Debe habilitar los registros de errores para OpenSearch los dominios y enviarlos a CloudWatch Logs para su conservación y respuesta. Los registros de errores de los dominios pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

Corrección

Para habilitar la publicación de registros, consulta Habilitar la publicación de registros (consola) en la Guía para desarrolladores de Amazon OpenSearch Service.

[Opensearch.5] OpenSearch los dominios deben tener activado el registro de auditoría

Requisitos relacionados: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2 NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), (9) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (8), NIST.800-53.r5 SI-3 (20), NIST.800-53.r5 SI-4 NIST.800-53.r5 SI-7 (8), PCI DSS v4.0. 1/102.2.1

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: `AWS::OpenSearch::Domain`

Regla de AWS Config: `opensearch-audit-logging-enabled`

Tipo de horario: provocado por un cambio

Parámetros:

- `cloudWatchLogsLogGroupArnList`(no personalizable): Security Hub CSPM no completa este parámetro. Comma-separated lista de grupos de CloudWatch registros que deben configurarse para los registros de auditoría.

Este control comprueba si OpenSearch los dominios tienen habilitado el registro de auditoría. Este control produce un error si un OpenSearch dominio no tiene activado el registro de auditoría.

Los registros de auditoría son altamente personalizables. Le permiten realizar un seguimiento de la actividad de los usuarios en sus OpenSearch clústeres, incluidos los aciertos y los errores de autenticación, las solicitudesOpenSearch, los cambios de indexación y las consultas de búsqueda entrantes.

Corrección

Para obtener instrucciones sobre cómo habilitar los registros de auditoría, consulta Habilitar los registros de auditoría en la Guía para desarrolladores de Amazon OpenSearch Service.

[Opensearch.6] OpenSearch los dominios deben tener al menos tres nodos de datos

Requisitos relacionados: NIST.800-53.r5 CP-10 NIST.800-53.r5 CP-6 (2) NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoría: Recuperación > Resiliencia > Alta disponibilidad

Gravedad: media

Tipo de recurso: `AWS::OpenSearch::Domain`

Regla de AWS Config: `opensearch-data-node-fault-tolerance`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si OpenSearch los dominios están configurados con al menos tres nodos de datos y lo `zoneAwarenessEnabled` está`true`. Este control falla para un OpenSearch dominio si `instanceCount` es menor que 3 o `zoneAwarenessEnabled` es`false`.

Para lograr una alta disponibilidad y tolerancia a errores a nivel de clúster, un OpenSearch dominio debe tener al menos tres nodos de datos. La implementación de un OpenSearch dominio con al menos tres nodos de datos garantiza las operaciones del clúster en caso de que un nodo falle.

Corrección

Para modificar la cantidad de nodos de datos de un OpenSearch dominio

1. Inicia sesión en la AWS consola y abre la consola OpenSearch de Amazon Service en https://console.aws.amazon.com/aos/.
2. En Mis dominios, elija el nombre del dominio que desee editar y elija Editar.
3. En Nodos de datos, establezca Número de nodos en un número superior a `3`. Si va a realizar la implementación en tres zonas de disponibilidad, establezca el número en un múltiplo de tres para garantizar una distribución equitativa entre las zonas de disponibilidad.
4. Seleccione Enviar.

[Opensearch.7] OpenSearch los dominios deben tener habilitado un control de acceso detallado

Requisitos relacionados: NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-5 NIST.800-53.r5 AC-6

Categoría: Proteger > Gestión del acceso seguro > Acciones confidenciales de la API restringidas

Gravedad: alta

Tipo de recurso: `AWS::OpenSearch::Domain`

Regla de AWS Config: `opensearch-access-control-enabled`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si OpenSearch los dominios tienen habilitado el control de acceso detallado. El control falla si el control de acceso detallado no está habilitado. Fine-grained el control de acceso requiere que `advanced-security-options` el OpenSearch parámetro esté habilitadoupdate-`domain-config`.

Fine-grained el control de acceso ofrece formas adicionales de controlar el acceso a tus datos en Amazon OpenSearch Service.

Corrección

Para habilitar un control de acceso detallado, consulta el control de Fine-grained acceso en Amazon OpenSearch Service en la Guía para desarrolladores de Amazon OpenSearch Service.

[Opensearch.8] Las conexiones a los OpenSearch dominios deben cifrarse con la última política de seguridad de TLS

Requisitos relacionados: NIST.800-53.r5 AC-17 (2) NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), NIST.800-53.r5 SC-12 (3), NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (3), NIST.800-53.r5 SC-7 (4) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SI-7 (6)

Categoría: Proteger > Protección de datos > Cifrado de datos en tránsito

Gravedad: media

Tipo de recurso: `AWS::OpenSearch::Domain`

Regla de AWS Config: `opensearch-https-required`

Tipo de horario: provocado por un cambio

Parámetros:

- `tlsPolicies: Policy-Min-TLS-1-2-PFS-2023-10` (no personalizable)

Este control comprueba si un punto de enlace de dominio de Amazon OpenSearch Service está configurado para usar la política de seguridad TLS más reciente. El control falla si el punto de enlace del OpenSearch dominio no está configurado para usar la última política compatible o si HTTPs no está habilitado.

Puede utilizar HTTPS (TLS) para ayudarle a evitar posibles ataques de tipo “intermediario”, de espionaje o de manipulación del tráfico de red. Solo se deben permitir las conexiones cifradas a través de HTTPS (TLS). El cifrado de los datos en tránsito puede afectar al rendimiento. Debe probar su aplicación con esta característica para comprender el perfil de rendimiento y el impacto del TLS. TLS 1.2 proporciona varias mejoras de seguridad con respecto a las versiones anteriores de TLS.

Corrección

Para habilitar el cifrado TLS, usa la operación de UpdateDomainConfigAPI. Configure el DomainEndpointOptionscampo para especificar el valor de`TLSSecurityPolicy`. Para obtener

más información, consulta el Node-to-node cifrado en la Guía para desarrolladores OpenSearch de Amazon Service.

[Opensearch.9] OpenSearch los dominios deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::OpenSearch::Domain`

AWS Configregla: `tagged-opensearch-domain` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	`No default value`

Este control comprueba si un dominio de Amazon OpenSearch Service tiene etiquetas con las claves específicas definidas en el parámetro`requiredTagKeys`. El control falla si el dominio no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si el dominio no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno

u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte Etiquetar sus AWS recursos en el. Referencia general de AWS

Corrección

Para añadir etiquetas a un dominio OpenSearch de servicio, consulta Cómo trabajar con etiquetas en la Guía para desarrolladores de Amazon OpenSearch Service.

[Opensearch.10] OpenSearch los dominios deben tener instalada la última actualización de software

Requisitos relacionados: NIST.800-53.r5 SI-2 NIST.800-53.r5 SI-2 (2), NIST.800-53.r5 SI-2 (4), NIST.800-53.r5 SI-2 (5), PCI DSS v4.0. 1/63.3.3

Categoría: Identificar > Administración de vulnerabilidades, parches y versiones

Gravedad: media

Tipo de recurso: `AWS::OpenSearch::Domain`

Regla de AWS Config: `opensearch-update-check`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un dominio de Amazon OpenSearch Service tiene instalada la última actualización de software. Se produce un error en el control si hay una actualización de software disponible, pero no está instalada para el dominio.

OpenSearch Las actualizaciones de software de servicio proporcionan las últimas correcciones, actualizaciones y funciones de plataforma disponibles para el entorno. Mantenerse al día con la instalación de los parches ayuda a mantener la seguridad y la disponibilidad del dominio. Si no se adoptan medidas respecto de las actualizaciones necesarias, actualizaremos el software de servicio automáticamente después de un tiempo determinado (por lo general, dos semanas). Recomendamos programar las actualizaciones en momentos de poco tráfico en el dominio para minimizar las interrupciones del servicio.

Corrección

Para instalar actualizaciones de software para un OpenSearch dominio, consulta Cómo iniciar una actualización en la Guía para desarrolladores de Amazon OpenSearch Service.

[Opensearch.11] OpenSearch los dominios deben tener al menos tres nodos principales dedicados

Requisitos relacionados: NIST.800-53.r5 CP-10 NIST.800-53.r5 CP-2, NIST.800-53.r5 SC-5, NIST.800-53.r5 SC-36, NIST.800-53.r5 SI-13

Categoría: Recuperación > Resiliencia > Alta disponibilidad

Gravedad: baja

Tipo de recurso: `AWS::OpenSearch::Domain`

Regla de AWS Config: `opensearch-primary-node-fault-tolerance`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un dominio de Amazon OpenSearch Service está configurado con al menos tres nodos principales dedicados. El control falla si el dominio tiene menos de tres nodos principales dedicados.

OpenSearch El servicio utiliza nodos principales dedicados para aumentar la estabilidad del clúster. Un nodo principal dedicado realiza tareas de administración de clústeres, pero no contiene datos ni

responde a las solicitudes de carga de datos. Le recomendamos que utilice Multi-AZ con modo de espera, lo que añade tres nodos principales dedicados a cada OpenSearch dominio de producción.

Corrección

Para cambiar el número de nodos principales de un OpenSearch dominio, consulte Creación y gestión de dominios de Amazon OpenSearch Service en la Guía para desarrolladores de Amazon OpenSearch Service.

Controles CSPM de Security Hub paraAWS Privada CA

Estos AWS Security Hub CSPM controles evalúan el AWS Autoridad de certificación privada (AWS Privada CA) servicio y los recursos.

Es posible que estos controles no estén disponibles en todosRegiones de AWS. Para obtener más información, consulte Disponibilidad de los controles por región.

[PCA.1]AWS Privada CALa autoridad emisora de certificados raíz debe estar deshabilitada

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Categoría: Proteger - Configuración de red segura

Gravedad: baja

Tipo de recurso: `AWS::ACMPCA::CertificateAuthority`

Regla de AWS Config: `acm-pca-root-ca-disabled`

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si AWS Privada CA tiene una autoridad de certificación (CA) raíz deshabilitada. Se produce un error en el control si la autoridad emisora de certificados raíz está habilitada.

Con AWS Privada CA él, puede crear una jerarquía de CA que incluya una CA raíz y una CA subordinada. Debe minimizar el uso de la autoridad emisora de certificados raíz para las tareas diarias, especialmente en los entornos de producción. La autoridad emisora de certificados raíz solo debe utilizarse para emitir certificados para las autoridades intermedias emisoras de certificados. Esto permite que la entidad de certificación raíz se almacene fuera de peligro mientras que las entidades de certificación intermedias realizan la tarea diaria de emitir certificados de entidad final.

Corrección

Para deshabilitar la autoridad emisora de certificados raíz, consulte Actualización del estado de CA en la Guía del usuario de AWS Autoridad de certificación privada.

[PCA.2]AWSLas autoridades de certificación de CA privadas deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::ACMPCA::CertificateAuthority`

Regla de AWS Config: `acmpca-certificate-authority-tagged`

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredKeyTags`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si una entidad emisora de certificados AWS privada tiene etiquetas con las claves específicas definidas en el parámetro`requiredKeyTags`. El control falla si la autoridad del certificado no tiene ninguna clave de etiqueta o si no cuenta con todas las claves especificadas en el parámetro `requiredKeyTags`. Si no se proporciona el parámetro `requiredKeyTags`, el control solo verifica la existencia de una clave de etiqueta y falla si la autoridad del certificado no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte Definición de permisos basados en atributos con autorización ABAC en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte las mejores prácticas y estrategias en los AWSrecursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para añadir etiquetas a una autoridad de CA AWS privada, consulte Añadir etiquetas para una entidad de certificación privada en la Guía del AWS Autoridad de certificación privadausuario.

Controles de CSPM de Security Hub para Amazon RDS

Estos AWS Security Hub CSPM controles evalúan los recursos de Amazon Relational Database Service (Amazon RDS) y Amazon RDS. Es posible que los controles no estén disponibles en todos los casos. Regiones de AWS Para obtener más información, consulte Disponibilidad de los controles por región.

[RDS.1] La instantánea de RDS debe ser privada

Requisitos relacionados: PCI DSS v3.2. 1/11.2.1, PCI DSS v3.2. 1/11.3.1, PCI DSS v3.2. 1/13.3.4, PCI DSS v3.2. 1/13.3.6, PCI DSS v3.2. 1/7.2.1, NIST.800-53.r5 AC-21 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 AC-4, (11) NIST.800-53.r5 AC-6

NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9) NIST.800-53.r5 SC-7

Categoría: Proteger - Configuración de red segura

Gravedad: crítica

Tipo de recurso: `AWS::RDS::DBClusterSnapshot`, `AWS::RDS::DBSnapshot`

Regla de AWS Config : `rds-snapshots-public-prohibited`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si las instantáneas de Amazon RDS son públicas. El control falla si las instantáneas de RDS son públicas. Este control evalúa instancias de RDS, instancias de base de datos de Aurora, instancias de base de datos de Neptune y clústeres de Amazon DocumentDB.

Las instantáneas de RDS se utilizan para realizar copias de seguridad de los datos de las instancias de RDS en un momento determinado. Se pueden utilizar para restaurar estados anteriores de instancias de RDS.

Una instantánea de RDS no debe ser pública a menos que se quiera. Si comparte una instantánea manual sin cifrar públicamente, estará disponible para todas las cuentas de Cuentas de AWS. Esto puede provocar una exposición no intencionada de los datos de su instancia de RDS.

Tenga en cuenta que si se cambia la configuración para permitir el acceso público, es posible que la AWS Config regla no pueda detectar el cambio hasta dentro de 12 horas. Hasta que la AWS Config regla detecte el cambio, la comprobación se realizará aunque la configuración infrinja la regla.

Para obtener más información sobre cómo compartir una instantánea de base de datos, consulte Cómo compartir una instantánea de base de datos en la Guía del usuario de Amazon RDS.

Corrección

Para eliminar el acceso público de las instantáneas de RDS, consulte Compartir una instantánea en la Guía del usuario de Amazon RDS. En Visibilidad de las instantáneas de base de datos, elija Privada.

[RDS.2] Las instancias de base de datos de RDS deben prohibir el acceso público, según lo determine la configuración PubliclyAccessible

Requisitos relacionados: CIS AWS Foundations Benchmark v5.0. 0/2.2.3, CIS AWS Foundations Benchmark v3.0. 0/2.3.3 NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), (11) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (5), PCI DSS v3.2. 1/11.2.1, PCI DSS versión 3.2. 1/11.3.1, PCI DSS v3.2. 1/13.3.2, PCI DSS v3.2. 1/13.3.4, PCI DSS v3.2. 1/13.3.6, PCI DSS v3.2. 1/71.2.1, PCI DSS versión 4.0. 1/14.4.4

Categoría: Proteger - Configuración de red segura

Gravedad: crítica

Tipo de recurso: `AWS::RDS::DBInstance`

Regla de AWS Config : `rds-instance-public-access-check`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si las instancias de Amazon RDS son accesibles públicamente mediante la evaluación del campo `PubliclyAccessible` en el elemento de configuración de instancia.

El valor `PubliclyAccessible` de la configuración de la instancia de RDS indica si la instancia de base de datos es accesible públicamente. Cuando la instancia de base de datos se configura con`PubliclyAccessible`, es una Internet-facing instancia con un nombre DNS que se puede resolver públicamente, que se resuelve en una dirección IP pública. Cuando la instancia de base de datos no es accesible públicamente, se trata de una instancia interna con un nombre DNS que se resuelve en una dirección IP privada.

A menos que tenga la intención de dar acceso público a su instancia de RDS, la instancia de RDS no debe configurarse con el valor `PubliclyAccessible`. Si lo hace, podría generar tráfico innecesario a su instancia de base de datos.

Corrección

Para eliminar el acceso público a las instancias de base de datos de RDS, consulte Modificación de una instancia de base de datos de Amazon RDS en la Guía del usuario de Amazon RDS. En Acceso público, elija No.

[RDS.3] Las instancias de base de datos de RDS deben tener habilitado el cifrado en reposo

Requisitos relacionados: CIS AWS Foundations Benchmark v5.0. 0/21.2.1, CIS AWS Foundations Benchmark v3.0. 0/2.3.1, CIS AWS Foundations Benchmark v1.4. 0/2.3.1, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28 (1) NIST.800-53.r5 SC-28, (10), NIST.800-53.r5 SC-7 (6) NIST.800-53.r5 SI-7

Categoría: Proteger > Protección de datos > Cifrado de datos en reposo

Gravedad: media

Tipo de recurso: `AWS::RDS::DBInstance`

Regla de AWS Config : `rds-storage-encrypted`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si el cifrado de almacenamiento está habilitado para las instancias de base de datos de Amazon RDS.

Este control está diseñado para instancias de base de datos de RDS. Sin embargo, también puede generar resultados para instancias de base de datos de Aurora, instancias de base de datos de Neptune y clústeres de Amazon DocumentDB. Si estos resultados no son útiles, puede suprimirlos.

Para obtener una capa adicional de seguridad para la información confidencial en las instancias de base de datos de RDS, debe configurar las instancias de base de datos de RDS de tal manera que se cifren en reposo. Para cifrar las instancias de base de datos de RDS y las instantáneas en reposo, debe habilitar la opción de cifrado para las instancias de base de datos de RDS. Los datos cifrados en reposo incluyen el almacenamiento subyacente de una instancia de base de datos, sus copias de seguridad automatizadas, sus réplicas de lectura y sus instantáneas.

Las instancias de base de datos cifradas de RDS utilizan el algoritmo de AES-256 cifrado de estándar abierto para cifrar los datos en el servidor que aloja las instancias de base de datos de RDS. Una vez cifrados los datos, Amazon RDS se encarga de la autenticación de acceso y del descifrado de los datos de forma transparente, con un impacto mínimo en el desempeño. No es necesario modificar las aplicaciones cliente de base de datos para utilizar el cifrado.

El cifrado de Amazon RDS actualmente está disponible para todos los motores de bases de datos y tipos de almacenamiento. El cifrado de Amazon RDS está disponible para la mayoría de las clases

de instancias de bases de datos. Para obtener información acerca de las clases de instancia de base de datos que no admiten el cifrado de Amazon RDS, consulte Cifrado de recursos de Amazon RDS en la Guía del usuario de Amazon RDS.

Corrección

Para obtener información sobre el cifrado de instancias de base de datos en Amazon RDS, consulte Cifrar los recursos de Amazon RDS en la Guía del usuario de Amazon RDS.

[RDS.4] Las instantáneas de clústeres de RDS y las instantáneas de bases de datos deben cifrarse en reposo

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28 (1) NIST.800-53.r5 SC-28, (10), NIST.800-53.r5 SC-7 (6) NIST.800-53.r5 SI-7

Categoría: Proteger > Protección de datos > Cifrado de datos en reposo

Gravedad: media

Tipo de recurso: `AWS::RDS::DBClusterSnapshot`, `AWS::RDS::DBSnapshot`

Regla de AWS Config : `rds-snapshot-encrypted`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una instantánea de base de datos de RDS está cifrada. El control falla si una instantánea de base de datos de RDS no está cifrada.

Este control está diseñado para instancias de base de datos de RDS. Sin embargo, también puede generar resultados para instantáneas de instancias de base de datos de Aurora, instancias de base de datos de Neptune y clústeres de Amazon DocumentDB. Si estos resultados no son útiles, puede suprimirlos.

El cifrado de los datos en reposo reduce el riesgo de que un usuario no autenticado acceda a los datos almacenados en el disco. Los datos de las instantáneas de RDS deben cifrarse en reposo para ofrecer un nivel de seguridad adicional.

Corrección

Para cifrar una instantánea de RDS, consulte Cifrar los recursos de Amazon RDS en la Guía del usuario de Amazon RDS. Cuando cifra una instancia de base de datos de RDS, los datos cifrados

incluyen el almacenamiento subyacente de la instancia, sus copias de seguridad automatizadas, sus réplicas de lectura y sus instantáneas.

Solo se puede cifrar una instancia de base de datos de RDS al crearla, no después de que se haya creado. Sin embargo, debido a que se puede cifrar una copia de una instantánea de base de datos sin cifrar, en la práctica es posible agregar el cifrado a una instancia de base de datos sin cifrar. Es decir, puede crear una instantánea de una instancia de base de datos y, a continuación, crear una copia cifrada de esa instantánea. A continuación, se puede restaurar una instancia de base de datos a partir de la instantánea cifrada y de este modo, se tiene una copia cifrada de la instancia de base de datos original.

[RDS.5] Las instancias de base de datos de RDS deben configurarse con varias zonas de disponibilidad

Requisitos relacionados: CIS AWS Foundations Benchmark v5.0. 0/2.2.4 NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 SC-5 (2) NIST.800-53.r5 SC-36, NIST.800-53.r5 SI-13 (5)

Categoría: Recuperación > Resiliencia > Alta disponibilidad

Gravedad: media

Tipo de recurso: `AWS::RDS::DBInstance`

Regla de AWS Config : `rds-multi-az-support`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si la alta disponibilidad está habilitada para sus instancias de base de datos de RDS. El control lanza un error si una instancia de base de datos de RDS no se configura con varias zonas de disponibilidad (AZ). Este control no se aplica a las instancias de base de datos de RDS que forman parte de una implementación de Multi-AZ clúster de base de datos.

La configuración de las instancias de base de datos de Amazon RDS con AZ ayuda a garantizar la disponibilidad de los datos almacenados. Multi-AZ las implementaciones permiten la conmutación por error automática si hay algún problema con la disponibilidad de las zonas de disponibilidad y durante el mantenimiento regular de un RDS.

Corrección

Para implementar sus instancias de base de datos en varias zonas de disponibilidad, consulte la Guía del usuario de Amazon RDS para modificar una Multi-AZ instancia de base de datos para convertirla en una implementación de instancia de base de datos.

[RDS.6] Se debe configurar una supervisión mejorada para las instancias de base de datos de RDS

Requisitos relacionados: NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-2

Categoría: Detectar - Servicios de detección

Gravedad: baja

Tipo de recurso: `AWS::RDS::DBInstance`

Regla de AWS Config : `rds-enhanced-monitoring-enabled`

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub CSPM	
`monitoringInterval`	Número de segundos entre los intervalos de recopilación de métricas de supervisión	Enum	`1`, `5`, `10`, `15`, `30`, `60`	Sin valor predeterminado	

Este control comprueba si la supervisión mejorada está habilitada para una instancia de base de datos de Amazon Relational Database Service (Amazon RDS). Se produce un error en el control si la supervisión mejorada no está habilitada para la instancia. Si proporciona un valor personalizado para el parámetro `monitoringInterval`, el control pasa si se recopilan métricas de supervisión mejoradas para la instancia en el intervalo especificado.

En Amazon RDS, la supervisión mejorada permite una respuesta más rápida a los cambios de rendimiento en la infraestructura subyacente. Estos cambios en el rendimiento podrían provocar una falta de disponibilidad de los datos. El monitoreo mejorado proporciona métricas en tiempo real para el sistema operativo en el que se ejecuta la instancia de base de datos de RDS. El agente está instalado en la instancia. El agente puede obtener métricas con mayor precisión de lo que es posible desde la capa del hipervisor.

Las métricas de monitorización mejoradas son útiles cuando desea ver cómo diferentes procesos o subprocesos en una instancia de base de datos usan la CPU. Para obtener más información, consulte Enhanced Monitoring (Supervisión mejorada) en la Guía del usuario de Amazon RDS.

Corrección

Para obtener instrucciones detalladas sobre cómo habilitar la supervisión mejorada para su instancia de base de datos, consulte Configuración y activación de la supervisión mejorada en la Guía del usuario de Amazon RDS.

[RDS.7] Los clústeres de RDS deben tener habilitada la protección contra eliminaciones

Requisitos relacionados: NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2)

Categoría: Proteger > Protección de datos > Protección contra la eliminación de datos

Gravedad: media

Tipo de recurso: `AWS::RDS::DBCluster`

Regla de AWS Config : `rds-cluster-deletion-protection-enabled`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un clúster de base de datos RDS tiene habilitada la protección contra eliminación. El control falla si un clúster de base de datos RDS no tiene habilitada la protección contra eliminación.

Este control está diseñado para instancias de base de datos de RDS. Sin embargo, también puede generar resultados para instancias de base de datos de Aurora, instancias de base de datos de Neptune y clústeres de Amazon DocumentDB. Si estos resultados no son útiles, puede suprimirlos.

Habilitar la protección contra la eliminación de clústeres es un nivel adicional de protección contra la eliminación accidental de la base de datos o la eliminación por parte de una entidad no autorizada.

Cuando la protección de eliminación está habilitada, no se puede eliminar un clúster de base de datos. Para que una solicitud de eliminación se pueda realizar correctamente, la protección contra la eliminación debe estar deshabilitada.

Corrección

Para habilitar la protección contra la eliminación de un clúster de base de datos de RDS, consulte Modificación del clúster de base de datos mediante la consola, la CLI y la API en la Guía del usuario de Amazon RDS. En Protección contra eliminación, elija Habilitar la protección contra eliminación.

[RDS.8] Las instancias de base de datos de RDS deben tener habilitada la protección contra eliminaciones

Requisitos relacionados: NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoría: Proteger > Protección de datos > Protección contra la eliminación de datos

Gravedad: baja

Tipo de recurso: `AWS::RDS::DBInstance`

Regla de AWS Config : `rds-instance-deletion-protection-enabled`

Tipo de horario: provocado por un cambio

Parámetros:

- `databaseEngines`: `mariadb,mysql,custom-oracle-ee,oracle-ee-cdb,oracle-se2-cdb,oracle-ee,oracle-se2,oracle-se1,oracle-se,postgres,sqlserver-ee,sqlserver-se,sqlserver-ex,sqlserver-web` (no personalizable)

Este control comprueba si las instancias de base de datos de RDS que utilizan uno de los motores de bases de datos de la lista tienen habilitada la protección contra la eliminación. El control falla si una instancia de base de datos RDS no tiene habilitada la protección contra eliminación.

La activación de la protección contra la eliminación de instancias es un nivel adicional de protección contra la eliminación accidental de la base de datos o la eliminación por parte de una entidad no autorizada.

Mientras la protección contra la eliminación está habilitada, no se puede eliminar una instancia de base de datos de RDS. Para que una solicitud de eliminación se pueda realizar correctamente, la protección contra la eliminación debe estar deshabilitada.

Corrección

Para habilitar la protección contra la eliminación de una instancia de base de datos de RDS, consulte Modificación de una instancia de base de datos de Amazon RDS en la Guía del usuario de Amazon RDS. En Protección contra eliminación, elija Habilitar la protección contra eliminación.

[RDS.9] Las instancias de base de datos de RDS deben publicar los registros en Logs CloudWatch

Requisitos relacionados: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9),, NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12 NIST.800-53.r5 AU-2 NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), (10) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SC-7 (8), NIST.800-53.r5 SI-3 (20), NIST.800-53.r5 SI-4 NIST.800-53.r5 SI-7 (8), PCI DSS v4.0. 1/102.2.1

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: `AWS::RDS::DBInstance`

Regla de AWS Config : `rds-logging-enabled`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una instancia de base de datos de Amazon RDS está configurada para publicar los siguientes registros en Amazon CloudWatch Logs. El control falla si la instancia no está configurada para publicar los siguientes registros en CloudWatch Logs:

- Oracle: Alert, Audit, Trace, Listener
- PostgreSQL: Postgresql, Upgrade
- MySQL: auditoría, error, general, SlowQuery
- MariaDB: Auditoría, error, general, SlowQuery
- SQL Server: Error, Agent
- Aurora-MySQL: Auditoría, error, general, SlowQuery
- Aurora-PostgreSQL: Postgresql

Las bases de datos de RDS deben tener habilitados los registros relevantes. El registro de la base de datos proporciona registros detallados de las solicitudes realizadas a RDS. Los registros de

las bases de datos pueden ayudar con las auditorías de seguridad y acceso y pueden ayudar a diagnosticar problemas de disponibilidad.

Corrección

Para obtener información sobre la publicación de registros de bases de datos de RDS en CloudWatch Logs, consulte Especificar los registros que se van a publicar en CloudWatch Logs en la Guía del usuario de Amazon RDS.

[RDS.10] La autenticación de IAM debe configurarse para las instancias de RDS

Requisitos relacionados: NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-6

Categoría: Proteger > Gestión del acceso seguro > Autenticación sin contraseña

Gravedad: media

Tipo de recurso: `AWS::RDS::DBInstance`

Regla de AWS Config : `rds-instance-iam-authentication-enabled`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una instancia de base de datos de RDS tiene habilitada la autenticación de bases de datos de IAM. El control falla si la autenticación de IAM no está configurada para las instancias de base de datos de RDS. Este control solo evalúa las instancias de RDS con los siguientes tipos de motor: `mysql`, `postgres`, `aurora`, `aurora-mysql`, `aurora-postgresql` y `mariadb`. Una instancia de RDS también debe estar en uno de los siguientes estados para que se genere un resultado: `available`, `backing-up`, `storage-optimization` o `storage-full`.

La autenticación de bases de datos de IAM permite autenticar las instancias de bases de datos con un token de autenticación en lugar de una contraseña. El tráfico de red hacia y desde la base de datos se cifra mediante SSL. Para obtener más información, consulte Autenticación de bases de datos de IAM en la Guía del usuario de Amazon Aurora.

Corrección

Para activar la autenticación de bases de datos de IAM en una instancia de base de datos de RDS, consulte Habilitar y deshabilitar la autenticación de bases de datos de IAM en la Guía del usuario de Amazon RDS.

[RDS.11] Las instancias de RDS deben tener habilitadas las copias de seguridad automáticas

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6 (1), NIST.800-53.r5 CP-6 (2) NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2) NIST.800-53.r5 SI-12, NIST.800-53.r5 SI-13 (5)

Categoría: Recuperación > Resiliencia > Respaldos habilitados

Gravedad: media

Tipo de recurso: `AWS::RDS::DBInstance`

Regla de AWS Config : `db-instance-backup-enabled`

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub CSPM
`backupRetentionMinimum`	El periodo mínimo de retención de copias de seguridad en días	Entero	De 7 a 35	7
`checkReadReplicas`	Comprueba si las instancias de base de datos de RDS tienen habilitadas las copias de seguridad para las réplicas de lectura	Booleano	No personalizable	`false`

Este control comprueba si la instancia de Amazon Relational Database Service tiene habilitadas las copias de seguridad automáticas y si el periodo de retención de las copias de seguridad es superior o igual al periodo especificado. Las réplicas de lectura se excluyen de la evaluación. Se produce un error en el control si las copias de seguridad no están habilitadas para la instancia o si el periodo

de retención es inferior al periodo especificado. A menos que proporcione un valor de parámetro personalizado para el período de retención de la copia de seguridad, Security Hub CSPM utiliza un valor predeterminado de 7 días.

Las copias de seguridad le ayudan a recuperarse más rápidamente de un incidente de seguridad y refuerzan la resiliencia de sus sistemas. Amazon RDS permite configurar instantáneas diarias del volumen de instancias completo. Para más información sobre las copias de seguridad automatizadas de Amazon RDS, consulte Trabajo con copias de seguridad en la Guía del usuario de Amazon RDS.

Corrección

Para habilitar copias de seguridad automatizadas para una instancia de base de datos de RDS, consulte Habilitación de copias de seguridad automatizadas en Guía del usuario de Amazon RDS.

[RDS.12] La autenticación de IAM debe configurarse para los clústeres de RDS

Requisitos relacionados: NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-6

Categoría: Proteger > Gestión del acceso seguro > Autenticación sin contraseña

Gravedad: media

Tipo de recurso: `AWS::RDS::DBCluster`

Regla de AWS Config : `rds-cluster-iam-authentication-enabled`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un clúster de base de datos de Amazon RDS tiene habilitada la autenticación de bases de datos de IAM.

La autenticación de bases de datos de IAM permite autenticar las instancias de bases de datos sin contraseña. La autenticación usa un token de autenticación. El tráfico de red hacia y desde la base de datos se cifra mediante SSL. Para obtener más información, consulte Autenticación de bases de datos de IAM en la Guía del usuario de Amazon Aurora.

Corrección

Para habilitar la autenticación de IAM para un clúster de base de datos, consulte Habilitar y deshabilitar la autenticación de bases de datos de IAM en la Guía del usuario de Amazon Aurora.

[RDS.13] Las actualizaciones automáticas de las versiones secundarias de RDS deben estar habilitadas

Requisitos relacionados: CIS AWS Foundations Benchmark v5.0. 0/2.2.2, CIS AWS Foundations Benchmark v3.0. 0/2.3.2, NIST.800-53.r5 SI-2 (2) NIST.800-53.r5 SI-2, (4), NIST.800-53.r5 SI-2 NIST.800-53.r5 SI-2 (5), PCI DSS v4.0. 1/63.3.3

Categoría: Identificar > Administración de vulnerabilidades, parches y versiones

Gravedad: alta

Tipo de recurso: `AWS::RDS::DBInstance`

Regla de AWS Config : `rds-automatic-minor-version-upgrade-enabled`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una instancia de base de datos de Amazon RDS tiene habilitadas las actualizaciones automáticas de versiones secundarias. El control falla si las actualizaciones automáticas de versiones secundarias no están habilitadas para la instancia de base de datos de RDS.

> **Note**
>
> Este control evalúa cada instancia de base de datos de Amazon RDS de forma independiente. En el caso de los clústeres de Amazon Aurora, las actualizaciones automáticas de versiones secundarias requieren que habilite esta configuración en el clúster. También debe habilitar esta configuración en todas las instancias del clúster. La `PASSED` determinación de una instancia individual no garantiza que se realicen actualizaciones si no has habilitado también la configuración a nivel de clúster.
> Este control tampoco tiene en cuenta las configuraciones que no admiten las actualizaciones automáticas de versiones secundarias. Estos incluyen los clústeres de Aurora en una base de datos global de Aurora y los clústeres de Aurora MySQL con réplicas de lectura entre regiones. Para estas configuraciones, el control puede producir resultados de evaluación que no reflejen con precisión el comportamiento real de la actualización.

Las actualizaciones automáticas de versiones secundarias actualizan periódicamente la base de datos a versiones recientes del motor. Sin embargo, es posible que la actualización no siempre

incluya la versión más reciente del motor de base de datos. Si necesita mantener las bases de datos en versiones específicas en momentos determinados, le recomendamos que las actualice manualmente a las versiones de base de datos que necesite según el calendario requerido. En casos de problemas críticos de seguridad o cuando una versión alcanza su fecha de fin de soporte, Amazon RDS podría aplicar una actualización de versión secundaria incluso si no habilitó la opción Actualización automática de versión secundaria. Para obtener más información, consulte la documentación de actualización de Amazon RDS correspondiente al motor de base de datos:

- Actualizaciones automáticas de versiones secundarias de RDS para MariaDB
- Actualizaciones automáticas de versiones secundarias para RDS para MySQL
- Actualizaciones automáticas de versiones secundarias para RDS para PostgreSQL
- Db2 en las versiones de Amazon RDS
- Actualizaciones de versiones secundarias de Oracle
- Actualizaciones del motor de base de datos de Microsoft SQL Server

Corrección

Para habilitar las actualizaciones automáticas de las versiones secundarias de una instancia de base de datos existente, consulte Modificación de una instancia de base de datos de Amazon RDS en la Guía del usuario de Amazon RDS. Para la actualización automática de una versión secundaria, seleccione Sí.

[RDS.14] Los clústeres de Amazon Aurora deben tener habilitado el retroceso

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6 (1), NIST.800-53.r5 CP-6 (2) NIST.800-53.r5 CP-9, NIST.800-53.r5 SI-13 (5)

Categoría: Recuperación > Resiliencia > Respaldos habilitados

Gravedad: media

Tipo de recurso: `AWS::RDS::DBCluster`

Regla de AWS Config : `aurora-mysql-backtracking-enabled`

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub CSPM	
`BacktrackWindowInHours`	Número de horas necesarias para hacer búsquedas de datos anteriores en un clúster Aurora MySQL	Double	De `0.1` a `72`	Sin valor predeterminado	

Este control comprueba si un clúster de Amazon Aurora tiene habilitada la característica de búsqueda de datos anteriores. Se produce un error en el control si el clúster no tiene habilitada la búsqueda de datos anteriores. Si proporciona un valor personalizado para el parámetro `BacktrackWindowInHours`, el control solo pasa si la búsqueda de datos anteriores en el clúster se hace durante el periodo especificado.

Las copias de seguridad le ayudan a recuperarse más rápidamente de un incidente de seguridad. También refuerzan la resiliencia de sus sistemas. La búsqueda de datos anteriores de Aurora reduce el tiempo de recuperación de una base de datos en un punto en el tiempo. Para ello, no es necesario restaurar la base de datos.

Corrección

Para habilitar la búsqueda de datos anteriores de Aurora, consulte Configuración de la búsqueda de datos anteriores en la Guía del usuario de Amazon Aurora.

Tenga en cuenta que no puede habilitar la búsqueda de datos anteriores en un clúster existente. En su lugar, puede crear un clon que tenga habilitado la búsqueda de datos anteriores. Para obtener más información sobre las limitaciones del búsqueda de datos anteriores de Aurora, consulte la lista de limitaciones en Descripción general de búsqueda de datos anteriores.

[RDS.15] Los clústeres de bases de datos de RDS deben configurarse para varias zonas de disponibilidad

Requisitos relacionados: CIS AWS Foundations Benchmark v5.0. 0/2.2.4 NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 SC-5 (2) NIST.800-53.r5 SC-36, NIST.800-53.r5 SI-13 (5)

Categoría: Recuperación > Resiliencia > Alta disponibilidad

Gravedad: media

Tipo de recurso: `AWS::RDS::DBCluster`

Regla de AWS Config : `rds-cluster-multi-az-enabled`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si la alta disponibilidad está habilitada para sus clústeres de base de datos de RDS. El control falla si un clúster de base de datos de RDS no se implementa en varias zonas de disponibilidad (AZ).

Los clústeres de bases de datos de RDS deben configurarse para varias zonas de disponibilidad a fin de garantizar la disponibilidad de los datos almacenados. La implementación en varias zonas de disponibilidad permite la conmutación por error automática en caso de que se produzca un problema de disponibilidad de las zonas de disponibilidad y durante los eventos de mantenimiento habituales del RDS.

Corrección

Para implementar sus clústeres de bases de datos en varias zonas de disponibilidad, consulte la Guía del usuario de Amazon RDS para modificar una Multi-AZ instancia de base de datos para convertirla en una implementación de instancia de base de datos.

Los pasos de solución son diferentes para las bases de datos globales de Aurora. Para configurar varias zonas de disponibilidad para una base de datos global de Aurora, seleccione su clúster de base de datos. A continuación, elija Acciones y Añadir lector y especifique varias zonas de disponibilidad (AZ). Para obtener más información, consulte Agregar réplicas Aurora a un clúster de base de datos en la Guía del usuario de Amazon Aurora.

[RDS.16] Los clústeres de bases de datos de Aurora deben configurarse para copiar las etiquetas a las instantáneas de bases de datos

Requisitos relacionados: NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoría: Identificar - Inventario

Gravedad: baja

Tipo de recurso: `AWS::RDS::DBCluster`

AWS Config regla: `rds-cluster-copy-tags-to-snapshots-enabled` (regla CSPM personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control verifica si un clúster de bases de datos de Amazon Aurora está configurado para copiar automáticamente las etiquetas en las instantáneas del clúster cuando dichas instantáneas se crean. El control falla si el clúster de bases de datos Aurora no está configurado para copiar automáticamente las etiquetas en las instantáneas del clúster cuando estas se crean.

La identificación y el inventario de sus activos de TI es un aspecto fundamental de seguridad y control. Debe tener visibilidad de todos los clústeres de bases de datos de Amazon Aurora para evaluar su posición de seguridad y tomar medidas ante posibles áreas de debilidad. Las instantáneas de bases de datos Aurora deben tener las mismas etiquetas que sus clústeres de bases de datos de origen. En Amazon Aurora, puede configurar un clúster de bases de datos para copiar automáticamente todas las etiquetas del clúster en sus instantáneas. Al habilitar este ajuste, las instantáneas de bases de datos heredan las mismas etiquetas que sus clústeres de origen.

Corrección

Para obtener información sobre cómo configurar un clúster de bases de datos de Amazon Aurora para copiar automáticamente las etiquetas en las instantáneas de bases de datos, consulte Modificación de un clúster de bases de datos de Amazon Aurora en la Guía del usuario de Amazon Aurora.

[RDS.17] Las instancias de base de datos de RDS deben configurarse para copiar las etiquetas de las instantáneas

Requisitos relacionados: NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoría: Identificar - Inventario

Gravedad: baja

Tipo de recurso: `AWS::RDS::DBInstance`

AWS Config regla: `rds-instance-copy-tags-to-snapshots-enabled` (regla CSPM personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si las instancias de base de datos de RDS están configuradas para copiar todas las etiquetas a las instantáneas cuando se crean las instantáneas.

La identificación y el inventario de sus activos de TI es un aspecto fundamental de seguridad y control. Tiene que tener una visión de todas sus instancias de base de datos de RDS para que pueda evaluar sus posiciones de seguridad y tomar así las acciones pertinentes respecto a las posibles áreas débiles. Las instantáneas se deben etiquetar de la misma manera que las instancias de base de datos RDS principales. Al habilitar esta configuración, se garantiza que las instantáneas hereden las etiquetas de sus instancias de base de datos principales.

Corrección

Para copiar automáticamente las etiquetas en las instantáneas de una instancia de base de datos de RDS, consulte Modificación de una instancia de base de datos de Amazon RDS en la Guía del usuario de Amazon RDS. Seleccione Copiar etiquetas en instantáneas

[RDS.19] Las suscripciones de notificación de eventos de RDS existentes deben configurarse para los eventos críticos del clúster

Requisitos relacionados: NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-2

Categoría: Detectar > Servicios de detección > Supervisión de aplicaciones

Gravedad: baja

Tipo de recurso: `AWS::RDS::EventSubscription`

AWS Config regla: `rds-cluster-event-notifications-configured` (regla CSPM personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una suscripción a eventos de Amazon RDS existente para clústeres de base de datos tiene habilitadas notificaciones para los siguientes pares clave-valor de tipo de origen y categoría de evento:

```
DBCluster: ["maintenance","failure"]
```

El control se transfiere si no hay suscripciones a eventos existentes en su cuenta.

Las notificaciones de eventos de RDS utilizan Amazon SNS para informarle de los cambios en la disponibilidad o la configuración de sus recursos de RDS. Estas notificaciones permiten una respuesta rápida. Para obtener más información sobre las notificaciones de eventos de RDS, consulte Uso de las notificaciones de eventos de Amazon RDS en la Guía del usuario de Amazon RDS.

Corrección

Para suscribirse a las notificaciones de eventos del clúster de RDS, consulte Suscribirse a las notificaciones de eventos de Amazon RDS en la Guía del usuario de Amazon RDS. Use los siguientes valores:

Campo	Valor
Tipo de origen	Clústeres
Clústeres que se van a incluir	Todos los clústeres
Categorías de eventos a incluir	Seleccione categorías de eventos específicas o Todas las categorías de eventos

[RDS.20] Las suscripciones de notificación de eventos de RDS existentes deben configurarse para los eventos críticos de las instancias de bases de datos

Requisitos relacionados: NIST.800-53.r5 CA-7 NIST.800-53.r5 SI-2, PCI DSS v4.0. 1/115.5.2

Categoría: Detectar > Servicios de detección > Supervisión de aplicaciones

Gravedad: baja

Tipo de recurso: `AWS::RDS::EventSubscription`

AWS Config regla: `rds-instance-event-notifications-configured` (regla CSPM personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una suscripción a eventos de Amazon RDS existente para instancias de base de datos tiene habilitadas notificaciones para los siguientes pares clave-valor de tipo de origen y categoría de evento:

```
DBInstance: ["maintenance","configuration change","failure"]
```

El control se transfiere si no hay suscripciones a eventos existentes en su cuenta.

Las notificaciones de eventos de RDS utilizan Amazon SNS para informarle de los cambios en la disponibilidad o la configuración de sus recursos de RDS. Estas notificaciones permiten una respuesta rápida. Para obtener más información sobre las notificaciones de eventos de RDS, consulte Uso de las notificaciones de eventos de Amazon RDS en la Guía del usuario de Amazon RDS.

Corrección

Para suscribirse a las notificaciones de eventos de instancias de RDS, consulte Suscribirse a las notificaciones de eventos de Amazon RDS en la Guía del usuario de Amazon RDS. Use los siguientes valores:

Campo	Valor
Tipo de origen	instancias
Instancias que se van a incluir	Todas las instancias
Categorías de eventos a incluir	Seleccione categorías de eventos específicas o Todas las categorías de eventos

[RDS.21] Se debe configurar una suscripción a las notificaciones de eventos de RDS para los eventos de grupos de parámetros de base de datos críticos

Requisitos relacionados: NIST.800-53.r5 CA-7 NIST.800-53.r5 SI-2, PCI DSS v4.0. 1/115.5.2

Categoría: Detectar > Servicios de detección > Supervisión de aplicaciones

Gravedad: baja

Tipo de recurso: `AWS::RDS::EventSubscription`

AWS Config regla: `rds-pg-event-notifications-configured` (regla CSPM personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si existe una suscripción a eventos de Amazon RDS con notificaciones habilitadas para los siguientes pares clave-valor de tipo de fuente y categoría de evento. El control se transfiere si no hay suscripciones a eventos existentes en su cuenta.

```
DBParameterGroup: ["configuration change"]
```

Las notificaciones de eventos de RDS utilizan Amazon SNS para informarle de los cambios en la disponibilidad o la configuración de sus recursos de RDS. Estas notificaciones permiten una respuesta rápida. Para obtener más información sobre las notificaciones de eventos de RDS, consulte Uso de las notificaciones de eventos de Amazon RDS en la Guía del usuario de Amazon RDS.

Corrección

Para suscribirse a las notificaciones de eventos del grupo de parámetros de la base de datos de RDS, consulte Suscripción a la notificación de eventos de Amazon RDS en la Guía del usuario de Amazon RDS. Use los siguientes valores:

Campo	Valor
Tipo de origen	Grupos de parámetros
Grupos de parámetros que se van a incluir	Todos los grupos de parámetros
Categorías de eventos a incluir	Seleccione categorías de eventos específicas o Todas las categorías de eventos

[RDS.22] Se debe configurar una suscripción a las notificaciones de eventos de RDS para los eventos críticos de grupos de seguridad de bases de datos

Requisitos relacionados: NIST.800-53.r5 CA-7 NIST.800-53.r5 SI-2, PCI DSS v4.0. 1/115.5.2

Categoría: Detectar > Servicios de detección > Supervisión de aplicaciones

Gravedad: baja

Tipo de recurso: `AWS::RDS::EventSubscription`

AWS Config regla: `rds-sg-event-notifications-configured` (regla CSPM personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si existe una suscripción a eventos de Amazon RDS con notificaciones habilitadas para los siguientes pares clave-valor de tipo de fuente y categoría de evento. El control se transfiere si no hay suscripciones a eventos existentes en su cuenta.

```
DBSecurityGroup: ["configuration change","failure"]
```

Las notificaciones de eventos de RDS utilizan Amazon SNS para informarle de los cambios en la disponibilidad o la configuración de sus recursos de RDS. Estas notificaciones permiten una respuesta rápida. Para obtener más información sobre las notificaciones de eventos de RDS, consulte Uso de las notificaciones de eventos de Amazon RDS en la Guía del usuario de Amazon RDS.

Corrección

Para suscribirse a las notificaciones de eventos de instancias de RDS, consulte Suscribirse a las notificaciones de eventos de Amazon RDS en la Guía del usuario de Amazon RDS. Use los siguientes valores:

Campo	Valor
Tipo de origen	Grupos de seguridad
Grupos de seguridad que se van a incluir	Todos los grupos de seguridad
Categorías de eventos a incluir	Seleccione categorías de eventos específicas o Todas las categorías de eventos

[RDS.23] Las instancias de RDS no deben usar el puerto predeterminado de un motor de base de datos

Requisitos relacionados: NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (5)

Categoría: Proteger - Configuración de red segura

Gravedad: baja

Tipo de recurso: `AWS::RDS::DBInstance`

AWS Config regla: `rds-no-default-ports` (regla CSPM personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un clúster o instancia de RDS utiliza un puerto distinto del puerto predeterminado del motor de base de datos. El control falla si el clúster o la instancia de RDS utilizan el puerto predeterminado. Este control no se aplica a las instancias de RDS que forman parte de un clúster.

Si utiliza un puerto conocido para implementar un clúster o una instancia de RDS, un atacante puede adivinar la información sobre el clúster o la instancia. El atacante puede usar esta información junto con otra información para conectarse a un clúster o instancia de RDS u obtener información adicional sobre la aplicación.

Al cambiar el puerto, también debe actualizar las cadenas de conexión existentes que se utilizaron para conectarse al puerto anterior. También debe comprobar el grupo de seguridad de la instancia de base de datos para asegurarse de que incluye una regla de entrada que permita la conectividad en el nuevo puerto.

Corrección

Para modificar el puerto predeterminado de una instancia de base de datos de RDS existente, consulte Modificación de una instancia de base de datos de Amazon RDS en la Guía del usuario de Amazon RDS. Para modificar el puerto predeterminado de un clúster de base de datos de RDS existente, consulte Modificación del clúster de base de datos mediante la consola, la CLI y la API en la Guía del usuario de Amazon Aurora. Para el Puerto de base de datos, cambie el valor del puerto por un valor que no sea el predeterminado.

[RDS.24] Los clústeres de bases de datos de RDS deben usar un nombre de usuario de administrador personalizado

Requisitos relacionados: NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, PCI DSS v4.0. 1/22.2.2

Categoría: Identificar > Configuración de recursos

Gravedad: media

Tipo de recurso: `AWS::RDS::DBCluster`

Regla de AWS Config : `rds-cluster-default-admin-check`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un clúster de base de datos de Amazon RDS ha cambiado el nombre de usuario de administrador con respecto a su valor predeterminado. El control no se aplica a los motores del tipo neptune (Neptune DB) o docdb (DocumentDB). Esta regla fallará si el nombre de usuario del administrador está establecido en el valor predeterminado.

Al crear una base de datos de Amazon RDS, debe cambiar el nombre de usuario de administrador predeterminado por un valor único. Los nombres de usuario predeterminados son de dominio público y deben cambiarse durante la creación de la base de datos de RDS. Cambiar los nombres de usuario predeterminados reduce el riesgo de accesos no deseados.

Corrección

Para cambiar el nombre de usuario de administrador asociado al clúster de base de datos de Amazon RDS, cree un nuevo clúster de base de datos de RDS y cambie el nombre de usuario de administrador predeterminado al crear la base de datos.

[RDS.25] Las instancias de bases de datos de RDS deben usar un nombre de usuario de administrador personalizado

Requisitos relacionados: NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, PCI DSS v4.0. 1/22.2.2

Categoría: Identificar > Configuración de recursos

Gravedad: media

Tipo de recurso: `AWS::RDS::DBInstance`

Regla de AWS Config : `rds-instance-default-admin-check`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si ha cambiado el nombre de usuario administrativo de las instancias de base de datos de Amazon Relational Database Service (Amazon RDS) con respecto al valor predeterminado. El control falla si el nombre de usuario administrativo está establecido en el valor predeterminado. El control no se aplica a motores del tipo Neptune (Neptune-DB) o DocDB (DocumentDB), ni a las instancias de RDS que forman parte de un clúster.

Los nombres de usuario administrativos predeterminados en las bases de datos de Amazon RDS son de dominio público. Al crear una base de datos de Amazon RDS, debe cambiar el nombre de usuario administrativo predeterminado por un valor único para reducir el riesgo de accesos no deseados.

Corrección

Para cambiar el nombre de usuario administrativo asociado a una instancia de base de datos de RDS, cree primero una nueva instancia de base de datos de RDS. Cambie el nombre de usuario administrativo predeterminado al crear la base de datos.

[RDS.26] Las instancias de base de datos de RDS deben protegerse mediante un plan de respaldo

Categoría: Recuperación > Resiliencia > Respaldos habilitados

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6 (1), NIST.800-53.r5 CP-6 (2) NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2) NIST.800-53.r5 SI-12, NIST.800-53.r5 SI-13 (5)

Gravedad: media

Tipo de recurso: `AWS::RDS::DBInstance`

AWS Config regla: `rds-resources-protected-by-backup-plan`

Tipo de programa: Periódico

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub CSPM
`backupVaultLockCheck`	El control produce un `PASSED` resultado si el parámetro está establecido en verdadero y el recurso usa AWS Backup Vault Lock.	Booleano	`true` o `false`	Sin valor predeterminado

Este control evalúa si las instancias de base de datos de Amazon RDS están cubiertas por un plan de copias de seguridad. Se produce un error en este control si la instancia de base de datos de RDS no está cubierta por un plan de copias de seguridad. Si estableces el `backupVaultLockCheck` parámetro en`true`, el control solo se realizará si se ha realizado una copia de seguridad de la instancia en un almacén AWS Backup cerrado.

> **Note**
>
> Este control no evalúa las instancias de Neptune ni las de DocumentDB. Tampoco evalúa las instancias de bases de datos de RDS que son miembros de un clúster.

AWS Backup es un servicio de respaldo totalmente administrado que centraliza y automatiza el respaldo de los datos en todas partes. Servicios de AWS Con AWS Backup, puede crear políticas de respaldo denominadas planes de respaldo. Puede utilizar estos planes para definir los requisitos de copia de seguridad, como la frecuencia con la que se va a realizar la copia de seguridad de los datos y el tiempo durante el que se van a conservar esas copias de seguridad. La inclusión de instancias de base de datos de RDS en un plan de copias de seguridad le ayuda a proteger sus datos contra pérdidas o eliminaciones involuntarias.

Corrección

Para agregar una instancia de base de datos de RDS a un plan de AWS Backup respaldo, consulte Asignar recursos a un plan de respaldo en la Guía para AWS Backup desarrolladores.

[RDS.27] Los clústeres de bases de datos de RDS deben cifrarse en reposo

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6),, NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6)

Categoría: Proteger > Protección de datos > Cifrado de datos en reposo

Gravedad: media

Tipo de recurso: `AWS::RDS::DBCluster`

AWS Config regla: `rds-cluster-encrypted-at-rest`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un clúster de base de datos de RDS está cifrado en reposo. El control falla si un clúster de base de datos de RDS no está cifrado en reposo.

Los datos en reposo se refieren a cualquier dato que se almacene en un almacenamiento persistente y no volátil durante cualquier período de tiempo. El cifrado le ayuda a proteger la confidencialidad de dichos datos, reduciendo el riesgo de que un usuario no autorizado pueda acceder a ellos. El cifrado de los clústeres de bases de datos de RDS protege sus datos y metadatos contra el acceso no autorizado. También cumple con los requisitos de conformidad para el cifrado de datos en reposo de los sistemas de archivos de producción.

Corrección

Puede habilitar el cifrado en reposo al crear un clúster de base de datos de RDS. No se puede cambiar la configuración de cifrado después de crear un clúster. Para obtener más información, consulte Cifrado de un clúster de base de datos de Amazon Aurora en la Guía del usuario de Amazon Aurora.

[RDS.28] Los clústeres de bases de datos de RDS deben etiquetarse

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::RDS::DBCluster`

AWS Config regla: `tagged-rds-dbcluster` (regla CSPM personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub CSPM
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si un clúster de base de datos de Amazon RDS tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza un error si el clúster de base de datos no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si el clúster de base de datos no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y se compone de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWSen la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Las etiquetas son accesibles para muchos Servicios de AWS, incluso AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulta Cómo etiquetar tus AWS recursos en. Referencia general de AWS

Corrección

Para agregar etiquetas a un clúster de base de datos de RDS, consulte Etiquetado de los recursos de Amazon RDS en la Guía del usuario de Amazon RDS.

[RDS.29] Las instantáneas del clúster de bases de datos de RDS deben etiquetarse

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::RDS::DBClusterSnapshot`

AWS Config regla: `tagged-rds-dbclustersnapshot` (regla CSPM personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub CSPM
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si una instantánea de clúster de base de datos de Amazon RDS tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza un error si la instantánea de clúster de base de datos no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si la instantánea de clúster de base de datos no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y se compone de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWSen la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Las etiquetas son accesibles para muchos Servicios de AWS, incluso AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulta Cómo etiquetar tus AWS recursos en. Referencia general de AWS

Corrección

Para agregar etiquetas a la instantánea de clúster de base de datos de RDS, consulte Etiquetado de los recursos de Amazon RDS en la Guía del usuario de Amazon RDS.

[RDS.30] Las instancias de base de datos de RDS deben etiquetarse

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::RDS::DBInstance`

AWS Config regla: `tagged-rds-dbinstance` (regla CSPM personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub CSPM
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si una instancia de base de datos de Amazon RDS tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza un error si la instancia de base de datos no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si la instancia de base de datos no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y se compone de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan

operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWSen la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Las etiquetas son accesibles para muchos Servicios de AWS, incluso AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulta Cómo etiquetar tus AWS recursos en. Referencia general de AWS

Corrección

Para agregar etiquetas a una instancia de base de datos de RDS, consulte Etiquetado de los recursos de Amazon RDS en la Guía del usuario de Amazon RDS.

[RDS.31] Los grupos de seguridad de la base de datos de RDS deben etiquetarse

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::RDS::DBSecurityGroup`

AWS Config regla: `tagged-rds-dbsecuritygroup` (regla CSPM personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub CSPM
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que	Sin valor predeterminado

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub CSPM
	recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.		cumplan los requisitos de AWS.	

Este control comprueba si un grupo de seguridad de base de datos de Amazon RDS tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza un error si el grupo de seguridad de base de datos no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si el grupo de seguridad de base de datos no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y se compone de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWSen la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Las etiquetas son accesibles para muchos Servicios de AWS, incluso AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulta Cómo etiquetar tus AWS recursos en. Referencia general de AWS

Corrección

Para agregar etiquetas a un grupo de seguridad de base de datos de RDS, consulte Etiquetado de los recursos de Amazon RDS en la Guía del usuario de Amazon RDS.

[RDS.32] Las instantáneas de la base de datos de RDS deben etiquetarse

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::RDS::DBSnapshot`

AWS Config regla: `tagged-rds-dbsnapshot` (regla CSPM personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub CSPM
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si una instantánea de base de datos de Amazon RDS tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza un error si la instantánea de base de datos no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si la instantánea de base de datos no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y se compone de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWSen la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Las etiquetas son accesibles para muchos Servicios de AWS, incluso AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulta Cómo etiquetar tus AWS recursos en. Referencia general de AWS

Corrección

Para agregar una instantánea de base de datos de RDS, consulte Etiquetado de los recursos de Amazon RDS en la Guía del usuario de Amazon RDS.

[RDS.33] Los grupos de subredes de bases de datos de RDS deben etiquetarse

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::RDS::DBSubnetGroup`

AWS Config regla: `tagged-rds-dbsubnetgroups` (regla CSPM personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub CSPM
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si un grupo de subredes de bases de datos de Amazon RDS tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza un error si el grupo de subredes de bases de datos no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si el grupo de subredes de bases de datos no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y se compone de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWSen la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Las etiquetas son accesibles para muchos Servicios de AWS, incluso AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulta Cómo etiquetar tus AWS recursos en. Referencia general de AWS

Corrección

Para agregar etiquetas a un grupo de subredes de bases de datos de RDS, consulte Etiquetado de los recursos de Amazon RDS en la Guía del usuario de Amazon RDS.

[RDS.34] Los clústeres de bases de datos Aurora MySQL deben publicar los registros de auditoría en Logs CloudWatch

Requisitos relacionados: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9),, NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12 NIST.800-53.r5 AU-2 NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), (9) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (8), NIST.800-53.r5 SI-3 (20), NIST.800-53.r5 SI-4 NIST.800-53.r5 SI-7 (8), PCI DSS v4.0. 1/102.2.1

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: `AWS::RDS::DBCluster`

AWS Config regla: `rds-aurora-mysql-audit-logging-enabled`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un clúster de base de datos Amazon Aurora MySQL está configurado para publicar registros de auditoría en Amazon CloudWatch Logs. El control falla si el clúster no está configurado para publicar los registros de auditoría en CloudWatch Logs. El control no genera resultados para los clústeres de base de datos Aurora sin servidor v1.

Los registros de auditoría recopilan un registro de la actividad de la base de datos, incluidos los intentos de inicio de sesión, las modificaciones de datos, los cambios de esquema y otros eventos que se pueden auditar por motivos de seguridad y conformidad. Al configurar un clúster de base de

datos Aurora MySQL para publicar los registros de auditoría en un grupo de CloudWatch registros de Amazon Logs, puede realizar un análisis de los datos de registro en tiempo real. CloudWatch Logs conserva los registros en un almacenamiento muy duradero. También puede crear alarmas y ver las métricas en CloudWatch.

> **Note**
>
> Una forma alternativa de publicar los registros de auditoría en CloudWatch Logs es habilitar la auditoría avanzada y establecer el parámetro de base de datos a nivel de clúster en. `server_audit_logs_upload` 1 El valor predeterminado de `server_audit_logs_upload parameter` es `0`. Sin embargo, le recomendamos que utilice las siguientes instrucciones de corrección para pasar este control.

Corrección

Para publicar los registros de auditoría de clústeres de bases de datos de Aurora MySQL en CloudWatch Logs, consulte Publicación de registros de Amazon Aurora MySQL en Amazon Logs en la Guía del CloudWatch usuario de Amazon Aurora.

[RDS.35] Los clústeres de bases de datos de RDS deben tener habilitada la actualización automática de versiones secundarias

Requisitos relacionados: NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2 (2), NIST.800-53.r5 SI-2 (4), NIST.800-53.r5 SI-2 (5), PCI DSS v4.0. 1/63.3.3

Categoría: Identificar > Administración de vulnerabilidades, parches y versiones

Gravedad: media

Tipo de recurso: `AWS::RDS::DBCluster`

AWS Config regla: `rds-cluster-auto-minor-version-upgrade-enable`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si la actualización automática de versiones secundarias está habilitada para un clúster de base de datos de Amazon RDS, incluidos los clústeres de bases de datos Aurora. El

control falla si la actualización automática de versiones secundarias no está habilitada para el clúster de base de datos.

Con la actualización automática de versiones secundarias, puede mantener su clúster de base de datos actualizado. Las versiones secundarias pueden introducir nuevas funciones de software, correcciones de errores, parches de seguridad y mejoras de rendimiento. Al habilitar la actualización automática de las versiones secundarias en los clústeres de bases de datos de RDS, el clúster, junto con las instancias del clúster, recibirá actualizaciones automáticas de la versión secundaria cuando haya nuevas versiones disponibles. Las actualizaciones se aplican automáticamente durante el período de mantenimiento.

Corrección

Para habilitar la actualización automática de versiones secundarias en los clústeres de Multi-AZ bases de datos, consulte Modificación de un Multi-AZ clúster de bases de datos en la Guía del usuario de Amazon RDS.

Para habilitar la actualización automática de versiones secundarias en los clústeres de bases de datos de Aurora, consulte Modificación de un clúster de base de datos de Amazon Aurora en la Guía del usuario de Amazon Aurora.

[RDS.36] Las instancias de base de datos de RDS para PostgreSQL deben publicar los registros en Logs CloudWatch

Requisitos relacionados: PCI DSS v4.0. 1/104.2.2

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: `AWS::RDS::DBInstance`

Regla de AWS Config : rds-postgresql-logs-to-cloudwatch

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub CSPM
`logTypes`	Comma-separated lista de tipos de registro que se publicarán en Logs CloudWatch	StringList	No personalizable	`postgresql`

Este control comprueba si una instancia de base de datos de Amazon RDS para PostgreSQL está configurada para publicar registros en Amazon Logs. CloudWatch El control falla si la instancia de base de datos de PostgreSQL no está configurada para publicar los tipos de registro mencionados en el parámetro en Logs. `logTypes` CloudWatch

El registro de base de datos proporciona detalles sobre las solicitudes realizadas a una instancia de RDS. PostgreSQL genera registros de eventos que contienen información útil para los administradores. La publicación de estos registros en CloudWatch Logs centraliza la administración de los registros y le ayuda a realizar un análisis en tiempo real de los datos de registro. CloudWatch Logs conserva los registros en un almacenamiento muy duradero. También puede crear alarmas y ver las métricas enCloudWatch.

Corrección

Para publicar registros de instancias de base de datos de PostgreSQL en CloudWatch Logs, consulte Publicación de registros de PostgreSQL en Amazon Logs en la guía del CloudWatch usuario de Amazon RDS.

[RDS.37] Los clústeres de bases de datos de Aurora PostgreSQL deben publicar los registros en Logs CloudWatch

Requisitos relacionados: PCI DSS v4.0. 1/104.2.2

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: `AWS::RDS::DBCluster`

Regla de AWS Config : rds-aurora-postgresql-logs-to-cloudwatch

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un clúster de base de datos PostgreSQL de Amazon Aurora está configurado para publicar registros en Amazon Logs. CloudWatch El control falla si el clúster de base de datos Aurora PostgreSQL no está configurado para publicar los registros de PostgreSQL en Logs. CloudWatch

El registro de base de datos proporciona detalles sobre las solicitudes realizadas a un clúster de RDS. Aurora PostgreSQL genera registros de eventos que contienen información útil para los administradores. La publicación de estos registros en Logs centraliza la administración de CloudWatch los registros y le ayuda a realizar un análisis en tiempo real de los datos de registro. CloudWatch Logs conserva los registros en un almacenamiento muy duradero. También puede crear alarmas y ver las métricas en CloudWatch.

Corrección

Para publicar los registros del clúster de bases de datos de Aurora PostgreSQL en CloudWatch Logs, consulte Publicar los registros de Aurora PostgreSQL en Amazon Logs en la guía del CloudWatch usuario de Amazon RDS.

[RDS.38] Las instancias de base de datos de RDS para PostgreSQL deben cifrarse en tránsito

Categoría: Proteger > Protección de datos > Cifrado de datos en tránsito

Gravedad: media

Tipo de recurso: `AWS::RDS::DBInstance`

Regla de AWS Config : rds-postgres-instance-encrypted-in-transit

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si una conexión a una instancia Amazon RDS for PostgreSQL de base de datos (DB) está cifrada en tránsito. El control falla si el parámetro `rds.force_ssl`, correspondiente al grupo de parámetros asociado con la instancia, está configurado en `0` (desactivado). Este control no evalúa las instancias de bases de datos de RDS que forman parte de un clúster de bases de datos.

Los datos en tránsito hacen referencia a los datos que se mueven de una ubicación a otra, por ejemplo, entre los nodos del clúster o entre el clúster y la aplicación. Los datos pueden moverse a través de Internet o dentro de una red privada. El cifrado de los datos en tránsito reduce el riesgo de que un usuario no autorizado pueda espiar el tráfico de la red.

Corrección

Para exigir que todas las conexiones a la instancia de base de datos RDS para PostgreSQL usen SSL, consulte Uso de SSL con una instancia de base de datos PostgreSQL en la Guía del usuario de Amazon RDS.

[RDS.39] Las instancias de base de datos de RDS para MySQL deben cifrarse en tránsito

Categoría: Proteger > Protección de datos > Cifrado de datos en tránsito

Gravedad: media

Tipo de recurso: `AWS::RDS::DBInstance`

Regla de AWS Config : rds-mysql-instance-encrypted-in-transit

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si una conexión a una instancia de Amazon RDS for MySQL base de datos (DB) está cifrada en tránsito. El control falla si el parámetro `rds.require_secure_transport`, correspondiente al grupo de parámetros asociado con la instancia, está configurado en `0` (desactivado). Este control no evalúa las instancias de bases de datos de RDS que forman parte de un clúster de bases de datos.

Los datos en tránsito hacen referencia a los datos que se mueven de una ubicación a otra, por ejemplo, entre los nodos del clúster o entre el clúster y la aplicación. Los datos pueden moverse a través de Internet o dentro de una red privada. El cifrado de los datos en tránsito reduce el riesgo de que un usuario no autorizado pueda espiar el tráfico de la red.

Corrección

Para exigir que todas las conexiones a su instancia de base de datos de RDS para MySQL utilicen SSL, consulte la SSL/TLS compatibilidad de las instancias de base de datos de MySQL en Amazon RDS en la guía del usuario de Amazon RDS.

[RDS.40] Las instancias de base de datos de RDS para SQL Server deben publicar los registros en Logs CloudWatch

Requisitos relacionados: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2 NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8)

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: `AWS::RDS::DBInstance`

Regla de AWS Config : rds-sql-server-logs-to-cloudwatch

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub CSPM
`logTypes`	Una lista de los tipos de registros que una instancia de base de datos de RDS para SQL Server debe configurarse para publicar en Logs. CloudWatch Este control falla si una instancia de base de datos no está configurada para publicar un tipo de registro especificado en la lista.	EnumList (máximo de 2 elementos)	`agent`, `error`	`agent`, `error`

Este control comprueba si una instancia de base de datos de Amazon RDS para Microsoft SQL Server está configurada para publicar registros en Amazon CloudWatch Logs. El control falla si la instancia de base de datos de RDS para SQL Server no está configurada para publicar registros en Logs. CloudWatch Puede indicar, si así lo desea, los tipos de registros que la instancia de base de datos debe publicar.

El registro de base de datos proporciona registros detallados de las solicitudes hechas a una instancia de base de datos de Amazon RDS. La publicación de registros en CloudWatch Logs centraliza la administración de registros y le ayuda a realizar análisis de los datos de registro en tiempo real. CloudWatch Logs conserva los registros en un almacenamiento muy duradero. Además, esta capacidad permite configurar alarmas para errores que puedan presentarse, como reinicios frecuentes registrados en el registro de errores. Del mismo modo, puede configurar alarmas para errores o advertencias registrados en los registros del agente de SQL Server relacionados con trabajos del agente de SQL.

Corrección

Para obtener información sobre la publicación de registros en CloudWatch Logs para una instancia de base de datos de RDS para SQL Server, consulte los archivos de registro de bases de datos de Amazon RDS para Microsoft SQL Server en la Guía del usuario de Amazon Relational Database Service.

[RDS.41] Las instancias de base de datos de RDS para SQL Server deben cifrarse en tránsito

Categoría: Proteger > Protección de datos > Cifrado de datos en tránsito

Gravedad: media

Tipo de recurso: `AWS::RDS::DBInstance`

Regla de AWS Config : rds-sqlserver-encrypted-in-transit

Tipo de programa: Periódico

Parámetros: ninguno

Este control verifica si la conexión a una instancia de base de datos de Amazon RDS para Microsoft SQL Server está cifrada en tránsito. El control falla si el parámetro `rds.force_ssl` del grupo de parámetros asociado con la instancia está configurado en `0 (off)`.

Los datos en tránsito corresponden a datos que se desplazan de un lugar a otro, por ejemplo, entre nodos dentro de un clúster de bases de datos o entre un clúster de base de datos y una aplicación

cliente. Los datos se pueden trasladar por Internet o dentro de una red privada. Cifrar los datos en tránsito reduce el riesgo de que usuarios no autorizados intercepten el tráfico de red.

Corrección

Para obtener información sobre cómo habilitar SSL/TLS las conexiones a instancias de base de datos de Amazon RDS que ejecuten Microsoft SQL Server, consulte Cómo usar SSL con una instancia de base de datos de Microsoft SQL Server en la Guía del usuario de Amazon Relational Database Service.

[RDS.42] Las instancias de base de datos de RDS para MariaDB deben publicar los registros en Logs CloudWatch

Requisitos relacionados: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-2 NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4),,, NIST.800-53.r5 AU-10 NIST.800-53.r5 AU-12, NIST.800-53.r5 SC-7 (9) NIST.800-53.r5 CA-7, (10), NIST.800-53.r5 SC-7 (8), NIST.800-53.r5 SI-3 (20), NIST.800-53.r5 SI-4 (8) NIST.800-53.r5 SI-7

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: `AWS::RDS::DBInstance`

Regla de AWS Config : mariadb-publish-logs-to-cloudwatch-logs

Tipo de programa: Periódico

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub CSPM
`logTypes`	Una lista de los tipos de registros que una instancia de base de datos de MariaDB debe configurarse para	EnumList (máximo de 4 elementos)	`audit`, `error`, `general`, `slowquery`	`audit, error`

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub CSPM
	publicar en Logs. CloudWatch El control genera un resultado `FAILED` si la instancia no está configurada para publicar alguno de los tipos de registros especificados en la lista.			

Este control comprueba si una instancia de base de datos de Amazon RDS para MariaDB está configurada para publicar determinados tipos de registros en Amazon Logs. CloudWatch El control falla si la instancia de base de datos de MariaDB no está configurada para publicar los registros en Logs. CloudWatch Puede indicar, si así lo desea, los tipos de registros que la instancia de MariaDB debe publicar.

El registro de base de datos proporciona información detallada sobre las solicitudes realizadas a una instancia de Amazon RDS para MariaDB. La publicación de los registros en Amazon CloudWatch Logs centraliza la administración de los registros y le ayuda a realizar un análisis en tiempo real de los datos de registro. Además, CloudWatch Logs conserva los registros en un almacenamiento duradero, lo que permite realizar auditorías y revisiones de seguridad, acceso y disponibilidad. Con CloudWatch Logs, también puedes crear alarmas y revisar las métricas.

Corrección

Para obtener información sobre la configuración de una instancia de base de datos de Amazon RDS para MariaDB para publicar registros en Amazon Logs, consulte Publicación de CloudWatch registros de MariaDB en Amazon Logs en la Guía del usuario de Amazon CloudWatch Relational Database Service.

[RDS.43] Los proxies de bases de datos de RDS deben requerir el cifrado TLS para las conexiones

Categoría: Proteger > Protección de datos > Cifrado de datos en tránsito

Gravedad: media

Tipo de recurso: `AWS::RDS::DBProxy`

Regla de AWS Config : rds-proxy-tls-encryption

Tipo de programa: Periódico

Parámetros: ninguno

Este control verifica si un proxy de bases de datos de Amazon RDS exige TLS para todas las conexiones entre el proxy y la instancia de base de datos de RDS subyacente. El control falla si el proxy no exige TLS para todas las conexiones entre el proxy y la instancia de base de datos de RDS.

Amazon RDS Proxy puede actuar como una capa adicional de seguridad entre las aplicaciones cliente y las instancias de bases de datos de RDS subyacentes. Por ejemplo, se puede conectar a un proxy de RDS con TLS 1.3, incluso si la instancia de base de datos subyacente solo admite una versión anterior de TLS. Al utilizar RDS Proxy, puede imponer requisitos estrictos de autenticación para las aplicaciones de base de datos.

Corrección

Para obtener información sobre cómo modificar la configuración de un proxy de Amazon RDS para exigir TLS, consulte la Modificación de un proxy de RDS en la Guía del usuario de Amazon Relational Database Service.

[RDS.44] Las instancias de base de datos de RDS para MariaDB deben cifrarse durante el tránsito

Categoría: Proteger > Protección de datos > Cifrado de datos en tránsito

Gravedad: media

Tipo de recurso: `AWS::RDS::DBInstance`

Regla de AWS Config : rds-mariadb-instance-encrypted-in-transit

Tipo de programa: Periódico

Parámetros: ninguno

Este control verifica si las conexiones a una instancia de base de datos de Amazon RDS para MariaDB están cifradas en tránsito. El control falla si el grupo de parámetros de base

de datos asociado con la instancia de base de datos no está sincronizado o si el parámetro `require_secure_transport` del grupo de parámetros no está configurado en 0N.

> **Note**
>
> Este control no evalúa instancias de bases de datos de Amazon RDS que utilizan versiones de MariaDB anteriores a la versión 10.5. El parámetro `require_secure_transport` se admite únicamente para versiones de MariaDB 10.5 y posteriores.

Los datos en tránsito corresponden a datos que se desplazan de un lugar a otro, por ejemplo, entre nodos dentro de un clúster de bases de datos o entre un clúster de base de datos y una aplicación cliente. Los datos se pueden trasladar por Internet o dentro de una red privada. Cifrar los datos en tránsito reduce el riesgo de que usuarios no autorizados intercepten el tráfico de red.

Corrección

Para obtener información sobre cómo habilitar SSL/TLS las conexiones a una instancia de base de datos de Amazon RDS para MariaDB, consulte Cómo exigir SSL/TLS todas las conexiones a una instancia de base de datos de MariaDB en la Guía del usuario del Amazon Relational Database Service.

[RDS.45] Los clústeres de bases de datos Aurora MySQL deben tener habilitado el registro de auditoría

Requisitos relacionados: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9),, NIST.800-53.r5 AU-2 NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4),, NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8)

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: `AWS::RDS::DBCluster`

Regla de AWS Config : aurora-mysql-cluster-audit-logging

Tipo de programa: Periódico

Parámetros: ninguno

Este control verifica si un clúster de bases de datos de Amazon Aurora MySQL tiene habilitado el registro de auditoría. El control falla si el grupo de parámetros de base de datos asociado al clúster de base de datos no está sincronizado, si el parámetro `server_audit_logging` no está configurado en `1` o si el parámetro `server_audit_events` está configurado en un valor vacío.

Los registros de bases de datos pueden ayudar con auditorías de seguridad y acceso, y contribuir al diagnóstico de problemas de disponibilidad. Los registros de auditoría recopilan un registro de la actividad de la base de datos, incluidos los intentos de inicio de sesión, las modificaciones de datos, los cambios de esquema y otros eventos que se pueden auditar por motivos de seguridad y conformidad.

Corrección

Para obtener información sobre cómo habilitar el registro en un clúster de base de datos de Amazon Aurora MySQL, consulte la publicación de los registros de Amazon Aurora MySQL en Amazon CloudWatch Logs en la guía del usuario de Amazon Aurora.

[RDS.46] Las instancias de base de datos de RDS no deben implementarse en subredes públicas con rutas a pasarelas de Internet

Categoría: Proteger > Configuración de red segura > Recursos no accesibles públicamente

Gravedad: alta

Tipo de recurso: `AWS::RDS::DBInstance`

Regla de AWS Config : rds-instance-subnet-igw-check

Tipo de programa: Periódico

Parámetros: ninguno

Este control verifica si una instancia de base de datos de Amazon RDS está implementada en una subred pública que tiene una ruta hacia una puerta de enlace de Internet. El control falla si la instancia de base de datos de RDS está implementada en una subred que tiene una ruta hacia una puerta de enlace de Internet y el destino está configurado en `0.0.0.0/0` o `::/0`.

Al aprovisionar los recursos de Amazon RDS en subredes privadas, puede evitar que los recursos de RDS reciban tráfico entrante desde Internet pública, lo cual puede prevenir accesos no intencionados a las instancias de bases de datos de RDS. Si los recursos de RDS se aprovisionan en una subred

pública que está abierta a Internet, estos podrían ser vulnerables a riesgos como la filtración de datos.

Corrección

Para obtener información sobre cómo aprovisionar una subred privada para una instancia de base de datos de Amazon RDS, consulte la Uso de una instancia de base de datos en una VPC en la Guía del usuario de Amazon Relational Database Service.

[RDS.47] Los clústeres de bases de datos de RDS para PostgreSQL deben configurarse para copiar las etiquetas a las instantáneas de bases de datos

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::RDS::DBCluster`

Regla de AWS Config : rds-pgsql-cluster-copy-tags-to-snapshot-check

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control verifica si un clúster de bases de datos de Amazon RDS para PostgreSQL está configurado para copiar etiquetas automáticamente en las instantáneas del clúster de base de datos cuando estas se crean. El control falla si el parámetro `CopyTagsToSnapshot` está configurado en `false` para el clúster de bases de datos de RDS para PostgreSQL.

Copiar etiquetas en las instantáneas de bases de datos ayuda a mantener un seguimiento adecuado de recursos, una gobernanza correcta y una asignación de costos apropiada entre los recursos de copia de seguridad. Esto permite una identificación coherente de recursos, control de acceso y supervisión de cumplimiento tanto en las bases de datos activas como en sus instantáneas. Las instantáneas etiquetadas correctamente mejoran las operaciones de seguridad al garantizar que los recursos de copia de seguridad hereden los mismos metadatos que sus bases de datos de origen.

Corrección

Para obtener información sobre cómo configurar un clúster de bases de datos de Amazon RDS para PostgreSQL para copiar etiquetas automáticamente en las instantáneas de bases de datos, consulte

la Etiquetado de recursos de Amazon RDS en la Guía del usuario de Amazon Relational Database Service.

[RDS.48] Los clústeres de bases de datos de RDS para MySQL deben configurarse para copiar etiquetas a las instantáneas de bases de datos

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::RDS::DBCluster`

Regla de AWS Config : rds-mysql-cluster-copy-tags-to-snapshot-check

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control verifica si un clúster de bases de datos de Amazon RDS para MySQL está configurado para copiar etiquetas automáticamente en las instantáneas del clúster de base de datos cuando estas se crean. El control falla si el parámetro `CopyTagsToSnapshot` está configurado en `false` para el clúster de bases de datos de RDS para MySQL.

Copiar etiquetas en las instantáneas de bases de datos ayuda a mantener un seguimiento adecuado de recursos, una gobernanza correcta y una asignación de costos apropiada entre los recursos de copia de seguridad. Esto permite una identificación coherente de recursos, control de acceso y supervisión de cumplimiento tanto en las bases de datos activas como en sus instantáneas. Las instantáneas etiquetadas correctamente mejoran las operaciones de seguridad al garantizar que los recursos de copia de seguridad hereden los mismos metadatos que sus bases de datos de origen.

Corrección

Para obtener información sobre cómo configurar un clúster de bases de datos de Amazon RDS para MySQL para copiar etiquetas automáticamente en las instantáneas de bases de datos, consulte Etiquetado de recursos de Amazon RDS en la Guía del usuario de Amazon Relational Database Service.

[RDS.50] Los clústeres de bases de datos de RDS deben tener un período de retención de copias de seguridad suficiente

Categoría: Recuperación > Resiliencia > Respaldos habilitados

Gravedad: media

Tipo de recurso: `AWS::RDS::DBCluster`

Regla de AWS Config : rds-cluster-backup-retention-check

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub CSPM
`minimumBackupRetentionPeriod`	El período mínimo de retención de copias de seguridad en días para que el control lo compruebe	Entero	De 7 a 35	7

Este control comprueba si un clúster de base de datos de RDS tiene un período mínimo de retención de copias de seguridad. El control falla si el período de retención de la copia de seguridad es inferior al valor del parámetro especificado. A menos que proporcione un valor de parámetro personalizado, Security Hub utiliza un valor predeterminado de 7 días.

Este control comprueba si un clúster de base de datos de RDS tiene un período mínimo de retención de copias de seguridad. El control falla si el período de retención de la copia de seguridad es inferior al valor del parámetro especificado. A menos que proporcione un valor de parámetro de cliente, Security Hub utiliza un valor predeterminado de 7 días. Este control se aplica a todos los tipos de clústeres de bases de datos de RDS, incluidos los clústeres de bases de datos Aurora, los clústeres de DocumentDB, los clústeres de NeptuneDB, etc.

Corrección

Para configurar el período de retención de las copias de seguridad de un clúster de base de datos de RDS, modifique la configuración del clúster y establezca el período de retención de las copias de seguridad en al menos 7 días (o el valor especificado en el parámetro de control). Para obtener

instrucciones detalladas, consulte el período de retención de las copias de seguridad en la Guía del usuario de Amazon Relational Database Service. Para los clústeres de bases de datos Aurora, consulte la descripción general de la copia de seguridad y la restauración de un clúster de bases de datos Aurora en la Guía del usuario de Amazon Aurora para Aurora. Para otros tipos de clústeres de bases de datos (por ejemplo, clústeres de DocumentDB), consulte la guía del usuario del servicio correspondiente para saber cómo actualizar el período de retención de copias de seguridad del clúster.

[RDS.51] Los clústeres globales de RDS deben ejecutarse en una versión compatible de Aurora MySQL

Categoría: Identificar > Administración de vulnerabilidades, parches y versiones

Gravedad: alta

Tipo de recurso: `AWS::RDS::GlobalCluster`

Regla de AWS Config : rds-global-cluster-aurora-mysql-supported-version

Tipo de horario: provocado por un cambio

Parámetros:

- `minSupportedEngineVersion`: `8.0.mysql_aurora.3.08.0` (no personalizable)
- `longTermSupportVersion`: `8.0.mysql_aurora.3.04.0, 8.0.mysql_aurora.3.04.1, 8.0.mysql_aurora.3.04.2, 8.0.mysql_aurora.3.04.3` (no personalizable)

Este control comprueba si un clúster global de Amazon Aurora MySQL se ejecuta en una versión de motor mínima admitida. El control falla si la versión del motor de clústeres globales de Aurora MySQL está por debajo de la versión mínima admitida especificada y no aparece en el parámetro de versión de soporte a largo plazo.

La ejecución de las bases de datos globales de Aurora MySQL en las versiones de motor compatibles ayuda a garantizar el acceso a los parches de seguridad, las correcciones de errores y las mejoras de rendimiento más recientes. Las versiones secundarias de Aurora MySQL tienen fechas de finalización del soporte estándar definidas, después de las cuales ya no reciben los parches críticos. La ejecución de una versión no compatible puede exponer su base de datos global a vulnerabilidades de seguridad y puede generar cargos por el soporte extendido de Amazon RDS. Dado que Aurora MySQL sigue un ciclo de vida de soporte no contiguo, en el que las versiones

con soporte a largo plazo (LTS) siguen siendo compatibles durante más tiempo que las versiones posteriores que no son LTS, este control también comprueba si las versiones LTS siguen siendo compatibles con el estándar. Para obtener más información, consulte los calendarios de lanzamiento de Amazon Aurora MySQL en las notas de lanzamiento de Amazon Aurora para Aurora MySQL.

Corrección

Para obtener información sobre la actualización de una base de datos global de Aurora MySQL a una versión de motor compatible, consulte Actualización de una base de datos global de Amazon Aurora y Actualización de Aurora MySQL modificando la versión del motor en la Guía del usuario de Amazon Aurora.

Controles CSPM de Security Hub para Amazon Redshift

Estos AWS Security Hub CSPM controles evalúan el servicio y los recursos de Amazon Redshift. Es posible que los controles no estén disponibles en todosRegiones de AWS. Para obtener más información, consulte Disponibilidad de los controles por región.

[Redshift.1] Los clústeres de Amazon Redshift deberían prohibir el acceso público

Requisitos relacionados: NIST.800-53.r5 AC-21 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), (21) NIST.800-53.r5 AC-4,, NIST.800-53.r5 AC-4 (11) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (21), (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), PCI DSS v3.2. 1/1.2.1, PCI DSS v3.2. 1/1.3.1, PCI DSS v3.2. 1/1.3.2, PCI DSS v3.2. 1/1.3.4, PCI DSS v3.2. 1/1.3.6, PCI DSS v4.0. 1/1.4.4

Categoría: Proteger > Configuración de red segura > Recursos no accesibles públicamente

Gravedad: crítica

Tipo de recurso: `AWS::Redshift::Cluster`

Regla de AWS Config: redshift-cluster-public-access-check

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si los clústeres de Amazon Redshift son de acceso público. Evalúa el campo `PubliclyAccessible` del elemento de configuración del clúster.

El atributo de la configuración del clúster de Amazon Redshift `PubliclyAccessible` indica si el clúster es de acceso público. Cuando el clúster se configura con el valor `PubliclyAccessible` establecido en`true`, se trata de una Internet-facing instancia que tiene un nombre DNS que se puede resolver públicamente y que se resuelve en una dirección IP pública.

Cuando el clúster no es accesible públicamente, se trata de una instancia interna con un nombre DNS que se resuelve en una dirección IP privada. A menos que desee que su clúster sea de acceso público, el clúster no debe configurarse con el valor `PubliclyAccessible` establecido como `true`.

Corrección

Para actualizar un clúster de Amazon Redshift para inhabilitar el acceso público, consulte Modificación de un clúster en la Guía de administración de Amazon Redshift. Establezca Accesible públicamente en No.

[Redshift.2] Las conexiones a los clústeres de Amazon Redshift deben cifrarse en tránsito

Requisitos relacionados: NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (3), NIST.800-53.r5 SC-7 (4), (1) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 NIST.800-53.r5 SC-8 (2), PCI DSS v4.0. 1/42.2.1

Categoría: Proteger > Protección de datos > Cifrado de datos en tránsito

Gravedad: media

Tipo de recurso: `AWS::Redshift::Cluster` `AWS::Redshift::ClusterParameterGroup`

Regla de AWS Config: redshift-require-tls-ssl

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si las conexiones a los clústeres de Amazon Redshift son necesarias para utilizar el cifrado en tránsito. La comprobación no se realiza correctamente si el parámetro de clúster de Amazon Redshift `require_SSL` no se ha establecido como `True`.

Se puede utilizar TLS para ayudar a evitar posibles ataques de «persona en medio» o similares para espiar o manipular el tráfico de red. Solo se deben permitir las conexiones cifradas a través de TLS. El cifrado de los datos en tránsito puede afectar al rendimiento. Debe probar su aplicación con esta característica para comprender el perfil de rendimiento y el impacto del TLS.

Corrección

Para actualizar un grupo de parámetros de Amazon Redshift para que requiera el cifrado, consulte Modificación de un grupo de parámetros en la Guía de administración de Amazon Redshift. Establecer `require_ssl` como True.

[Redshift.3] Los clústeres de Amazon Redshift deben tener habilitadas las instantáneas automáticas

Requisitos relacionados: NIST.800-53.r5 CP-10 NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6 (1), NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 SC-5 (2) NIST.800-53.r5 CP-9, (10), NIST.800-53.r5 SC-7 NIST.800-53.r5 SI-13 (5)

Categoría: Recuperación > Resiliencia > Respaldos habilitados

Gravedad: media

Tipo de recurso: `AWS::Redshift::Cluster`

Regla de AWS Config: redshift-backup-enabled

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub	
`MinRetentionPeriod`	Periodo mínimo de retención de instantáneas en días	Entero	De 7 a 35	7	

Este control comprueba si un clúster de Amazon Redshift tiene habilitadas las instantáneas automatizadas y si el periodo de retención es superior o igual al periodo especificado. Se produce un error en el control si las instantáneas automatizadas no están habilitadas para el clúster o si el periodo de retención es inferior al periodo especificado. A menos que proporciones un valor de

parámetro personalizado para el período de retención de las instantáneas, el CSPM de Security Hub utiliza un valor predeterminado de 7 días.

Las copias de seguridad le ayudan a recuperarse más rápidamente de un incidente de seguridad. Refuerzan la resiliencia de sus sistemas. Amazon Redshift toma instantáneas periódicas de forma predeterminada. Este control comprueba si las instantáneas automáticas están habilitadas y conservadas durante al menos siete días. Para obtener más información sobre las instantáneas automatizadas de Amazon Redshift, consulte Instantáneas automatizadas en la Guía de administración de Amazon Redshift.

Corrección

Para actualizar el período de retención de instantáneas de un clúster de Amazon Redshift, consulte Modificación de un clúster en la Guía de administración de Amazon Redshift. Para Copia de seguridad, establezca la Retención de instantáneas en un valor de 7 o superior.

[Redshift.4] Los clústeres de Amazon Redshift deben tener habilitado el registro de auditoría

Requisitos relacionados: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9),, NIST.800-53.r5 AU-10 NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-6 (3) NIST.800-53.r5 AU-2 NIST.800-53.r5 AU-3, (4), NIST.800-53.r5 AU-6 (9) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), (8), NIST.800-53.r5 SI-3 (20), NIST.800-53.r5 SI-4 NIST.800-53.r5 SI-7 (8), PCI DSS v4.0. 1/102.2.1

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: `AWS::Redshift::Cluster`

AWS Configregla: `redshift-cluster-audit-logging-enabled` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un clúster de Amazon Redshift tiene activado el registro de auditoría.

El registro de auditoría de Amazon Redshift proporciona información adicional acerca de las conexiones y las actividades de los usuarios en su clúster. Estos datos se pueden almacenar y proteger en Amazon S3 y pueden ser útiles en las auditorías e investigaciones de seguridad. Para obtener más información, consulte Registro de auditoría de base de datos en la Guía de administración de Amazon Redshift.

Corrección

Para configurar el registro de auditoría para un clúster de Amazon Redshift, consulte Configuración de la auditoría mediante la consola en la Guía de administración de Amazon Redshift.

[Redshift.6] Amazon Redshift debería tener habilitadas las actualizaciones automáticas a las versiones principales

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2 NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2) NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2 (2), NIST.800-53.r5 SI-2 (4), NIST.800-53.r5 SI-2 (5)

Categoría: Identificar > Administración de vulnerabilidades, parches y versiones

Gravedad: media

Tipo de recurso: `AWS::Redshift::Cluster`

Regla de AWS Config: redshift-cluster-maintenancesettings-check

Tipo de horario: provocado por un cambio

Parámetros:

- `allowVersionUpgrade = true` (no personalizable)

Este control comprueba si las actualizaciones automáticas de las versiones principales están habilitadas para el clúster de Amazon Redshift.

La activación de las actualizaciones automáticas de las versiones principales garantiza que las últimas actualizaciones de las versiones principales de los clústeres de Amazon Redshift se instalen durante el período de mantenimiento. Estas actualizaciones pueden incluir parches de seguridad y correcciones de errores. Mantenerse al día con la instalación de los parches es un paso importante para proteger los sistemas.

Corrección

Para solucionar este problemaAWS CLI, utilice el comando Amazon `modify-cluster` Redshift y `--allow-version-upgrade` defina el atributo. *`clustername`*es el nombre de su clúster de Amazon Redshift.

```
aws redshift modify-cluster --cluster-identifier clustername --allow-version-upgrade
```

[Redshift.7] Los clústeres de Redshift deberían utilizar un enrutamiento de VPC mejorado

Requisitos relacionados: NIST.800-53.r5 AC-4 NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9)

Categoría: Proteger > Configuración de red segura > Acceso privado a la API

Gravedad: media

Tipo de recurso: `AWS::Redshift::Cluster`

Regla de AWS Config: redshift-enhanced-vpc-routing-enabled

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un clúster de Amazon Redshift ha habilitado `EnhancedVpcRouting`.

El Enhanced VPC Routing fuerza a todo `COPY` y el tráfico de `UNLOAD` entre el clúster y los repositorios de datos para que pase a través de su VPC. A continuación, puede utilizar las funciones de la VPC, como los grupos de seguridad y las listas de control de acceso a la red, para proteger el tráfico de la red. También puede usar Registros de flujo de VPC para monitorear el tráfico de red.

Corrección

Para obtener instrucciones de corrección detalladas, consulte Habilitar el enrutamiento de VPC mejorado en la Guía de administración de Amazon Redshift.

[Redshift.8] Los clústeres de Amazon Redshift no deben usar el nombre de usuario de administrador predeterminado

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Categoría: Identificar > Configuración de recursos

Gravedad: media

Tipo de recurso: `AWS::Redshift::Cluster`

Regla de AWS Config: redshift-default-admin-check

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un clúster de Amazon Redshift ha cambiado el nombre de usuario de administrador con respecto a su valor predeterminado. Este control fallará si el nombre de usuario de administrador de un clúster de Redshift se ha establecido como `awsuser`.

Al crear un clúster de Redshift, debe cambiar el nombre de usuario de administrador predeterminado por un valor único. Los nombres de usuario predeterminados son de dominio público y deben cambiarse al configurarlos. Cambiar los nombres de usuario predeterminados reduce el riesgo de accesos no deseados.

Corrección

No se puede cambiar el nombre de usuario de administración de su clúster de Amazon Redshift después de crearlo. Para crear un clúster nuevo con un nombre de usuario que no sea el predeterminado, consulte Paso 1: crear un clúster de Amazon Redshift de muestra en la Guía de introducción a Amazon Redshift.

[Redshift.10] Los clústeres de Redshift deben cifrarse en reposo

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SI-7 (6)

Categoría: Proteger > Protección de datos > Cifrado de datos en reposo

Gravedad: media

Tipo de recurso: `AWS::Redshift::Cluster`

Regla de AWS Config: redshift-cluster-kms-enabled

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si los clústeres de Amazon Redshift están cifrados en reposo. El control falla si un clúster de Redshift no está cifrado en reposo o si la clave de cifrado es diferente de la clave proporcionada en el parámetro de la regla.

En Amazon Redshift, puede activar el cifrado de la base de datos de los clústeres para proteger los datos en reposo. Cuando activa el cifrado para un clúster, se cifran los bloques de datos y metadatos

del sistema para el clúster y sus instantáneas. El cifrado de los datos en reposo es una práctica recomendada, ya que añade una capa de administración del acceso a los datos. El cifrado de los clústeres de Redshift en reposo reduce el riesgo de que un usuario no autorizado pueda acceder a los datos almacenados en el disco.

Corrección

Para modificar un clúster de Redshift para que utilice el cifrado de KMS, consulte Cambiar el cifrado de clústeres en la Guía de administración de Amazon Redshift.

[Redshift.11] Los clústeres de Redshift deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::Redshift::Cluster`

AWS Configregla: `tagged-redshift-cluster` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	`No default value`

Este control comprueba si un clúster de Amazon Redshift tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza un error si el clúster no tiene ninguna

clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si el clúster no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte Etiquetar sus AWS recursos en el. Referencia general de AWS

Corrección

Para agregar etiquetas a un clúster de Redshift, consulte Etiquetado de recursos en Amazon Redshift en la Guía de administración de Amazon Redshift.

[Redshift.12] Las suscripciones a notificaciones de eventos de Redshift deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::Redshift::EventSubscription`

AWS Configregla: `tagged-redshift-eventsubscription` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	`No default value`

Este control comprueba si una instantánea del clúster de Amazon Redshift tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza un error si la instantánea del clúster no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si la instantánea de clúster no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte Etiquetar sus AWS recursos en el. Referencia general de AWS

Corrección

Para agregar etiquetas a una suscripción a notificaciones de eventos de Redshift, consulte Etiquetado de recursos en Amazon Redshift en la Guía de administración de Amazon Redshift.

[Redshift.13] Las instantáneas del clúster de Redshift deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::Redshift::ClusterSnapshot`

AWS Configregla: `tagged-redshift-clustersnapshot` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	`No default value`

Este control comprueba si una instantánea del clúster de Amazon Redshift tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza un error si la instantánea del clúster no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si la instantánea de clúster no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte Etiquetar sus AWS recursos en el. Referencia general de AWS

Corrección

Para agregar etiquetas a la instantánea del clúster de Redshift, consulte Etiquetado de recursos en Amazon Redshift en la Guía de administración de Amazon Redshift.

[Redshift.14] Los grupos de subredes del clúster de Redshift deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::Redshift::ClusterSubnetGroup`

AWS Configregla: `tagged-redshift-clustersubnetgroup` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	`No default value`

Este control comprueba si un grupo de subredes del clúster de Amazon Redshift tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza un error si el grupo de subredes del clúster no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si el grupo de subredes del clúster no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan

operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte Etiquetar sus AWS recursos en el. Referencia general de AWS

Corrección

Para agregar etiquetas a un grupo de subredes del clúster de Redshift, consulte Etiquetado de recursos en Amazon Redshift en la Guía de administración de Amazon Redshift.

[Redshift.15] Los grupos de seguridad de Redshift deberían permitir la entrada en el puerto del clúster solo desde orígenes restringidos

Requisitos relacionados: PCI DSS v4.0. 1/13.3.1

Categoría: Proteger > Configuración de red segura > Configuración de grupos de seguridad

Gravedad: alta

Tipo de recurso: `AWS::Redshift::Cluster`

Regla de AWS Config: redshift-unrestricted-port-access

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si un grupo de seguridad asociado a un clúster de Amazon Redshift tiene reglas de entrada que permiten el acceso al puerto del clúster desde Internet (0.0.0). 0/0 o: :/0). El control lanza un error si las reglas de entrada del grupo de seguridad permiten el acceso al puerto del clúster desde Internet.

Permitir el acceso al puerto del clúster de Redshift (dirección IP con el sufijo /0) sin restricciones puede provocar un acceso no autorizado o incidentes de seguridad. Recomendamos aplicar el

principio de acceso con privilegio mínimo al crear grupos de seguridad y configurar las reglas de entrada.

Corrección

Para restringir la entrada en el puerto del clúster de Redshift a orígenes restringidos, consulte Trabajar con reglas del grupo de seguridad en la Guía del usuario de Amazon VPC. Actualice las reglas en las que el rango de puertos coincida con el puerto del clúster de Redshift y el rango de puertos IP sea 0.0.0. 0/0.

[Redshift.16] Los grupos de subredes de clústeres de Redshift deben tener subredes de varias zonas de disponibilidad

Categoría: Recuperación > Resiliencia > Alta disponibilidad

Gravedad: media

Tipo de recurso: `AWS::Redshift::ClusterSubnetGroup`

Regla de AWS Config: redshift-cluster-subnet-group-multi-az

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control verifica si un grupo de subredes de un clúster de Amazon Redshift tiene subredes de más de una zona de disponibilidad (AZ). El control falla si el grupo de subredes del clúster no tiene subredes de al menos dos zonas de disponibilidad diferentes.

Configurar subredes en varias zonas de disponibilidad ayuda a garantizar que el almacén de datos de Redshift pueda continuar en funcionamiento incluso cuando ocurren eventos de falla.

Corrección

Para modificar un grupo de subredes de un clúster de Redshift para abarcar varias zonas de disponibilidad, consulte la Modificación de un grupo de subredes de clúster en la Guía de administración de Amazon Redshift.

[Redshift.17] Los grupos de parámetros del clúster de Redshift deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::Redshift::ClusterParameterGroup`

Regla de AWS Config: redshift-cluster-parameter-group-tagged

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredKeyTags`	Una lista de claves de etiqueta que no son del sistema y que se deben asignar a un recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control verifica si un grupo de parámetros de clúster de Amazon Redshift tiene las claves de etiquetas especificadas por el parámetro `requiredKeyTags`. El control falla si el grupo de parámetros no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas por el parámetro `requiredKeyTags`. Si no especifica valores para el parámetro `requiredKeyTags`, el control verifica únicamente la existencia de una clave de etiqueta y falla si el grupo de parámetros no tiene ninguna clave de etiqueta. El control ignora las etiquetas del sistema, que se aplican automáticamente y tienen el prefijo `aws:`.

Una etiqueta es una etiqueta que se crea y se asigna a un AWS recurso. Cada etiqueta consta de una clave de etiqueta necesaria y un valor de etiqueta opcional. Utilice etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. También pueden ayudar a identificar, organizar, buscar y filtrar recursos. También pueden ayudar a rastrear propietarios de recursos para acciones y notificaciones. También puede usar etiquetas para implementar control de acceso basado en atributos (ABAC) como estrategia de autorización. Para obtener más información sobre estrategias ABAC, consulte Definición de permisos basados en atributos con autorización ABAC en la Guía del usuario de IAM. Para obtener más información sobre las etiquetas, consulte los AWSrecursos de etiquetado y la Guía del usuario del editor de etiquetas.

> **Note**
>
> No almacene información de identificación personal (PII) ni otra información confidencial en las etiquetas. Se puede acceder a las etiquetas desde muchos Servicios de AWS sitios. No están destinadas a usarse para datos privados o información confidencial.

Corrección

Para obtener información sobre cómo agregar etiquetas a un grupo de parámetros de clúster de Amazon Redshift, consulte la Etiquetado de recursos en Amazon Redshift en la Guía de administración de Amazon Redshift.

[Redshift.18] Los clústeres de Redshift deberían tener Multi-AZ las implementaciones habilitadas

Categoría: Recuperación > Resiliencia > Alta disponibilidad

Gravedad: media

Tipo de recurso: `AWS::Redshift::Cluster`

Regla de AWS Config: redshift-cluster-multi-az-enabled

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si están habilitadas varias implementaciones de Availability Zones (Multi-AZ) para un clúster de Amazon Redshift. El control falla si Multi-AZ las implementaciones no están habilitadas para el clúster de Amazon Redshift.

Amazon Redshift admite múltiples implementaciones de zonas de disponibilidad (Multi-AZ) para clústeres aprovisionados. Si Multi-AZ las implementaciones están habilitadas para un clúster, un almacén de datos de Amazon Redshift puede seguir funcionando en caso de fallo si se produce un suceso inesperado en una zona de disponibilidad (AZ). Una Multi-AZ implementación implementa recursos de cómputo en más de una zona de disponibilidad y se puede acceder a estos recursos de cómputo a través de un único punto final. En caso de una falla completa en una zona de disponibilidad, los recursos de computación restantes en otra zona estarán disponibles para continuar el procesamiento de las cargas de trabajo. Puede convertir un almacén de Single-AZ datos existente en un almacén de Multi-AZ datos. Luego se aprovisionan recursos de computación adicionales en una segunda zona de disponibilidad.

Corrección

Para obtener información sobre la configuración de Multi-AZ las implementaciones de un clúster de Amazon Redshift, consulte Convertir Single-AZ un almacén de datos en un almacén de datos en la Guía de administración de Amazon Redshift. Multi-AZ

Controles CSPM de Security Hub para Amazon Redshift Serverless

Estos AWS Security Hub CSPM controles evalúan el servicio y los recursos de Amazon Redshift Serverless. Es posible que los controles no estén disponibles en todos. Regiones de AWS Para obtener más información, consulte Disponibilidad de los controles por región.

[RedshiftServerless.1] Los grupos de trabajo sin servidor de Amazon Redshift deberían utilizar un enrutamiento de VPC mejorado

Categoría: Proteger > Configuración de red segura > Recursos dentro de VPC

Gravedad: alta

Tipo de recurso: `AWS::RedshiftServerless::Workgroup`

Regla de AWS Config: redshift-serverless-workgroup-routes-within-vpc

Tipo de programa: Periódico

Parámetros: ninguno

Este control verifica si el enrutamiento de VPC mejorado está habilitado para un grupo de trabajo de Amazon Redshift sin servidor. El control falla si el enrutamiento de VPC mejorado está desactivado para el grupo de trabajo.

Si el enrutamiento de VPC mejorado está deshabilitado para un grupo de trabajo sin servidor de Amazon Redshift, Amazon Redshift direcciona el tráfico a través de Internet, incluido el tráfico a otros servicios de la red. AWS Si habilita el enrutamiento de VPC mejorado para un grupo de trabajo, Amazon Redshift fuerza todo el tráfico `COPY` y `UNLOAD` entre el clúster y los repositorios de datos a pasar por la nube virtual privada (VPC), basada en el servicio Amazon VPC. Con el enrutamiento de VPC mejorado, puede usar características estándar de VPC para controlar el flujo de datos entre el clúster de Amazon Redshift y otros recursos. Esto incluye características como grupos de seguridad de VPC y políticas de puntos de conexión, listas de control de acceso de la red (ACL) y servidores del sistema de nombres de dominio (DNS). También puede usar los registros de flujo de VPC para supervisar el tráfico `COPY` y `UNLOAD`.

Corrección

Para obtener información sobre el enrutamiento de VPC mejorado y sobre cómo habilitarlo para un grupo de trabajo, consulte Control del tráfico de red con el enrutamiento de VPC mejorado de Redshift en la Guía de administración de Amazon Redshift.

[RedshiftServerless.2] Las conexiones a los grupos de trabajo sin servidor de Redshift deberían ser obligatorias para usar SSL

Categoría: Proteger > Protección de datos > Cifrado de datos en tránsito

Gravedad: media

Tipo de recurso: `AWS::RedshiftServerless::Workgroup`

Regla de AWS Config: redshift-serverless-workgroup-encrypted-in-transit

Tipo de programa: Periódico

Parámetros: ninguno

Este control verifica si las conexiones a un grupo de trabajo de Amazon Redshift sin servidor deben requerir cifrar los datos en tránsito. El control falla si el parámetro de configuración `require_ssl` del grupo de trabajo está configurado en `false`.

Un grupo de trabajo de Amazon Redshift sin servidor es un conjunto de recursos de computación que agrupa recursos de computación como RPU, grupos de subredes de VPC y grupos de seguridad. Las propiedades de un grupo de trabajo incluyen configuraciones de red y seguridad. Estas configuraciones especifican si las conexiones a un grupo de trabajo deben requerir el uso de SSL para cifrar los datos en tránsito.

Corrección

Para obtener información sobre cómo actualizar las configuraciones de un grupo de trabajo de Amazon Redshift sin servidor para requerir conexiones SSL, consulte Conexión a Amazon Redshift sin servidor en la Guía de administración de Amazon Redshift.

[RedshiftServerless.3] Los grupos de trabajo sin servidor de Redshift deberían prohibir el acceso público

Categoría: Proteger > Configuración de red segura > Recursos no accesibles públicamente

Gravedad: alta

Tipo de recurso: `AWS::RedshiftServerless::Workgroup`

Regla de AWS Config: redshift-serverless-workgroup-no-public-access

Tipo de programa: Periódico

Parámetros: ninguno

Este control verifica si el acceso público está desactivado para un grupo de trabajo de Amazon Redshift sin servidor. Evalúa la propiedad `publiclyAccessible` de un grupo de trabajo de Redshift sin servidor. El control falla si el acceso público está habilitado (`true`) para el grupo de trabajo.

La configuración de acceso público (`publiclyAccessible`) de un grupo de trabajo de Amazon Redshift sin servidor especifica si se puede acceder al grupo de trabajo desde una red pública. Si el acceso público está habilitado (`true`) para un grupo de trabajo, Amazon Redshift crea una dirección IP elástica que hace que el grupo de trabajo sea accesible públicamente desde fuera de la VPC. Si no desea que un grupo de trabajo sea accesible públicamente, desactive el acceso público para ese grupo de trabajo.

Corrección

Para obtener información sobre cómo cambiar la configuración de acceso público de un grupo de trabajo de Amazon Redshift sin servidor, consulte Visualización de las propiedades de un grupo de trabajo en la Guía de administración de Amazon Redshift.

[RedshiftServerless.4] Los espacios de nombres de Redshift Serverless deben cifrarse y administrarse por el clienteAWS KMS keys

Requisitos relacionados: NIST.800-53.r5 AU-9 NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SC-12 (2),, (1) NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (6) NIST.800-53.r5 SI-7

Categoría: Proteger > Protección de datos > Cifrado de datos en reposo

Gravedad: media

Tipo de recurso: `AWS::RedshiftServerless::Namespace`

Regla de AWS Config: redshift-serverless-namespace-cmk-encryption

Tipo de programa: Periódico

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`kmsKeyArns`	Una lista de los nombres de recursos de Amazon (ARN) AWS KMS keys para incluirlos en la evaluación. El control genera un resultado `FAILED` si un espacio de nombres de Redshift sin servidor no está cifrado con una clave de KMS de la lista.	StringList (máximo de 3 elementos)	Entre 1 y 3 ARN de claves de KMS existentes. Por ejemplo: `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab` .	Sin valor predeterminado

Este control verifica si un espacio de nombres de Amazon Redshift sin servidor está cifrado en reposo con una AWS KMS key administrada por el cliente. El control falla si el espacio de nombres de Redshift sin servidor no está cifrado con una clave de KMS administrada por el cliente. Puede especificar opcionalmente una lista de claves de KMS para que el control las incluya en la evaluación.

En Amazon Redshift sin servidor, un espacio de nombres define un contenedor lógico para objetos de base de datos. Este control comprueba periódicamente si la configuración de cifrado de un espacio de nombres especifica una clave de KMS gestionada por el clienteAWS KMS key, en lugar

de una AWS gestionada, para el cifrado de los datos del espacio de nombres. Con una clave de KMS administrada por el cliente, ejerce control pleno sobre la clave. Esto incluye definir y mantener la política de claves, administrar concesiones, rotar el material criptográfico, asignar etiquetas, crear alias y habilitar y desactivar la clave.

Corrección

Para obtener información sobre cómo actualizar la configuración de cifrado de un espacio de nombres de Amazon Redshift Serverless y especificar un espacio de nombres gestionado por el clienteAWS KMS key, consulte Cambiar el espacio de nombres de un espacio de nombres en la AWS KMS key Guía de administración de Amazon Redshift.

[RedshiftServerless.5] Los espacios de nombres Redshift Serverless no deben usar el nombre de usuario de administrador predeterminado

Categoría: Identificar > Configuración de recursos

Gravedad: media

Tipo de recurso: `AWS::RedshiftServerless::Namespace`

Regla de AWS Config: redshift-serverless-default-admin-check

Tipo de programa: Periódico

Parámetros: ninguno

Este control verifica si el nombre de usuario de administrador de un espacio de nombres de Amazon Redshift sin servidor es el nombre de administrador predeterminado, `admin`. El control falla si el nombre de usuario de administrador del espacio de nombres de Redshift sin servidor es `admin`.

Al crear un espacio de nombres de Amazon Redshift sin servidor, debe especificar un nombre de usuario de administrador personalizado para el espacio de nombres. El nombre de usuario de administrador predeterminado es de conocimiento público. Al especificar un nombre de usuario de administrador personalizado, puede, por ejemplo, ayudar a mitigar el riesgo o la efectividad de ataques de fuerza bruta contra el espacio de nombres.

Corrección

Puede cambiar el nombre de usuario de administrador de un espacio de nombres de Amazon Redshift sin servidor mediante la consola o la API de Amazon Redshift sin servidor. Para cambiarlo

mediante la consola, seleccione la configuración del espacio de nombres y luego seleccione Editar credenciales de administrador en el menú Acciones. Para cambiarlo mediante programación, utilice la UpdateNamespaceoperación o, si está utilizando la, ejecute el comando update-namespace. AWS CLI Si cambia el nombre de usuario de administrador, también debe cambiar la contraseña de administrador al mismo tiempo.

[RedshiftServerless.6] Los espacios de nombres Redshift Serverless deberían exportar los registros a los registros CloudWatch

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: `AWS::RedshiftServerless::Namespace`

Regla de AWS Config: redshift-serverless-publish-logs-to-cloudwatch

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si un espacio de nombres Amazon Redshift Serverless está configurado para exportar los registros de conexión y de usuario a Amazon Logs. CloudWatch El control falla si el espacio de nombres Redshift Serverless no está configurado para exportar los registros a Logs. CloudWatch

Si configura Amazon Redshift Serverless para que exporte los datos del registro de conexión (`connectionlog`) y del registro de usuario (`userlog`) a un grupo de CloudWatch registros de Amazon Logs, podrá recopilar y almacenar sus registros de registro en un almacenamiento duradero que permita realizar revisiones y auditorías de seguridad, acceso y disponibilidad. Con CloudWatch Logs, también puede realizar análisis de los datos de registro en tiempo real y utilizarlos CloudWatch para crear alarmas y revisar métricas.

Corrección

Para exportar los datos de registro de un espacio de nombres Amazon Redshift Serverless a CloudWatch Amazon Logs, se deben seleccionar los registros correspondientes para su exportación en los ajustes de configuración de los registros de auditoría del espacio de nombres. Para obtener información sobre cómo actualizar estas configuraciones, consulte Edición de la seguridad y el cifrado en la Guía de administración de Amazon Redshift.

Controles CSPM de Security Hub para Route 53

Estos AWS Security Hub CSPM controles evalúan el servicio y los recursos de Amazon Route 53.

Es posible que estos controles no estén disponibles en todosRegiones de AWS. Para obtener más información, consulte Disponibilidad de los controles por región.

[Route53.1] Los controles de salud de Route 53 deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::Route53::HealthCheck`

AWS Configregla: `tagged-route53-healthcheck` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control verifica si una comprobación de estado de Amazon Route 53 tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control falla si la comprobación de estado no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control

solo comprueba la existencia de una clave de etiqueta y falla si la comprobación de estado no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte Etiquetar sus AWS recursos en el. Referencia general de AWS

Corrección

Para agregar etiquetas a una comprobación de estado de Route 53, consulte Nombrar y etiquetar las comprobaciones de estado en la Guía para desarrolladores de Amazon Route 53.

[Route53.2] Las zonas alojadas públicas de Route 53 deberían registrar las consultas de DNS

Requisitos relacionados: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9),, NIST.800-53.r5 AU-10 NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-6 (3) NIST.800-53.r5 AU-2 NIST.800-53.r5 AU-3, (4), NIST.800-53.r5 AU-6 (9) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8), PCI DSS v4.0. 1/104.4.2

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: `AWS::Route53::HostedZone`

Regla de AWS Config: `route53-query-logging-enabled`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si el registro de consultas de DNS está habilitado en una zona alojada pública de Amazon Route 53. El control falla si el registro de consultas de DNS no está habilitado en una zona alojada pública de Route 53.

Al registrar las consultas de DNS para una zona alojada de Route 53, se abordan los requisitos de seguridad y conformidad del DNS y se garantiza la visibilidad. Los registros incluyen información como el dominio o subdominio que se ha consultado, la fecha y la hora de la consulta, el tipo de registro de DNS (por ejemplo, A o AAAA) y el código de respuesta de DNS (por ejemplo, `NoError` o `ServFail`). Cuando el registro de consultas de DNS está habilitado, Route 53 publica los archivos de registro en Amazon CloudWatch Logs.

Corrección

Para registrar las consultas de DNS para las zonas alojadas públicas de Route 53, consulte Configuración del registro de consultas de DNS en la Guía para desarrolladores de Amazon Route 53.

Controles de CSPM de Security Hub para Amazon S3

Estos AWS Security Hub CSPM controles evalúan el servicio y los recursos de Amazon Simple Storage Service (Amazon S3). Es posible que los controles no estén disponibles en todos los casos Regiones de AWS. Para obtener más información, consulte Disponibilidad de los controles por región.

[S3.1] Los cubos de uso general de S3 deben tener habilitada la configuración de bloqueo del acceso público

Requisitos relacionados: CIS AWS Foundations Benchmark v5.0. 0/21.1.4, CIS AWS Foundations Benchmark v3.0. 0/2.1.4, CIS AWS Foundations Benchmark v1.4. 0/2.1.5, NIST.800-53.r5 AC-21 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), (21) NIST.800-53.r5 AC-4,, NIST.800-53.r5 AC-4 (11) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7

(20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), PCI DSS v3.2. 1/1.2.1, PCI DSS versión 3.2. 1/11.3.1, PCI DSS v3.2. 1/13.3.2, PCI DSS v3.2. 1/13.3.4, PCI DSS v3.2. 1/13.3.6, PCI DSS versión 4.0. 1/14.4.4

Categoría: Proteger - Configuración de red segura

Gravedad: media

Tipo de recurso: `AWS::::Account`

Regla de AWS Config : s3-account-level-public-access-blocks-periodic

Tipo de programa: Periódico

Parámetros:

- `ignorePublicAcls`: `true` (no personalizable)
- `blockPublicPolicy`: `true` (no personalizable)
- `blockPublicAcls`: `true` (no personalizable)
- `restrictPublicBuckets`: `true` (no personalizable)

Este control comprueba si la anterior configuración del bloqueo de acceso público de Amazon S3 está configurada en el nivel de cuenta para un bucket de uso general de S3. El control lanza un error si una o más de las configuraciones del bloqueo de acceso público se han establecido como `false`.

El control falla si alguna de las configuraciones se ha establecido como `false` o si alguna de las configuraciones no está configurada.

El bloque de acceso público de Amazon S3 está diseñado para proporcionar controles a nivel de bucket de S3 completo Cuenta de AWS o individual a fin de garantizar que los objetos nunca tengan acceso público. El acceso público se otorga a grupos y objetos a través de listas de control de acceso (ACL), políticas de bucket o ambas.

A menos que quiera que se pueda acceder públicamente a sus buckets de S3, debe configurar la característica de Bloqueo de acceso público de Amazon S3 de nivel de cuenta.

Para obtener más información, consulte Uso de Bloqueo de acceso público de Amazon S3 en la Guía del usuario de Amazon Simple Storage Service.

Corrección

Para habilitar el bloqueo del acceso público de Amazon S3 Cuenta de AWS, consulte Configurar los ajustes de bloqueo del acceso público de su cuenta en la guía del usuario de Amazon Simple Storage Service.

[S3.2] Los cubos de uso general de S3 deberían bloquear el acceso de lectura pública

Requisitos relacionados: PCI DSS v3.2. 1/11.2.1, PCI DSS v3.2. 1/11.3.1, PCI DSS v3.2. 1/13.3.2, PCI DSS v3.2. 1/13.3.6, PCI DSS v3.2. 1/7.2.1, NIST.800-53.r5 AC-21 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 AC-4, (11) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9) NIST.800-53.r5 SC-7

Categoría: Proteger - Configuración de red segura

Gravedad: crítica

Tipo de recurso: `AWS::S3::Bucket`

Regla de AWS Config : s3-bucket-public-read-prohibited

Tipo de programa: periódico y activado por cambios

Parámetros: ninguno

Este control comprueba si un bucket de uso general de Amazon S3 permite el acceso público de lectura. Evalúa la configuración de Block Public Access, la política del bucket y la lista de control de acceso (ACL) del bucket. El control lanza un error si el bucket permite el acceso público de lectura.

> **Note**
>
> Si un bucket de S3 tiene una política de bucket, este control no evalúa condiciones de políticas que utilicen caracteres comodín o variables. Para producir un resultado `PASSED`, las condiciones en la política de bucket deben usar únicamente valores fijos, que son valores que no contienen caracteres comodín ni variables de políticas. Para obtener información sobre variables de políticas, consulte Variables y etiquetas en la Guía del usuario de AWS Identity and Access Management .

Algunos casos de uso probablemente requieran que todos en Internet puedan leer desde su bucket S3. Sin embargo, esas situaciones son poco habituales. Para garantizar la integridad y la seguridad de los datos, el bucket de S3 no debe tener acceso de lectura público.

Corrección

Para bloquear el acceso público de lectura en sus buckets de Amazon S3, consulte Configuración de los ajustes de bloqueo de acceso público para sus buckets de S3 en la Guía del usuario de Amazon Simple Storage Service.

[S3.3] Los cubos S3 de uso general deberían bloquear el acceso público a la escritura

Requisitos relacionados: PCI DSS v3.2. 1/11.2.1, PCI DSS v3.2. 1/11.3.1, PCI DSS v3.2. 1/13.3.2, PCI DSS v3.2. 1/13.3.4, PCI DSS v3.2. 1/13.3.6, PCI DSS v3.2. 1/7.2.1, NIST.800-53.r5 AC-21 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 AC-4, (11) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9) NIST.800-53.r5 SC-7

Categoría: Proteger - Configuración de red segura

Gravedad: crítica

Tipo de recurso: `AWS::S3::Bucket`

Regla de AWS Config : s3-bucket-public-write-prohibited

Tipo de programa: periódico y activado por cambios

Parámetros: ninguno

Este control comprueba si un bucket de uso general de Amazon S3 permite el acceso público de escritura. Evalúa la configuración de Block Public Access, la política del bucket y la lista de control de acceso (ACL) del bucket. El control lanza un error si el bucket permite el acceso público de escritura.

> **Note**
>
> Si un bucket de S3 tiene una política de bucket, este control no evalúa condiciones de políticas que utilicen caracteres comodín o variables. Para producir un resultado `PASSED`, las condiciones en la política de bucket deben usar únicamente valores fijos, que son valores que no contienen caracteres comodín ni variables de políticas. Para obtener información

sobre variables de políticas, consulte Variables y etiquetas en la Guía del usuario de AWS Identity and Access Management .

Algunos casos de uso requieren que todos en Internet puedan escribir en su bucket S3. Sin embargo, esas situaciones son poco habituales. Para garantizar la integridad y la seguridad de los datos, el bucket de S3 no debe tener acceso de escritura público.

Corrección

Para bloquear el acceso público de escritura en sus buckets de Amazon S3, consulte Configuración de los ajustes de bloqueo de acceso público para sus buckets de S3 en la Guía del usuario de Amazon Simple Storage Service.

[S3.5] Los cubos de uso general de S3 deberían requerir que las solicitudes usen TLS

Requisitos relacionados: CIS AWS Foundations Benchmark v5.0. 0/21.1.1, CIS AWS Foundations Benchmark v3.0. 0/2.1.1, CIS AWS Foundations Benchmark v1.4. 0/2.1.2, NIST.800-53.r5 AC-17 (2), (1) NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (3),, NIST.800-53.r5 SC-12 (3) NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23 (3) NIST.800-53.r5 SC-23, (4), NIST.800-53.r5 SC-7 (1) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SI-7 (6), NIST.800-53.r5 SC-8 NIST.800-171.r2 3.13.8, 3.13.15, PCI DSS v3.2 NIST.800-171.r2 . 1/41. PCI DSS versión 4.0. 1/41.2.1

Categoría: Proteger - Administración de acceso seguro

Gravedad: media

Tipo de recurso: `AWS::S3::Bucket`

Regla de AWS Config : s3-bucket-ssl-requests-only

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un bucket de uso general de Amazon S3 tiene una política que exige que las solicitudes usen TLS. El control falla si la política de cubos no exige que las solicitudes usen TLS.

Los buckets S3 deben tener políticas que exijan que todas las solicitudes (`Action: S3:*`) solo acepten la transmisión de datos a través de HTTPS en la política de recursos de S3, indicada mediante la clave de condición `aws:SecureTransport`.

Corrección

Para actualizar una política de bucket de Amazon S3 de manera que deniegue el transporte no seguro, consulte Agregar una política de bucket mediante la consola de Amazon S3 en la Guía del usuario de Amazon Simple Storage Service.

Añada una declaración de política similar a la de la siguiente política. Sustituya `amzn-s3-demo-bucket` por el nombre del bucket que está modificando.

JSON

```
{
    "Id": "ExamplePolicy",
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowSSLRequestsOnly",
            "Action": "s3:*",
            "Effect": "Deny",
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket",
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ],
            "Condition": {
                "Bool": {
                     "aws:SecureTransport": "false"
                }
            },
           "Principal": "*"
        }
    ]
}
```

Para obtener más información, consulta ¿Qué política de bucket de S3 debo usar para cumplir con la AWS Config regla s3-bucket-ssl-requests-only? en el Centro de conocimiento oficial. AWS

[S3.6] Las políticas de bucket de uso general de S3 deberían restringir el acceso a otros Cuentas de AWS

Requisitos relacionados: NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, NIST.800-171.r2 3.13.4

Categoría: Proteger > Gestión del acceso seguro > Se restringen las acciones de operaciones confidenciales de la API

Gravedad: alta

Tipo de recurso: `AWS::S3::Bucket`

Regla de AWS Config: s3-bucket-blacklisted-actions-prohibited

Tipo de horario: provocado por un cambio

Parámetros:

- `blacklistedactionpatterns`: `s3:DeleteBucketPolicy, s3:PutBucketAcl, s3:PutBucketPolicy, s3:PutEncryptionConfiguration, s3:PutObjectAcl` (no personalizable)

Este control comprueba si la política del bucket de uso general de Amazon S3 impide que las entidades principales de otras Cuentas de AWS realicen acciones denegadas en los recursos del bucket de S3. El control lanza un error si la política de buckets permite una o más de las acciones anteriores a una entidad principal en otra Cuenta de AWS.

La implementación del acceso con privilegios mínimos es esencial a la hora de reducir los riesgos de seguridad y el impacto de los errores o intentos malintencionados. Si una política de buckets S3 permite el acceso desde cuentas externas, podría provocar la exfiltración de datos por parte de una amenaza interna o de un atacante.

El parámetro `blacklistedactionpatterns` permite evaluar correctamente la regla para los buckets S3. El parámetro otorga acceso a cuentas externas para los patrones de acción que no están incluidos en la lista de `blacklistedactionpatterns`.

Corrección

Para actualizar una política de bucket de Amazon S3 para eliminar permisos, consulte. Agregar una política de bucket mediante la consola de Amazon S3 en la Guía del usuario de Amazon Simple Storage Service.

En la página Editar política de bucket, en el cuadro de texto de edición de políticas, lleve a cabo una de las siguientes acciones:

- Elimine las declaraciones que otorgan a otras Cuentas de AWS el acceso a las acciones denegadas.
- Elimine las acciones denegadas permitidas de las declaraciones.

[S3.7] Los cubos de uso general de S3 deben utilizar la replicación entre regiones

Requisitos relacionados: PCI DSS v3.2. 1/2.2, NIST.800-53.r5 AU-9 (2), NIST.800-53.r5 CP-6 (1) NIST.800-53.r5 CP-10 NIST.800-53.r5 CP-6, (2), NIST.800-53.r5 CP-6 (2) NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-36 (2), (2), NIST.800-53.r5 SC-5 (5) NIST.800-53.r5 SI-13

Categoría: Proteger - Administración de acceso seguro

Gravedad: baja

Tipo de recurso: `AWS::S3::Bucket`

AWS Config regla: s3-bucket-cross-region-replication-enabled

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si los buckets de uso general de Amazon S3 tienen habilitada la replicación entre regiones. El control lanza un error si el bucket no tiene habilitada la replicación entre regiones.

La replicación es la copia automática y asincrónica de objetos en cubos iguales o diferentes. Regiones de AWS La replicación copia los objetos recientemente creados y las actualizaciones de objetos de un bucket de origen a un bucket o buckets de destino. Las mejores prácticas de AWS recomiendan la replicación de los buckets de origen y destino que son propiedad de la misma Cuenta de AWS. Además de la disponibilidad, debe plantearse otras configuraciones de protección de sistemas.

Este control produce un resultado `FAILED` para un bucket de destino de la replicación si no tiene habilitada la replicación entre regiones. Si hay una razón legítima por la que el bucket de destino no necesita que se habilite la replicación entre regiones, puede suprimir los resultados correspondientes a este bucket.

Corrección

Para habilitar la Cross-Region replicación en un bucket de S3, consulte Configurar la replicación para los cubos de origen y destino que pertenecen a la misma cuenta en la Guía del usuario de

Amazon Simple Storage Service. En el Bucket de origen, seleccione Aplicar a todos los objetos del bucket.

[S3.8] Los cubos de uso general de S3 deben bloquear el acceso público

Requisitos relacionados: CIS AWS Foundations Benchmark v5.0. 0/2.1.4, CIS AWS Foundations Benchmark v3.0.02.1.4, CIS Foundations Benchmark v1.4. AWS 0/2.1.5, NIST.800-53.r5 AC-21 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), (21) NIST.800-53.r5 AC-4,, NIST.800-53.r5 AC-4 (11) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SC-7 PCI DSS v4.0 NIST.800-53.r5 SC-7. 1/1.4.4

Categoría: Proteger - Administración de acceso seguro > Control de acceso

Gravedad: alta

Tipo de recurso: `AWS::S3::Bucket`

Regla de AWS Config : s3-bucket-level-public-access-prohibited

Tipo de horario: provocado por un cambio

Parámetros:

- `excludedPublicBuckets` (no personalizable): una lista separada por comas de nombres de buckets de S3 públicos permitidos conocidos

Este control comprueba si un bucket de uso general de Amazon S3 bloquea el acceso público a nivel de bucket. El control lanza un error si alguna de las siguientes configuraciones se establece como `false`:

- `ignorePublicAcls`
- `blockPublicPolicy`
- `blockPublicAcls`
- `restrictPublicBuckets`

Block Public Access a nivel de bucket de S3 proporciona controles para garantizar que los objetos nunca tengan acceso público. El acceso público se otorga a grupos y objetos a través de listas de control de acceso (ACL), políticas de bucket o ambas.

A menos que quiera que se pueda acceder públicamente a sus buckets de S3, debe configurar la característica de Bloqueo de acceso público de Amazon S3 de nivel de bucket.

Corrección

Para obtener información sobre cómo eliminar el acceso público a nivel de bucket, consulte Bloquear el acceso público a su almacenamiento de Amazon S3 en la Guía del usuario de Amazon S3.

[S3.9] Los cubos de uso general de S3 deben tener habilitado el registro de acceso al servidor

Requisitos relacionados: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9),, NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12 NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-6 (3) NIST.800-53.r5 AU-3, (4), NIST.800-53.r5 AU-6 (9) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (8), NIST.800-53.r5 SI-3 (20), NIST.800-53.r5 SI-4 (8), NIST.800-53.r5 SI-7 NIST.800-171.r2 3.3.8, PCI DSS v4.0. 1/102.1.

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: `AWS::S3::Bucket`

Regla de AWS Config : s3-bucket-logging-enabled

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si el registro de acceso al servidor está habilitado para los buckets de uso general de Amazon S3. El control lanza un error si no está habilitado el registro de acceso al servidor. Cuando activa el registro, Amazon S3 envía los registros de acceso de un bucket de origen a un bucket de destino que usted selecciona. El depósito de destino debe estar en el Región de AWS mismo lugar que el depósito de origen y no debe tener configurado un período de retención predeterminado. El bucket de registro de destino no necesita tener activado el registro de acceso al servidor, por lo que debe suprimir los resultados de este bucket.

El registro de acceso al servidor brinda registros detallados de las solicitudes realizadas a un bucket. Los registros de acceso al servidor pueden ayudar en auditorías de acceso y seguridad. Para obtener más información, consulte Prácticas recomendadas de seguridad para Amazon S3: Habilitar el registro de acceso al servidor de Amazon S3.

Corrección

Para habilitar el registro de acceso al servidor Amazon S3, consulte Habilitar el registro de acceso al servidor Amazon S3 en la Guía del usuario de Amazon S3.

[S3.10] Los cubos de uso general de S3 con el control de versiones habilitado deben tener configuraciones de ciclo de vida

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2) NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: `AWS::S3::Bucket`

Regla de AWS Config : s3-version-lifecycle-policy-check

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un bucket de uso general de Amazon S3 con control de versiones tiene una configuración de ciclo de vida. El control lanza un error si el bucket no tiene una configuración de ciclo de vida.

Recomendamos configurar el ciclo de vida en el bucket de S3 para que pueda definir las acciones que desea que Amazon S3 realice durante la vida útil de un objeto.

> **Tip**
>
> Permitir el control de versiones sin administrar el ciclo de vida puede generar un crecimiento ilimitado del almacenamiento y un aumento de los costos. Cada modificación de un objeto crea una nueva versión que se conserva indefinidamente. Configure las reglas del ciclo de vida de S3 para hacer la transición automática de las versiones no actuales a clases de almacenamiento más baratas o para que caduquen después de un período de retención definido.

Corrección

Para obtener más información sobre la configuración del ciclo de vida en un bucket de Amazon S3, consulte Uso del control de versiones de S3 con el ciclo de vida de S3, Configuración de la configuración del ciclo de vida en un bucket y Administración del ciclo de vida de los objetos en la guía del usuario de Amazon S3.

[S3.11] Los cubos de uso general de S3 deben tener habilitadas las notificaciones de eventos

Requisitos relacionados: NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-3 (8) NIST.800-53.r5 SI-4, NIST.800-53.r5 SI-4 (4), 3.3.8 NIST.800-171.r2

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: `AWS::S3::Bucket`

Regla de AWS Config : s3-event-notifications-enabled

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub CSPM
`eventTypes`	Lista de tipos de eventos de S3 preferidos	EnumList (un máximo de 28 elementos)	`s3:IntelligentTiering`, `s3:LifecycleExpiration:*`, `s3:LifecycleExpiration:Delete`,	Sin valor predeterminado

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub CSPM
			s3:LifecycleExpiration:DeleteMarkerCreated, s3:LifecycleTransition, s3:ObjectAcl:Put, s3:ObjectCreated:*, s3:ObjectCreated:CompleteMultipartUpload, s3:ObjectCreated:Copy, s3:ObjectCreated:Post, s3:ObjectCreated:Put, s3:ObjectRemoved:*, s3:Object	

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub CSPM
			`Removed:Delete, s3:ObjectRemoved:DeleteMarkerCreated, s3:ObjectRestore:*, s3:ObjectRestore:Completed, s3:ObjectRestore:Delete, s3:ObjectRestore:Post, s3:ObjectTagging:*, s3:ObjectTagging:Delete, s3:ObjectTagging:Put, s3:ReducedRedundancyLostObj`	

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub CSPM
			`ect, s3:Replication:*, s3:Replication:OperationFailedReplication, s3:Replication:OperationMissedThreshold, s3:Replication:OperationNotTracked, s3:Replication:OperationReplicatedAfterThreshold, s3:TestEvent`	

Este control comprueba si las notificaciones de eventos de S3 están habilitadas en un bucket de uso general de Amazon S3. El control lanza un error si las notificaciones de eventos de S3 no están habilitadas en el bucket. Si proporciona valores personalizados para el parámetro `eventTypes`, el

control solo se aprueba si las notificaciones de eventos están habilitadas para los tipos de eventos especificados.

Al habilitar las notificaciones de eventos de S3, recibe alertas cuando se producen eventos específicos que afecten sus buckets de S3. Por ejemplo, puede recibir notificaciones sobre la creación, eliminación y restauración de objetos. Estas notificaciones pueden alertar a los equipos pertinentes sobre modificaciones accidentales o intencionales que puedan provocar el acceso no autorizado a los datos.

Corrección

Para obtener información sobre la detección de cambios en los buckets y objetos S3, consulte Notificaciones de eventos de Amazon S3 en la Guía del usuario de Amazon S3.

[S3.12] Las ACL no deben usarse para administrar el acceso de los usuarios a los cubos de uso general de S3

Requisitos relacionados: NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-6

Categoría: Proteger - Administración de acceso seguro > Control de acceso

Gravedad: media

Tipo de recurso: `AWS::S3::Bucket`

Regla de AWS Config : s3-bucket-acl-prohibited

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un bucket de uso general de Amazon S3 proporciona permisos de usuario con una lista de control de acceso (ACL). El control lanza un error si las ACL están configuradas para administrar el acceso de los usuarios a los buckets.

Las ACL son un mecanismo de control de acceso heredado anterior a IAM. En lugar de las ACL, recomendamos utilizar políticas de bucket de S3 o políticas AWS Identity and Access Management (IAM) para gestionar el acceso a los buckets de S3.

Corrección

Para superar este control, debe deshabilitar las ACL de sus buckets S3. Para obtener instrucciones, consulte Control de la propiedad de los objetos y desactivación de las ACL de su bucket en la Guía del usuario de Amazon Simple Storage Service.

Para crear una política de bucket S3, consulte Agregar una política de bucket mediante la consola de Amazon S3. Para crear una política de usuario de IAM en un bucket de S3, consulte Controlar el acceso a un bucket con políticas de usuario.

[S3.13] Los cubos de uso general de S3 deben tener configuraciones de ciclo de vida

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2) NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoría: Proteger > Protección de datos

Gravedad: baja

Tipo de recurso: `AWS::S3::Bucket`

Regla de AWS Config : s3-lifecycle-policy-check

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub CSPM
`targetTransitionDays`	Número de días después de crear los objetos cuando estos se trasladan a una clase de almacenamiento específico	Entero	De 1 a 36500	Sin valor predeterminado
`targetExpirationDays`	Número de días después de crear los objetos cuando estos se eliminan	Entero	De 1 a 36500	Sin valor predeterminado

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub CSPM
`targetTransitionStorageClass`	Tipo de clase de almacenamiento de S3 de destino	Enum	`STANDARD_IA`, `INTELLIGENT_TIERING`, `ONEZONE_IA`, `GLACIER`, `GLACIER_IR`, `DEEP_ARCHIVE`	Sin valor predeterminado

Este control comprueba si un bucket de uso general de Amazon S3 tiene una configuración de ciclo de vida. El control lanza un error si el bucket no tiene una configuración de ciclo de vida. Si proporciona valores personalizados para uno o varios de los parámetros anteriores, el control solo pasa si la política incluye la clase de almacenamiento, el tiempo de eliminación o el tiempo de transición especificados.

Al generar una configuración de ciclo de vida para su bucket de S3, define las acciones que desea que Amazon S3 realice durante la vida útil de un objeto. Por ejemplo, puede realizar la transición de objetos a otra clase de almacenamiento, archivarlos o eliminarlos después de un periodo de tiempo especificado.

Corrección

Para obtener información sobre cómo configurar las políticas de ciclo de vida en un bucket de Amazon S3, consulte Establecer la configuración del ciclo de vida en un bucket y consulte Administrar el ciclo de vida de almacenamiento en la Guía del usuario de Amazon S3.

[S3.14] Los cubos de uso general de S3 deben tener habilitado el control de versiones

Categoría: Proteger > Protección de datos > Protección contra la eliminación de datos

Requisitos relacionados: NIST.800-53.r5 AU-9 (2), NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6 (1), NIST.800-53.r5 CP-6 (2) NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5) NIST.800-53.r5 SI-12, 3.3.8 NIST.800-171.r2

Gravedad: baja

Tipo de recurso: `AWS::S3::Bucket`

Regla de AWS Config : s3-bucket-versioning-enabled

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un bucket de uso general de Amazon S3 tiene habilitado el control de versiones. El control lanza un error si se suspende el control de versiones del bucket.

El control de versiones conserva diversas variantes de un objeto en el mismo bucket de S3. Puedes usar el control de versiones para conservar, recuperar y restaurar todas las versiones de todos los objetos almacenados en tu bucket de S3. EL control de versiones ayuda a recuperarse de acciones no deseadas del usuario y de errores de la aplicación.

> **Tip**
>
> Permitir el control de versiones sin administrar el ciclo de vida puede generar un crecimiento ilimitado del almacenamiento y un aumento de los costos. Cada modificación de un objeto crea una nueva versión que se conserva indefinidamente. Configure las reglas del ciclo de vida de S3 para hacer la transición automática de las versiones no actuales a clases de almacenamiento más baratas o para que caduquen después de un período de retención definido. Para obtener más información, consulte Uso del control de versiones de S3 con S3 Lifecycle y Administración del ciclo de vida de los objetos.

Corrección

Para usar el control de versiones en un bucket de S3, consulte Habilitar el control de versiones en buckets en la Guía del usuario de Amazon S3.

[S3.15] Los cubos de uso general de S3 deben tener activado el bloqueo de objetos

Categoría: Proteger > Protección de datos > Protección contra la eliminación de datos

Requisitos relacionados: NIST.800-53.r5 CP-6 (2), PCI DSS v4.0. 1/105.1.1

Gravedad: media

Tipo de recurso: `AWS::S3::Bucket`

Regla de AWS Config : s3-bucket-default-lock-enabled

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub CSPM
`mode`	Modo de retención de Bloqueo de objetos de S3	Enum	`GOVERNANCE` , `COMPLIANCE`	Sin valor predeterminado

Este control comprueba si un bucket de uso general de Amazon S3 tiene habilitado el bloqueo de objetos. El control lanza un error si el bloqueo de objetos no está habilitado para el bucket. Si proporciona un valor personalizado para el parámetro `mode`, el control solo pasa si el Bloqueo de objetos de S3 utiliza el modo de retención especificado.

Puede usar Bloqueo de objetos de S3 para almacenar objetos mediante un modelo de escritura única y lectura múltiple (WORM). S3 Bloqueo de objetos puede ayudar a evitar que se eliminen o se sobrescriban objetos durante un periodo de tiempo determinado o de manera indefinida. Puede usar Bloqueo de objetos de S3 para cumplir con los requisitos normativos que precisen de almacenamiento WORM o agregar una capa adicional de protección frente a cambios y eliminaciones de objetos.

Corrección

Para configurar Bloqueo de objetos para buckets de S3 nuevos y existentes, consulte Configuración del Bloqueo de objetos de S3 en la Guía del usuario de Amazon S3.

[S3.17] Los cubos de uso general de S3 deben cifrarse en reposo con AWS KMS keys

Categoría: Proteger > Protección de datos > Cifrado de datos en reposo

Requisitos relacionados: NIST.800-53.r5 SC-12 (2), NIST.800-53.r5 CM-3 (6),, NIST.800-53.r5 SC-28 (1) NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-28, (10), NIST.800-53.r5 SC-7 (1), NIST.800-53.r5 CA-9 NIST.800-53.r5 SI-7 (6), NIST.800-171.r2 3.8.9, NIST.800-171.r2 3.13.11 NIST.800-53.r5 AU-9, 3.13.16, PCI DSS NIST.800-171.r2 v4.0. 1/35.5.1

Gravedad: media

Tipo de recurso: `AWS::S3::Bucket`

Regla de AWS Config : s3-default-encryption-kms

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un bucket de uso general de Amazon S3 está cifrado con un AWS KMS key (SSE-KMS o DSSE-KMS). El control falla si el bucket está cifrado con el cifrado predeterminado (SSE-S3).

Server-side el cifrado (SSE) es el cifrado de los datos en su destino por parte de la aplicación o el servicio que los recibe. A menos que especifique lo contrario, los buckets de S3 utilizan las claves administradas de Amazon S3 (SSE-S3) de forma predeterminada para el cifrado del lado del servidor. Sin embargo, para tener un mayor control, puede optar por configurar los buckets para usar el cifrado del lado del servidor con (o) en su lugar. AWS KMS keys SSE-KMS DSSE-KMS Amazon S3 cifra sus datos a nivel de objeto a medida que los escribe en los discos de los centros de AWS datos y los descifra automáticamente cuando accede a ellos.

Corrección

Para cifrar un bucket de S3 con () SSE-KMS, consulte Especificar el cifrado del lado del servidor con AWS KMS (SSE-KMS) en la guía del usuario de Amazon S3. Para cifrar un bucket de S3 con () DSSE-KMS, consulte Especificar el cifrado de doble capa en el servidor con AWS KMS keys (DSSE-KMS) en la guía del usuario de Amazon S3.

[S3.19] Los puntos de acceso S3 deben tener habilitada la configuración de bloqueo de acceso público

Requisitos relacionados: NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21),, NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), PCI DSS v4.0. 1/14.4.4

Categoría: Proteger > Gestión del acceso seguro > Recurso no accesible públicamente

Gravedad: crítica

Tipo de recurso: `AWS::S3::AccessPoint`

Regla de AWS Config : s3-access-point-public-access-blocks

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un punto de acceso de Amazon S3 tiene habilitada la configuración de Bloqueo de acceso público. Se produce un error en el control si la configuración de Bloqueo de acceso público no está habilitada para el punto de acceso.

La característica Bloqueo de acceso público de Amazon S3 ayuda a administrar el acceso a sus recursos de S3 en tres niveles: cuenta, bucket y punto de acceso. La configuración de cada nivel se puede configurar de forma independiente, lo que permite tener diferentes niveles de restricciones de acceso público para los datos. La configuración del punto de acceso no puede anular individualmente la configuración más restrictiva en los niveles superiores (nivel de cuenta o bucket asignado al punto de acceso). Por el contrario, la configuración a nivel del punto de acceso es acumulativa, lo que significa que complementa la configuración de los demás niveles y funciona junto con esta. A menos que pretenda que un punto de acceso de S3 sea de acceso público, debe habilitar la configuración de Bloqueo de acceso público.

Corrección

Amazon S3 actualmente no admite cambiar la configuración de bloqueo de acceso público de un punto de acceso después de que se haya creado el punto de acceso. Todas las configuraciones de Bloqueo de acceso público están habilitadas de forma predeterminada al crear un punto de acceso nuevo. Le recomendamos que deje todas las configuraciones habilitadas a menos que sepa que

tiene una necesidad específica de desactivar cualquiera de ellas. Para más información, consulte Administración de acceso público a puntos de acceso en la Guía del usuario de Amazon Simple Storage Service.

[S3.20] Los cubos de uso general de S3 deben tener habilitada la eliminación de MFA

Requisitos relacionados: CIS AWS Foundations Benchmark v5.0. 0/21.1.2, CIS AWS Foundations Benchmark v3.0. 0/2.1.2, CIS AWS Foundations Benchmark v1.4. 0/21.1.3, NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2) NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2)

Categoría: Proteger > Protección de datos > Protección contra la eliminación de datos

Gravedad: baja

Tipo de recurso: `AWS::S3::Bucket`

Regla de AWS Config : s3-bucket-mfa-delete-enabled

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control verifica si la eliminación mediante autenticación multifactor (MFA) está habilitada para un bucket de uso general de Amazon S3. El control falla si la eliminación mediante MFA no está habilitada para el bucket. El control no produce resultados para buckets que tienen una configuración de ciclo de vida.

Si habilita el control de versiones para un bucket de uso general de S3, puede agregar otra capa de seguridad al configurar la eliminación mediante MFA para el bucket. Si lo hace, el propietario del bucket debe incluir dos formas de autenticación en cualquier solicitud para eliminar una versión de un objeto en el bucket o cambiar el estado de control de versiones del bucket. La eliminación mediante MFA proporciona una protección adicional si, por ejemplo, las credenciales de seguridad del propietario del bucket resultan comprometidas. La eliminación mediante MFA también puede ayudar a evitar eliminaciones accidentales del bucket al exigir que el usuario que inicia la acción demuestre la posesión física de un dispositivo MFA con un código MFA, lo que añade una capa adicional de seguridad y fricción al proceso de eliminación.

> **Note**
>
> Este control produce un resultado `PASSED` solo si la eliminación mediante MFA está habilitada para el bucket de uso general de S3. Para habilitar la eliminación mediante MFA

para un bucket, el control de versiones también debe estar habilitado para el bucket. El control de versiones del bucket es un método para almacenar múltiples variaciones de un objeto de S3 en el mismo bucket. Además, solo el propietario del bucket que haya iniciado sesión como usuario raíz puede habilitar la eliminación mediante MFA y realizar acciones de eliminación en el bucket. No puede usar la eliminación mediante MFA con un bucket que tiene una configuración de ciclo de vida.

Corrección

Para obtener información sobre habilitar el control de versiones y configurar la eliminación mediante MFA para un bucket de S3, consulte Configuración de la eliminación mediante MFA en la Guía del usuario Amazon Simple Storage Service.

[S3.22] Los cubos de uso general de S3 deben registrar los eventos de escritura a nivel de objeto

Requisitos relacionados: CIS AWS Foundations Benchmark v5.0. 0/33.8, CIS AWS Foundations Benchmark v3.0. 0/33.8, PCI DSS v4.0. 1/102.1.

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: `AWS::::Account`

Regla de AWS Config : cloudtrail-all-write-s3-data-event-check

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si Cuenta de AWS tiene al menos un registro AWS CloudTrail multirregional que registre todos los eventos de datos de escritura de los buckets de Amazon S3. El control lanza un error si la cuenta no tiene un registro de seguimiento de varias regiones que registre los eventos de escritura de datos en los buckets de S3.

Las operaciones de S3 a nivel de objeto, como `GetObject`, `DeleteObject` y `PutObject`, se denominan eventos de datos. De forma predeterminada, CloudTrail no registra los eventos de datos, pero puede configurar rutas para registrar los eventos de datos en los buckets de S3. Al

habilitar el registro a nivel de objeto para los eventos de escritura de datos, puede registrar cada vez que se accede a un objeto (archivo) en un bucket de S3. Habilitar el registro a nivel de objeto puede ayudarte a cumplir los requisitos de cumplimiento de los datos, realizar análisis de seguridad exhaustivos, supervisar patrones específicos del comportamiento de los usuarios en tus buckets de S3 y tomar medidas en Cuenta de AWS relación con la actividad de las API a nivel de objeto en tus buckets de S3 mediante Amazon Events. CloudWatch Este control produce un resultado `PASSED` si configura un registro de seguimiento de varias regiones que registre eventos de datos de solo escritura o de todo tipo para todos los buckets de S3.

Corrección

Para habilitar el registro a nivel de objeto para los cubos de S3, consulte Habilitar el registro de CloudTrail eventos para los cubos y objetos de S3 en la Guía del usuario de Amazon Simple Storage Service.

[S3.23] Los cubos de uso general de S3 deben registrar los eventos de lectura a nivel de objeto

Requisitos relacionados: CIS AWS Foundations Benchmark v5.0. 0/32.9, CIS AWS Foundations Benchmark v3.0. 0/32.9, PCI DSS v4.0. 1/102.1.

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: `AWS::::Account`

Regla de AWS Config : cloudtrail-all-read-s3-data-event-check

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si Cuenta de AWS tiene al menos un registro AWS CloudTrail multirregional que registre todos los eventos de datos de lectura de los buckets de Amazon S3. El control lanza un error si la cuenta no tiene un registro de seguimiento de varias regiones que registre los eventos de lectura de datos en los buckets de S3.

Las operaciones de S3 a nivel de objeto, como `GetObject`, `DeleteObject` y `PutObject`, se denominan eventos de datos. De forma predeterminada, CloudTrail no registra los eventos de datos, pero puede configurar rutas para registrar los eventos de datos en los buckets de S3. Al

habilitar el registro a nivel de objeto para los eventos de lectura de datos, puede registrar cada vez que se accede a un objeto (archivo) en un bucket de S3. Habilitar el registro a nivel de objeto puede ayudarte a cumplir los requisitos de cumplimiento de los datos, realizar análisis de seguridad exhaustivos, supervisar patrones específicos del comportamiento de los usuarios en tus buckets de S3 y tomar medidas en Cuenta de AWS relación con la actividad de las API a nivel de objeto en tus buckets de S3 mediante Amazon Events. CloudWatch Este control produce un resultado `PASSED` si configura un registro de seguimiento de varias regiones que registre eventos de datos de solo lectura o de todo tipo para todos los buckets de S3.

Corrección

Para habilitar el registro a nivel de objeto para los cubos de S3, consulte Habilitar el registro de CloudTrail eventos para los cubos y objetos de S3 en la Guía del usuario de Amazon Simple Storage Service.

[S3.24] Los puntos de Multi-Region acceso S3 deben tener habilitada la configuración de bloqueo del acceso público

Requisitos relacionados: PCI DSS v4.0. 1/14.4.4

Categoría: Proteger > Configuración de red segura > Recursos no accesibles públicamente

Gravedad: alta

Tipo de recurso: `AWS::S3::MultiRegionAccessPoint`

AWS Config regla: `s3-mrap-public-access-blocked` (regla CSPM personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un punto de Multi-Region acceso de Amazon S3 tiene habilitada la configuración de bloqueo del acceso público. El control falla cuando el punto de Multi-Region acceso no tiene habilitada la configuración de bloqueo del acceso público.

Los recursos de acceso público pueden provocar accesos no autorizados, filtraciones de datos o explotación de vulnerabilidades. Restringir el acceso mediante autenticación y autorización permite proteger la información confidencial y mantener la integridad de sus recursos.

Corrección

De forma predeterminada, todos los ajustes de bloqueo del acceso público están habilitados para un punto de Multi-Region acceso S3. Para obtener más información, consulte Bloquear el acceso público con los puntos de Multi-Region acceso de Amazon S3 en la guía del usuario de Amazon Simple Storage Service. No puede cambiar la configuración de bloqueo del acceso público de un punto de Multi-Region acceso una vez creado.

[S3.25] Los buckets de directorio de S3 deben tener configuraciones de ciclo de vida

Categoría: Proteger > Protección de datos

Gravedad: baja

Tipo de recurso: `AWS::S3Express::DirectoryBucket`

Regla de AWS Config : s3express-dir-bucket-lifecycle-rules-check

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub CSPM
`targetExpirationDays`	La cantidad de días después de la creación del objeto en que los objetos deben expirar.	Entero	De 1 a 2147483647	Sin valor predeterminado

Este control verifica si las reglas de ciclo de vida están configuradas para un bucket de directorio de S3. El control falla si las reglas de ciclo de vida no están configuradas para el bucket de directorio, o si una regla de ciclo de vida del bucket especifica configuraciones de expiración que no coinciden con el valor del parámetro que se especifica opcionalmente.

En Amazon S3, una configuración de ciclo de vida es un conjunto de reglas que definen acciones que Amazon S3 aplica a un grupo de objetos en un bucket. Para un bucket de directorio de

S3, puede crear una regla de ciclo de vida que especifica cuándo expiran los objetos según su antigüedad (en días). También puede crear una regla de ciclo de vida que elimine las cargas incompletas realizadas en partes. A diferencia de otros tipos de buckets de S3, como los buckets de uso general, los buckets de directorio no admiten otros tipos de acciones para reglas de ciclo de vida, como la transición de objetos entre clases de almacenamiento.

Corrección

Para definir una configuración de ciclo de vida para un bucket de directorio de S3, cree una regla de ciclo de vida para el bucket. Para obtener más información, consulte Cómo crear y administrar una configuración de ciclo de vida para el bucket de directorio en la Guía del usuario de Amazon Simple Storage Service.

Controles CSPM de Security Hub para IA SageMaker

Estos AWS Security Hub CSPM controles evalúan el servicio y los recursos de Amazon SageMaker AI. Es posible que los controles no estén disponibles en todos los casos Regiones de AWS. Para obtener más información, consulte Disponibilidad de los controles por región.

[SageMaker.1] Las instancias de Amazon SageMaker Notebook no deberían tener acceso directo a Internet

Requisitos relacionados: NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21),, NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), PCI DSS v3.2. 1/1.2.1, PCI DSS v3.2. 1/11.3.1, PCI DSS v3.2. 1/13.3.2, PCI DSS v3.2. 1/13.3.4, PCI DSS v3.2. 1/13.3.6, PCI DSS versión 4.0. 1/14.4.4

Categoría: Proteger - Configuración de red segura

Gravedad: alta

Tipo de recurso: `AWS::SageMaker::NotebookInstance`

Regla de AWS Config : sagemaker-notebook-no-direct-internet-access

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si el acceso directo a Internet está desactivado para una instancia de portátil con SageMaker IA. El control falla si el campo `DirectInternetAccess` está habilitado para la instancia de cuaderno.

Si configuras tu instancia de SageMaker IA sin una VPC, el acceso directo a Internet está habilitado de forma predeterminada en tu instancia. Debe configurar la instancia con una VPC y cambiar la configuración predeterminada a Deshabilitar: acceso a Internet a través de una VPC. Para entrenar o alojar modelos desde un cuaderno, necesita acceso a Internet. Para habilitar el acceso a Internet, su VPC debe tener un punto de conexión de interfaz (AWS PrivateLink) o una puerta de enlace NAT y un grupo de seguridad que permita las conexiones salientes. Para obtener más información sobre cómo conectar una instancia de bloc de notas a los recursos de una VPC, consulte Cómo conectar una instancia de bloc de notas a los recursos de una VPC en la Guía para desarrolladores de Amazon SageMaker AI. También debes asegurarte de que el acceso a tu configuración de SageMaker IA esté limitado solo a los usuarios autorizados. Restrinja los permisos de IAM que permiten a los usuarios cambiar la configuración y los recursos de la SageMaker IA.

Corrección

Después de crear una instancia de cuaderno, no se puede cambiar la configuración de acceso a Internet. En su lugar, puede detener, eliminar y volver a crear la instancia con el acceso a Internet bloqueado. Para eliminar una instancia de bloc de notas que permita el acceso directo a Internet, consulte Usar instancias de cuadernos para crear modelos: Clean up en la Guía para desarrolladores de Amazon SageMaker AI. Para recrear una instancia de cuaderno que deniegue el acceso a Internet, consulte Crear una instancia de cuaderno. En Red, acceso directo a Internet, seleccione Deshabilitar: acceso a Internet a través de una VPC.

[SageMaker.2] las instancias de SageMaker cuadernos deben lanzarse en una VPC personalizada

Requisitos relacionados: NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9)

Categoría: Proteger > Configuración de red segura > Recursos dentro de VPC

Gravedad: alta

Tipo de recurso: `AWS::SageMaker::NotebookInstance`

Regla de AWS Config : sagemaker-notebook-instance-inside-vpc

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una instancia de cuaderno de SageMaker IA de Amazon se lanza dentro de una nube privada virtual (VPC) personalizada. Este control falla si una instancia de cuaderno de SageMaker IA no se lanza en una VPC personalizada o si se lanza en la VPC del servicio de SageMaker IA.

Las subredes son un rango de direcciones IP de una VPC. Recomendamos mantener sus recursos dentro de una VPC personalizada siempre que sea posible para garantizar una protección de red segura de su infraestructura. Una Amazon VPC es una red virtual dedicada a su. Cuenta de AWS Con una Amazon VPC, puede controlar el acceso a la red y la conectividad a Internet de sus instancias de SageMaker AI Studio y notebook.

Corrección

No se puede cambiar la configuración de VPC después de crear una instancia de cuaderno. En su lugar, puede detener, eliminar y volver a crear la instancia. Para obtener instrucciones, consulte Uso de instancias de cuadernos para crear modelos: Clean up en la Guía para desarrolladores de Amazon SageMaker AI.

[SageMaker.3] Los usuarios no deben tener acceso root a las instancias de los SageMaker cuadernos

Requisitos relacionados: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6 (10), NIST.800-53.r5 AC-6 (2)

Categoría: Proteger > Gestión del acceso seguro > Restricciones de acceso para los usuarios raíz

Gravedad: alta

Tipo de recurso: `AWS::SageMaker::NotebookInstance`

Regla de AWS Config : sagemaker-notebook-instance-root-access-check

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si el acceso raíz está activado en una instancia de bloc de notas de Amazon SageMaker AI. El control falla si el acceso raíz está activado para una instancia de cuaderno con SageMaker IA.

Siguiendo el principio de privilegios mínimos, se recomienda restringir el acceso raíz a los recursos de la instancia para evitar un exceso de permisos involuntario.

Corrección

Para restringir el acceso raíz a las instancias de cuadernos de SageMaker IA, consulte Controlar el acceso de raíz a una instancia de cuaderno de SageMaker IA en la Guía para desarrolladores de Amazon SageMaker AI.

[SageMaker.4] Las variantes de producción de SageMaker terminales deben tener un recuento inicial de instancias superior a 1

Requisitos relacionados: NIST.800-53.r5 CP-10 NIST.800-53.r5 SC-5, NIST.800-53.r5 SC-36, NIST.800-53.r5 SA-13

Categoría: Recuperación > Resiliencia > Alta disponibilidad

Gravedad: media

Tipo de recurso: `AWS::SageMaker::EndpointConfig`

Regla de AWS Config : sagemaker-endpoint-config-prod-instance-count

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si las variantes de producción de un punto de enlace de Amazon SageMaker AI tienen un recuento inicial de instancias superior a 1. El control falla si las variantes de producción del punto de conexión tienen solo 1 instancia inicial.

Las variantes de producción que se ejecutan con un recuento de instancias superior a 1 permiten la redundancia de instancias Multi-AZ gestionada por SageMaker la IA. La implementación de recursos en varias zonas de disponibilidad es una práctica AWS recomendada para proporcionar una alta disponibilidad dentro de su arquitectura. La alta disponibilidad lo ayuda a recuperarse de los incidentes de seguridad.

> **Note**
>
> Este control se aplica solo a la configuración del punto de conexión basada en instancias.

Corrección

Para obtener más información sobre los parámetros de la configuración de puntos finales, consulte Crear una configuración de puntos finales en la Guía para desarrolladores de Amazon SageMaker AI.

SageMaker Los modelos [SageMaker.5] deben tener habilitado el aislamiento de red

Categoría: Proteger > Configuración de red segura > Recursos no accesibles públicamente

Gravedad: media

Tipo de recurso: `AWS::SageMaker::Model`

Regla de AWS Config : sagemaker-model-isolation-enabled

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un modelo alojado en Amazon SageMaker AI tiene habilitado el aislamiento de red. El control falla si el parámetro `EnableNetworkIsolation` para el modelo alojado está establecido en `False`.

SageMaker El entrenamiento de la IA y los contenedores de inferencia implementados están habilitados para Internet de forma predeterminada. Si no quieres que la SageMaker IA proporcione acceso de red externa a tus contenedores de entrenamiento o inferencia, puedes habilitar el aislamiento de la red. Si habilita el aislamiento de red, no se podrán realizar llamadas de red de entrada o salida hacia o desde el contenedor del modelo, incluidas las llamadas hacia o desde otros Servicios de AWS. Además, no hay AWS credenciales disponibles para el entorno de ejecución del contenedor. Habilitar el aislamiento de la red ayuda a evitar el acceso no deseado a tus recursos de SageMaker IA desde Internet.

> **Note**
>
> El 13 de agosto de 2025, Security Hub CSPM cambió el título y la descripción de este control. El nuevo título y la descripción reflejan con mayor precisión que el control comprueba la configuración del `EnableNetworkIsolation` parámetro de los modelos alojados en Amazon SageMaker AI. Anteriormente, el título de este control era: SageMaker models should block inbound traffic.

Corrección

Para obtener más información sobre el aislamiento de redes para los modelos de SageMaker IA, consulte Cómo ejecutar contenedores de entrenamiento e inferencia sin conexión a Internet en la Guía para desarrolladores de Amazon SageMaker AI. Cuando crea un modelo, puede habilitar el aislamiento de red al establecer el valor del parámetro `EnableNetworkIsolation` en `True`.

[SageMaker.6] las configuraciones de imagen de la SageMaker aplicación deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::SageMaker::AppImageConfig`

Regla de AWS Config : sagemaker-app-image-config-tagged

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub CSPM
`requiredKeyTags`	Una lista de claves de etiqueta que no son del sistema y que se deben asignar a un recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si la configuración de imagen de una aplicación Amazon SageMaker AI (`AppImageConfig`) tiene las claves de etiqueta especificadas en el `requiredKeyTags` parámetro. El control falla si la configuración de imagen de la aplicación no tiene ninguna clave de etiqueta o si no incluye todas las claves especificadas por el parámetro `requiredKeyTags`. Si no especifica ningún valor para el parámetro `requiredKeyTags`, el control verifica únicamente la existencia de

una clave de etiqueta y falla si la configuración de imagen de la aplicación no tiene ninguna clave de etiqueta. El control ignora las etiquetas del sistema, que se aplican automáticamente y tienen el prefijo `aws:`.

Una etiqueta es una etiqueta que se crea y se asigna a un AWS recurso. Cada etiqueta consta de una clave de etiqueta necesaria y un valor de etiqueta opcional. Utilice etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. También pueden ayudar a identificar, organizar, buscar y filtrar recursos. También pueden ayudar a rastrear propietarios de recursos para acciones y notificaciones. También puede usar etiquetas para implementar control de acceso basado en atributos (ABAC) como estrategia de autorización. Para obtener más información sobre estrategias ABAC, consulte Definición de permisos basados en atributos con autorización ABAC en la Guía del usuario de IAM. Para obtener más información sobre las etiquetas, consulte la Guía del usuario del editor de etiquetas y AWS los recursos de etiquetado.

> **Note**
>
> No almacene información de identificación personal (PII) ni otra información confidencial en las etiquetas. Se puede acceder a las etiquetas desde muchos Servicios de AWS lugares. No están destinadas a usarse para datos privados o información confidencial.

Corrección

Para añadir etiquetas a la configuración de imágenes de una aplicación Amazon SageMaker AI (`AppImageConfig`), puede utilizar el AddTags funcionamiento de la API de SageMaker IA o, si está utilizando AWS CLI, ejecutar el comando add-tags.

[SageMaker.7] SageMaker las imágenes deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::SageMaker::Image`

Regla de AWS Config : sagemaker-image-tagged

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub CSPM
`requiredKeyTags`	Una lista de claves de etiqueta que no son del sistema y que se deben asignar a un recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si una imagen de Amazon SageMaker AI tiene las claves de etiqueta especificadas en el `requiredKeyTags` parámetro. El control falla si la imagen no tiene ninguna clave de etiqueta o si no incluye todas las claves especificadas por el parámetro `requiredKeyTags`. Si no especifica ningún valor para el parámetro `requiredKeyTags`, el control verifica únicamente la existencia de una clave de etiqueta y falla si la imagen no tiene ninguna clave de etiqueta. El control ignora las etiquetas del sistema, que se aplican automáticamente y tienen el prefijo `aws:`.

Una etiqueta es una etiqueta que se crea y se asigna a un AWS recurso. Cada etiqueta consta de una clave de etiqueta necesaria y un valor de etiqueta opcional. Utilice etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. También pueden ayudar a identificar, organizar, buscar y filtrar recursos. También pueden ayudar a rastrear propietarios de recursos para acciones y notificaciones. También puede usar etiquetas para implementar control de acceso basado en atributos (ABAC) como estrategia de autorización. Para obtener más información sobre estrategias ABAC, consulte Definición de permisos basados en atributos con autorización ABAC en la Guía del usuario de IAM. Para obtener más información sobre las etiquetas, consulte la Guía del usuario del editor de etiquetas y AWS los recursos de etiquetado.

> **Note**
>
> No almacene información de identificación personal (PII) ni otra información confidencial en las etiquetas. Se puede acceder a las etiquetas desde muchos Servicios de AWS lugares. No están destinadas a usarse para datos privados o información confidencial.

Corrección

Para añadir etiquetas a una imagen de SageMaker IA de Amazon, puede AddTags utilizar la API de SageMaker IA o, si está utilizando AWS CLI, ejecutar el comando add-tags.

[SageMaker.8] las instancias de SageMaker notebooks deben ejecutarse en plataformas compatibles

Categoría: Detectar > Administración de vulnerabilidades, parches y versiones

Gravedad: media

Tipo de recurso: `AWS::SageMaker::NotebookInstance`

Regla de AWS Config : sagemaker-notebook-instance-platform-version

Tipo de programa: Periódico

Parámetros:

- `supportedPlatformIdentifierVersions`: `notebook-al2023-v1` (no personalizable)

Este control comprueba si una instancia de bloc de notas de Amazon SageMaker AI está configurada para ejecutarse en una plataforma compatible, en función del identificador de plataforma especificado para la instancia de bloc de notas. El control falla si la instancia de cuaderno está configurada para ejecutarse en una plataforma que ya no recibe soporte.

Si la plataforma para una instancia de bloc de notas de Amazon SageMaker AI ya no es compatible, es posible que no reciba parches de seguridad, correcciones de errores u otros tipos de actualizaciones. Es posible que las instancias de Notebook sigan funcionando, pero no recibirán actualizaciones de seguridad de la SageMaker IA ni correcciones de errores críticos. Asume los riesgos asociados con el uso de una plataforma que dejó de recibir soporte. Para obtener más información, consulte el control de JupyterLab versiones en la Guía para desarrolladores de Amazon SageMaker AI.

Corrección

Para obtener información sobre las plataformas que Amazon SageMaker AI admite actualmente y cómo migrar a ellas, consulte las instancias de cuadernos de Amazon Linux 2 en la Guía para desarrolladores de Amazon SageMaker AI.

[SageMaker.9] las definiciones de trabajos de calidad de los SageMaker datos deben tener habilitado el cifrado del tráfico entre contenedores

Categoría: Proteger > Protección de datos > Cifrado de datos en tránsito

Gravedad: media

Tipo de recurso: `AWS::SageMaker::DataQualityJobDefinition`

Regla de AWS Config : sagemaker-data-quality-job-encrypt-in-transit

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una definición de trabajo de calidad de datos de Amazon SageMaker AI tiene habilitado el cifrado para el tráfico entre contenedores. El control falla si la definición de un trabajo que monitorea la calidad y la variación de los datos no tiene habilitado el cifrado para el tráfico entre contenedores.

Al habilitar el cifrado del tráfico entre contenedores, se protegen los datos confidenciales del aprendizaje automático durante el procesamiento distribuido para analizar la calidad de los datos.

Corrección

Para obtener más información sobre el cifrado del tráfico entre contenedores para Amazon SageMaker AI, consulte Proteger las comunicaciones entre instancias de procesamiento automático en un trabajo de entrenamiento distribuido en la Guía para desarrolladores de SageMaker IA de Amazon. Al crear una definición de trabajo de calidad de datos, puede habilitar el cifrado del tráfico entre contenedores configurando el valor del `EnableInterContainerTrafficEncryption` parámetro en. `True`

[SageMaker.10] Las definiciones de trabajos de explicabilidad del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores

Categoría: Proteger > Protección de datos > Cifrado de datos en tránsito

Gravedad: media

Tipo de recurso: `AWS::SageMaker::ModelExplainabilityJobDefinition`

Regla de AWS Config : sagemaker-model-explainability-job-encrypt-in-transit

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una definición de trabajo de explicabilidad de un SageMaker modelo de Amazon tiene habilitado el cifrado del tráfico entre contenedores. El control falla si la definición del trabajo de explicabilidad del modelo no tiene habilitado el cifrado del tráfico entre contenedores.

Al habilitar el cifrado del tráfico entre contenedores, se protegen los datos confidenciales del aprendizaje automático, como los datos de los modelos, los conjuntos de datos de entrenamiento, los resultados del procesamiento intermedio, los parámetros y las ponderaciones de los modelos, durante el procesamiento distribuido para analizar la explicabilidad.

Corrección

En el caso de una definición de trabajo explicable de un SageMaker modelo existente, el cifrado del tráfico entre contenedores no se puede actualizar en su lugar. Para crear un nuevo SageMaker modelo de definición de trabajo explicativo con el cifrado del tráfico entre contenedores habilitado, utilice la API o la CLI o configúrelo en. CloudFormation `EnableInterContainerTrafficEncryption` `True`

[SageMaker.11] las definiciones de trabajos SageMaker de calidad de los datos deben tener habilitado el aislamiento de red

Categoría: Proteger - Configuración de red segura

Gravedad: media

Tipo de recurso: `AWS::SageMaker::DataQualityJobDefinition`

Regla de AWS Config : sagemaker-data-quality-job-isolation

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una definición de trabajo de supervisión de la calidad de los datos de Amazon SageMaker AI tiene habilitado el aislamiento de red. El control falla si la definición de un trabajo que monitorea la calidad y la variación de los datos tiene desactivado el aislamiento de la red.

El aislamiento de la red reduce la superficie de ataque e impide el acceso externo, lo que protege contra el acceso externo no autorizado, la exposición accidental de los datos y la posible exfiltración de datos.

Corrección

Para obtener más información sobre el aislamiento de redes para la SageMaker IA, consulte Cómo ejecutar contenedores de entrenamiento e inferencia sin conexión a Internet en la Guía para desarrolladores de SageMaker IA de Amazon. Al crear una definición de trabajo de calidad de datos, puede habilitar el aislamiento de la red estableciendo el valor del `EnableNetworkIsolation` parámetro en. `True`

[SageMaker.12] las definiciones de trabajo basadas en el sesgo del SageMaker modelo deben tener habilitado el aislamiento de red

Categoría: Proteger > Configuración de red segura > Configuración de políticas de recursos

Gravedad: media

Tipo de recurso: `AWS::SageMaker::ModelBiasJobDefinition`

Regla de AWS Config : sagemaker-model-bias-job-isolation

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una definición de trabajo basada en el sesgo del SageMaker modelo tiene habilitado el aislamiento de red. El control falla si la definición del trabajo de sesgo del modelo no tiene habilitado el aislamiento de red.

El aislamiento de la red evita que los trabajos basados en el SageMaker modelo se comuniquen con recursos externos a través de Internet. Al habilitar el aislamiento de la red, se asegura de que los contenedores del trabajo no puedan establecer conexiones salientes, lo que reduce la superficie de ataque y protege los datos confidenciales de la filtración. Esto es particularmente importante para los trabajos que procesan datos confidenciales o regulados.

Corrección

Para habilitar el aislamiento de la red, debe crear una nueva definición de trabajo basada en el sesgo del modelo con el `EnableNetworkIsolation` parámetro establecido en`True`. El aislamiento de la red no se puede modificar después de crear la definición de trabajo. Para crear una nueva definición

de trabajo basada CreateModelBiasJobDefinition en el sesgo del modelo, consulte la Guía para desarrolladores de Amazon SageMaker AI.

[SageMaker.13] las definiciones de trabajos de calidad del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores

Categoría: Proteger > Protección de datos > Cifrado de datos en tránsito

Gravedad: media

Tipo de recurso: `AWS::SageMaker::ModelQualityJobDefinition`

Regla de AWS Config : ssagemaker-model-quality-job-encrypt-in-transit

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si las definiciones de trabajos de calidad SageMaker modelo de Amazon tienen habilitado el cifrado en tránsito para el tráfico entre contenedores. El control falla si una definición de trabajo de calidad modelo no tiene habilitado el cifrado del tráfico entre contenedores.

Inter-container el cifrado del tráfico protege los datos transmitidos entre contenedores durante los trabajos de supervisión de la calidad de los modelos distribuidos. De forma predeterminada, el tráfico entre contenedores no está cifrado. La activación del cifrado ayuda a mantener la confidencialidad de los datos durante el procesamiento y contribuye al cumplimiento de los requisitos normativos para la protección de los datos en tránsito.

Corrección

Para habilitar el cifrado del tráfico entre contenedores en la definición de trabajo de calidad de su SageMaker modelo de Amazon, debe volver a crear la definición del trabajo con la configuración de cifrado en tránsito adecuada. Para crear una definición de trabajo con calidad de modelo, consulte la Guía para CreateModelQualityJobDefinition desarrolladores de Amazon SageMaker AI.

[SageMaker.14] los programas SageMaker de monitoreo deben tener habilitado el aislamiento de la red

Categoría: Proteger - Configuración de red segura

Gravedad: media

Tipo de recurso: `AWS::SageMaker::MonitoringSchedule`

Regla de AWS Config : sagemaker-monitoring-schedule-isolation

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si los programas de SageMaker monitorización de Amazon tienen activado el aislamiento de la red. El control falla si un programa de monitoreo se ha EnableNetworkIsolation establecido en falso o no está configurado

El aislamiento de la red impide que las tareas de supervisión realicen llamadas salientes a la red, lo que reduce la superficie de ataque al eliminar el acceso a Internet desde los contenedores.

Corrección

Para obtener información sobre cómo configurar el aislamiento de la red en el NetworkConfig parámetro al crear o actualizar un programa de monitorización, consulte CreateMonitoringSchedule o consulte UpdateMonitoringSchedule la Guía para desarrolladores de Amazon SageMaker AI.

[SageMaker.15] Las definiciones de trabajo basadas en el sesgo del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores

Categoría: Proteger > Protección de datos > Cifrado de datos en tránsito

Gravedad: media

Tipo de recurso: `AWS::SageMaker::ModelBiasJobDefinition`

Regla de AWS Config : sagemaker-model-bias-job-encrypt-in-transit

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si las definiciones de trabajos de sesgo de SageMaker modelo de Amazon tienen habilitado el cifrado del tráfico entre contenedores cuando se utilizan varias instancias de procesamiento. El control produce un error si `EnableInterContainerTrafficEncryption` se establece en falso o no está configurado para definiciones de trabajos con un recuento de instancias igual o superior a 2.

Inter-container el cifrado del tráfico protege los datos transmitidos entre las instancias de procesamiento durante las tareas de supervisión del sesgo del modelo distribuido. El cifrado evita el

acceso no autorizado a la información relacionada con el modelo, como los pesos que se transmiten entre instancias.

Corrección

Para habilitar el cifrado del tráfico entre contenedores para las definiciones de trabajos con sesgo de SageMaker modelo, defina el `EnableInterContainerTrafficEncryption` parámetro como `True` cuando la definición del trabajo utilice varias instancias de procesamiento. Para obtener información sobre la protección de las comunicaciones entre instancias de procesamiento automático, consulte Proteger las comunicaciones entre instancias de procesamiento automático en un trabajo de entrenamiento distribuido en la guía para desarrolladores de Amazon SageMaker AI.

SageMaker Los modelos [SageMaker.16] deben usar un registro privado en la VPC para los contenedores principales

Categoría: Proteger > Configuración de red segura > Recursos dentro de VPC

Gravedad: media

Tipo de recurso: `AWS::SageMaker::Model`

Regla de AWS Config : sagemaker-model-private-registry-required

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un modelo de SageMaker IA de Amazon extrae una imagen de contenedor de un registro privado en una VPC para el contenedor principal. El control falla si la imagen no está configurada o el modo de acceso al repositorio sí lo está. `Platform`

El uso de un registro Docker privado en una VPC para SageMaker modelos de contenedores garantiza que las imágenes de los contenedores provengan de fuentes controladas y confiables de la VPC. Además, garantiza que se acceda a las imágenes de los contenedores a través de los puntos finales de la VPC, sin necesidad de atravesar la Internet pública.

Corrección

Para configurar registros de Docker privados para contenedores de inferencia de SageMaker IA en tiempo real, consulte Usar un registro de Docker privado para contenedores de Real-Time inferencia en la Guía para desarrolladores de IA de Amazon. SageMaker

[SageMaker.17] SageMaker Las tiendas offline de los grupos de funciones deben cifrarse con AWS KMS claves

Categoría: Proteger > Protección de datos > Cifrado de datos en reposo

Gravedad: media

Tipo de recurso: `AWS::SageMaker::FeatureGroup`

Regla de AWS Config : sagemaker-featuregroup-encryption-at-rest

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una tienda SageMaker offline de Amazon de un grupo de funciones está cifrada en reposo con una AWS KMS clave. El control falla si el almacenamiento S3 de la tienda offline de un grupo de funciones no está cifrado con una clave de KMS.

El uso del cifrado gestionado AWS KMS keys por el cliente en las tiendas offline del resto de grupos de SageMaker funciones proporciona una seguridad mejorada. Customer-managed Las claves de KMS le proporcionan un control total sobre el ciclo de vida de las claves de cifrado y las políticas clave. Además, todo el uso de las claves de cifrado se puede registrar y supervisar AWS CloudTrail para poder auditarlo.

Corrección

Para obtener información sobre cómo habilitar el cifrado inactivo en las tiendas offline de SageMaker Feature Store con claves AWS KMS administradas por los clientes, consulta la sección Seguridad y control de acceso en la Guía para desarrolladores de Amazon SageMaker AI.

[SageMaker.18] las tiendas en línea de grupos de SageMaker funciones con almacenamiento estándar deben cifrarse con AWS KMS claves

Requisitos relacionados: NIST.800-53.r5 AU-9, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SC-12 (2), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SI-7 (6)

Categoría: Proteger - Protección de datos - Cifrado de datos en reposo

Gravedad: media

Tipo de recurso: `AWS::SageMaker::FeatureGroup`

Regla de AWS Config : sagemaker-featuregroup-online-store-encryption

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una tienda SageMaker online de Amazon de un grupo de características con almacenamiento estándar está cifrada en reposo con una AWS KMS clave. El control falla si el cifrado de la clave KMS no está configurado para la tienda en línea.

El uso del cifrado administrado AWS KMS keys por el cliente en el resto de las tiendas en línea del grupo de SageMaker funciones proporciona una seguridad mejorada. Customer-managed Las claves de KMS le brindan un control total sobre el ciclo de vida de las claves de cifrado y las políticas clave. Además, todo el uso de las claves de cifrado se puede registrar y supervisar AWS CloudTrail para poder auditarlo.

Corrección

Para obtener información sobre cómo habilitar el cifrado inactivo en las tiendas en línea de SageMaker Feature Store con claves AWS KMS administradas por los clientes, consulte Seguridad y control de acceso en la Guía para desarrolladores de Amazon SageMaker AI.

[SageMaker.19] SageMaker los modelos deben usar un registro privado en la VPC para las canalizaciones de inferencia de varios contenedores

Categoría: Proteger > Configuración de red segura > Recursos dentro de VPC

Gravedad: media

Tipo de recurso: `AWS::SageMaker::Model`

Regla de AWS Config : sagemaker-model-multicontainer-private-registry

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si los modelos de SageMaker IA de Amazon con canalizaciones de inferencia de varios contenedores extraen imágenes de contenedores de un registro de Docker privado en una VPC. El control falla si alguna definición de contenedor no tiene una configuración de imagen o tiene el modo de acceso al repositorio establecido en plataforma.

El uso de un registro Docker privado en una VPC para las canalizaciones de inferencia de múltiples contenedores con SageMaker IA garantiza que las imágenes de los contenedores se obtengan de fuentes controladas y confiables dentro de su VPC. Esto garantiza que se acceda a las imágenes de los contenedores a través de los puntos finales de la VPC, sin tener que atravesar la Internet pública, lo que reduce el riesgo de ataques a la cadena de suministro o de manipulación de imágenes.

Corrección

Para configurar registros de Docker privados para contenedores de inferencias de SageMaker IA en tiempo real, consulte Usar un registro de Docker privado para contenedores de inferencia en la Guía para Real-Time desarrolladores de IA de Amazon. SageMaker

[SageMaker.20] explicabilidad del SageMaker modelo: las definiciones de los trabajos deben tener habilitado el aislamiento de red

Categoría: Proteger > Configuración de red segura > Recursos no accesibles públicamente

Gravedad: alta

Tipo de recurso: `AWS::SageMaker::ModelExplainabilityJobDefinition`

Regla de AWS Config : sagemaker-model-explainability-job-network-isolation

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si la definición de un trabajo de explicabilidad de un modelo de SageMaker IA tiene habilitado el aislamiento de red. El control falla si la definición del trabajo no tiene habilitado el aislamiento de red.

El aislamiento de la red impide que los contenedores de trabajos explicativos del modelo realicen llamadas salientes a la red, lo que reduce el riesgo de filtración de datos y proporciona una defensa exhaustiva de los datos confidenciales del modelo y el entrenamiento.

Corrección

Para habilitar el aislamiento de la red para una definición del trabajo explicable de un modelo de SageMaker IA, configúrala al crear la definición del trabajo. `NetworkConfig.EnableNetworkIsolation` `true` Para obtener más información sobre el aislamiento de redes para la SageMaker IA, consulte Cómo ejecutar contenedores de entrenamiento e inferencia sin conexión a Internet en la Guía para desarrolladores de IA de Amazon SageMaker .

[SageMaker.21] las instancias de SageMaker cuadernos deben cifrarse y gestionarse por el cliente AWS KMS claves

Categoría: Proteger - Protección de datos - Cifrado de datos en reposo

Gravedad: media

Tipo de recurso: `AWS::SageMaker::NotebookInstance`

Regla de AWS Config : sagemaker-notebook-instance-storage-vol-kms-encrypted

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una instancia de portátil con SageMaker IA está configurada con una AWS KMS clave para el cifrado del volumen de almacenamiento. El control falla si no hay una clave de KMS configurada para la instancia del portátil.

El cifrado de los datos en reposo con una clave de KMS administrada por el cliente proporciona un control de acceso adicional en comparación con el cifrado AWS administrado predeterminado. SageMaker Las instancias de ordenadores portátiles con IA almacenan los cuadernos de los usuarios, los conjuntos de datos, los artefactos de modelos y los datos de procesamiento temporal en volúmenes de almacenamiento de aprendizaje automático. Una clave gestionada por el cliente permite un control detallado de las políticas de claves, un registro de CloudTrail auditoría del uso de las claves y el cumplimiento de los marcos que requieren un cifrado controlado por el cliente.

Corrección

Para configurar una clave de KMS para una instancia de cuaderno de SageMaker IA, consulte las instancias de Notebook, los trabajos de SageMaker IA y los puntos de enlace en la Guía para desarrolladores de Amazon AI. SageMaker Tenga en cuenta que solo `KmsKeyId` se puede configurar en el momento de la creación de la instancia de bloc de notas. Para solucionarlo, crea una nueva instancia de bloc de notas con la clave de KMS especificada y migra los datos de la instancia existente.

[SageMaker.22] los programas SageMaker de monitoreo deben tener habilitado el cifrado del tráfico entre contenedores

Categoría: Proteger - Protección de datos - Cifrado de datos en tránsito

Gravedad: media

Tipo de recurso: `AWS::SageMaker::MonitoringSchedule`

Regla de AWS Config : sagemaker-monitoring-schedule-traffic-encryption

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un programa de monitoreo de Amazon SageMaker AI tiene habilitado el cifrado para el tráfico entre contenedores. El control falla si la definición del trabajo de supervisión no tiene habilitado el cifrado para el tráfico entre contenedores.

Inter-container el cifrado del tráfico garantiza que los datos transmitidos entre los contenedores durante las tareas de supervisión se cifren en tránsito. Sin este cifrado, los datos confidenciales procesados durante la supervisión del modelo podrían quedar expuestos a un acceso no autorizado dentro de la red. Habilitar esta configuración ayuda a cumplir los requisitos de cumplimiento para proteger los datos en tránsito.

Corrección

En el caso de un cronograma de monitoreo de la SageMaker IA existente, el cifrado del tráfico entre contenedores no se puede actualizar en su lugar. Para crear un nuevo programa de monitoreo de la SageMaker IA con el cifrado del tráfico entre contenedores habilitado, utilice la API o la CLI o CloudFormation `EnableInterContainerTrafficEncryption` configúrelo como `true` en el `NetworkConfig` del. `MonitoringJobDefinition`

[SageMaker.23] los experimentos de SageMaker inferencia deben tener el volumen de almacenamiento de instancias cifrado y gestionado por el cliente AWS KMS claves

Categoría: Proteger - Protección de datos - Cifrado de datos en reposo

Gravedad: media

Tipo de recurso: `AWS::SageMaker::InferenceExperiment`

Regla de AWS Config : sagemaker-inf-experiment-instance-storage-kms-encrypted

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un experimento de inferencia de SageMaker IA está configurado con una AWS KMS clave, por ejemplo, el cifrado del volumen de almacenamiento. El control falla si no se especifica una clave de KMS para el cifrado del volumen de almacenamiento de la instancia.

El cifrado de los volúmenes de almacenamiento de instancias con claves de KMS administradas por el cliente proporciona una administración de claves centralizada, un registro de auditorías y un control de rotación de claves para los artefactos del modelo y los datos de inferencia temporales almacenados en las instancias de procesamiento de aprendizaje automático durante las pruebas clandestinas.

Corrección

Para configurar una clave de KMS para un experimento de inferencia de SageMaker IA, especifica el `KmsKey` parámetro al realizar la llamada. `CreateInferenceExperiment` `KmsKey`Puede ser un identificador de clave de KMS, un ARN, un alias o un ARN de alias. El rol de ejecución de la SageMaker IA debe tener `kms:CreateGrant` permiso sobre la clave. Para obtener más información sobre cómo especificar una AWS KMS clave de SageMaker IA gestionada por el cliente, consulte las instancias de Notebook, los trabajos de SageMaker IA y los puntos de enlace en la Guía para desarrolladores de Amazon SageMaker AI.

[SageMaker.24] los experimentos de SageMaker inferencia deben tener el almacenamiento de datos cifrado y gestionado por el cliente AWS KMS claves

Categoría: Proteger - Protección de datos - Cifrado de datos en reposo

Gravedad: media

Tipo de recurso: `AWS::SageMaker::InferenceExperiment`

Regla de AWS Config : sagemaker-inf-experiment-data-storage-kms-encrypted

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un experimento de inferencia de SageMaker IA con la captura de datos habilitada tiene una clave de KMS configurada para cifrar los datos capturados en reposo. El control falla si la configuración de almacenamiento de datos no especifica una clave de KMS para el cifrado.

El cifrado de los datos de solicitud de inferencia y respuesta capturados con claves de KMS administradas por el cliente garantiza que las cargas útiles de inferencia confidenciales almacenadas

en Amazon S3 estén protegidas con capacidades de auditoría y administración de claves centralizadas.

Corrección

Para configurar una clave de KMS para el almacenamiento de datos en un experimento de inferencia de SageMaker IA, especifique el campo en el que se encuentra al realizar la `KmsKey` llamada. `DataStorageConfig` `CreateInferenceExperiment` `KmsKey`Cifra los datos de respuesta y solicitud de inferencia capturados en reposo en el bucket de Amazon S3 especificado. Para obtener más información sobre cómo especificar una AWS KMS clave de SageMaker IA gestionada por el cliente, consulte las instancias de Notebook, los trabajos de SageMaker IA y los puntos de enlace en la Guía para desarrolladores de SageMaker IA de Amazon.

[SageMaker.25] las definiciones de trabajos de calidad del SageMaker modelo deben tener habilitado el aislamiento de red

Categoría: Proteger > Configuración de red segura > Recursos no accesibles públicamente

Gravedad: alta

Tipo de recurso: `AWS::SageMaker::ModelQualityJobDefinition`

Regla de AWS Config : sagemaker-model-quality-job-definition-isolation

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una definición de trabajo de calidad de un modelo de Amazon SageMaker AI tiene habilitado el aislamiento de red. El control falla si la definición del trabajo de calidad del modelo no tiene habilitado el aislamiento de red.

El aislamiento de la red reduce la superficie de ataque e impide el acceso externo, lo que protege contra el acceso externo no autorizado, la exposición accidental de datos y la posible filtración de datos.

Corrección

Al crear una definición de trabajo con calidad de modelo, puede habilitar el aislamiento de la red estableciendo el valor del `EnableNetworkIsolation` parámetro en. `True` Para obtener más información sobre el aislamiento de redes para la SageMaker IA, consulte Cómo ejecutar

contenedores de entrenamiento e inferencia sin conexión a Internet en la Guía para desarrolladores de Amazon SageMaker AI.

Controles CSPM de Security Hub para Secrets Manager

Estos AWS Security Hub CSPM controles evalúan el AWS Secrets Manager servicio y los recursos.

Es posible que estos controles no estén disponibles en todosRegiones de AWS. Para obtener más información, consulte Disponibilidad de los controles por región.

[SecretsManager.1] Los secretos de Secrets Manager deberían tener habilitada la rotación automática

Requisitos relacionados: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), PCI DSS v4.0. 1/83.6.3, PCI DSS v4.0. 1/8.3.9

Categoría: Proteger - Desarrollo seguro

Gravedad: media

Tipo de recurso: `AWS::SecretsManager::Secret`

Regla de AWS Config: `secretsmanager-rotation-enabled-check`

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`maximumAllowedRotationFrequency`	Número máximo de días permitidos para la frecuencia de rotación del secreto	Entero	De 1 a 365	Sin valor predeterminado

Este control comprueba si un secreto almacenado en AWS Secrets Manager está configurado con rotación automática. Se produce un error en el control si el secreto no está

configurado con rotación automática. Si proporciona un valor personalizado para el parámetro `maximumAllowedRotationFrequency`, el control solo pasa si el secreto gira automáticamente dentro del margen de tiempo especificado.

Secrets Manager le ayuda a mejorar la posición de seguridad de la organización. Los secretos incluyen credenciales de base de datos, contraseñas y claves de API de terceros. Puede usar Secrets Manager para almacenar secretos de forma centralizada, cifrarlos automáticamente, controlar el acceso a los secretos y renovar los secretos de forma segura y automática.

Secrets Manager puede renovar secretos. Puede usar la rotación para reemplazar los secretos a largo plazo por secretos a corto plazo. La renovar de sus secretos limita el tiempo que un usuario no autorizado puede usar un secreto comprometido. Por este motivo, debe renovar sus secretos con frecuencia. Para obtener más información sobre la rotación, consulte Cómo girar AWS Secrets Manager los secretos en la Guía del AWS Secrets Manager usuario.

Corrección

Para activar la rotación automática de los secretos de Secrets Manager, consulte Configurar la rotación automática de AWS Secrets Manager los secretos mediante la consola en la Guía del AWS Secrets Manager usuario. Debe elegir y configurar una AWS Lambda función de rotación.

[SecretsManager.2] Los secretos de Secrets Manager configurados con rotación automática deberían girar correctamente

Requisitos relacionados: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), PCI DSS v4.0. 1/83.6.3, PCI DSS v4.0. 1/8.3.9

Categoría: Proteger - Desarrollo seguro

Gravedad: media

Tipo de recurso: `AWS::SecretsManager::Secret`

Regla de AWS Config: `secretsmanager-scheduled-rotation-success-check`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un AWS Secrets Manager secreto se ha rotado correctamente en función del programa de rotación. El control tiene errores si `RotationOccurringAsScheduled` es `false`. El control solo evalúa los secretos que tienen la renovación activada.

Secrets Manager le ayuda a mejorar la posición de seguridad de la organización. Los secretos incluyen credenciales de base de datos, contraseñas y claves de API de terceros. Puede usar Secrets Manager para almacenar secretos de forma centralizada, cifrarlos automáticamente, controlar el acceso a los secretos y renovar los secretos de forma segura y automática.

Secrets Manager puede renovar secretos. Puede usar la rotación para reemplazar los secretos a largo plazo por secretos a corto plazo. La renovar de sus secretos limita el tiempo que un usuario no autorizado puede usar un secreto comprometido. Por este motivo, debe renovar sus secretos con frecuencia.

Además de configurar los secretos para que giren automáticamente, debe asegurarse de que esos secretos giren correctamente según el programa de renovación.

Para obtener más información sobre la renovación, consulte Cómo renovar sus secretos de AWS Secrets Manager en la Guía del usuario de AWS Secrets Manager.

Corrección

Si se produce un error en la renovación automática, es posible que Secrets Manager haya detectado errores en la configuración. La rotación de secretos en requiere el uso de una función de Lambda que defina cómo interactuar con la base de datos o el servicio al que pertenece el secreto.

Para obtener ayuda para diagnosticar y corregir errores comunes relacionados con la rotación de secretos, consulte Solución de problemas de AWS Secrets Manager rotación de secretos en la Guía del AWS Secrets Managerusuario.

[SecretsManager.3] Eliminar los secretos de Secrets Manager no utilizados

Requisitos relacionados: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15)

Categoría: Proteger - Administración de acceso seguro

Gravedad: media

Tipo de recurso: `AWS::SecretsManager::Secret`

Regla de AWS Config: `secretsmanager-secret-unused`

Tipo de programa: Periódico

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`unusedForDays`	Número máximo de días durante el que un secreto puede permanecer sin uso	Entero	De `1` a `365`	`90`

Este control comprueba si se ha accedido a un AWS Secrets Manager secreto dentro del período de tiempo especificado. Se produce un error en el control si un secreto no se utiliza más allá del periodo especificado. A menos que proporcione un valor de parámetro personalizado para el período de acceso, el CSPM de Security Hub utiliza un valor predeterminado de 90 días.

Eliminar los secretos no utilizados es tan importante como renovarlos. Los antiguos usuarios pueden abusar de los secretos no utilizados, ya que ya no necesitan acceder a ellos. Además, a medida que más usuarios acceden a un secreto, es posible que alguien lo haya manipulado mal y lo haya filtrado a una entidad no autorizada, lo que aumenta el riesgo de abuso. Eliminar los secretos no utilizados ayuda a revocar el acceso secreto a los usuarios que ya no lo necesitan. También ayuda a reducir el costo de usar Secrets Manager. Por lo tanto, es esencial eliminar de forma rutinaria los secretos no utilizados.

Corrección

Para eliminar los secretos inactivos de Secrets Manager, consulte Eliminar un AWS Secrets Manager secreto en la Guía del AWS Secrets Manager usuario.

[SecretsManager.4] Los secretos de Secrets Manager deben rotarse en un número específico de días

Requisitos relacionados: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), PCI DSS v4.0. 1/83.6.3, PCI DSS v4.0. 1/8.3.9

Categoría: Proteger - Administración de acceso seguro

Gravedad: media

Tipo de recurso: `AWS::SecretsManager::Secret`

Regla de AWS Config: `secretsmanager-secret-periodic-rotation`

Tipo de programa: Periódico

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`maxDaysSinceRotation`	Número máximo de días durante el que un secreto puede permanecer sin cambios	Entero	De `1` a `180`	`90`

Este control comprueba si un AWS Secrets Manager secreto se rota al menos una vez dentro del período de tiempo especificado. Se produce un error en el control si no se rota un secreto al menos con esta frecuencia. A menos que proporciones un valor de parámetro personalizado para el período de rotación, el CSPM de Security Hub utiliza un valor predeterminado de 90 días.

La rotación de los secretos puede ayudarle a reducir el riesgo de que se usen sus secretos sin autorización en su Cuenta de AWS. Los ejemplos incluyen credenciales de base de datos, contraseñas, claves de API de terceros e incluso texto arbitrario. Si no cambia sus secretos durante un largo período de tiempo, los secretos se vuelven más propensos a ser comprometidos.

Ya que hay más usuarios que acceden a un secreto, existen más probabilidades de que alguien haya cometido un error y lo haya filtrado a una entidad no autorizada. Los secretos se pueden filtrar a través de registros y datos de caché. Pueden compartirse con fines de depuración y no pueden cambiarse ni revocarse una vez que se complete la depuración. Por todas estas razones, los secretos deben rotarse con frecuencia.

Puede configurar la renovación automática de los datos secretos en AWS Secrets Manager. Con la rotación automática, puede reemplazar secretos a largo plazo con secretos a corto plazo, lo cual reducirá significativamente el riesgo de peligro. Le sugerimos que configure la rotación automática para sus secretos de Secrets Manager. Para obtener más información, consulte Rotación de sus secretos de AWS Secrets Manager en la Guía del usuario de AWS Secrets Manager.

Corrección

Para activar la rotación automática de los secretos de Secrets Manager, consulte Configurar la rotación automática de AWS Secrets Manager los secretos mediante la consola en la Guía del AWS Secrets Manager usuario. Debe elegir y configurar una AWS Lambda función de rotación.

[SecretsManager.5] Los secretos de Secrets Manager deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::SecretsManager::Secret`

AWS Configregla: `tagged-secretsmanager-secret` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	`No default value`

Este control comprueba si un AWS Secrets Manager secreto tiene etiquetas con las claves específicas definidas en el parámetro`requiredTagKeys`. El control falla si el secreto no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y falla si el secreto no está etiquetado con ninguna

clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, incluidasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte Etiquetar sus AWS recursos en el. Referencia general de AWS

Corrección

Para añadir etiquetas a un secreto de Secrets Manager, consulta Etiquetar AWS Secrets Manager secretos en la Guía del AWS Secrets Manager usuario.

Controles CSPM de Security Hub paraAWS Service Catalog

Este AWS Security Hub CSPM control evalúa el AWS Service Catalog servicio y los recursos. Es posible que el control no esté disponible en todas las Regiones de AWS. Para obtener más información, consulte Disponibilidad de los controles por región.

[ServiceCatalog.1] Las carteras de Service Catalog deben compartirse dentro de unAWSsolo una organización

Requisitos relacionados: NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-6, NIST.800-53.r5 CM-8, NIST.800-53.r5 SC-7

Categoría: Proteger - Administración de acceso seguro

Gravedad: media

Tipo de recurso: `AWS::ServiceCatalog::Portfolio`

Regla de AWS Config: service-catalog-shared-within-organization

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si AWS Service Catalog comparte carteras dentro de una organización cuando la integración con AWS Organizations está habilitada. El control falla si las carteras no se comparten dentro de una organización.

Compartir carteras solo dentro de Organizations permite garantizar que una cartera no se comparta con Cuentas de AWS incorrectas. Para compartir una cartera de Service Catalog con una cuenta de una organización, Security Hub CSPM recomienda utilizarla `ORGANIZATION_MEMBER_ACCOUNT` en lugar de. `ACCOUNT` Esto simplifica la administración al regular el acceso otorgado a la cuenta en toda la organización. Si tiene una necesidad empresarial de compartir carteras de Service Catalog con una cuenta externa, puede suprimir automáticamente los resultados de este control o deshabilitarlo.

Corrección

Para habilitar el uso compartido de carteras conAWS Organizations, consulte Compartir con AWS Organizations en la Guía del AWS Service Catalogadministrador.

Controles CSPM de Security Hub para Amazon SES

Estos AWS Security Hub CSPM controles evalúan el servicio y los recursos de Amazon Simple Email Service (Amazon SES).

Es posible que estos controles no estén disponibles en todosRegiones de AWS. Para obtener más información, consulte Disponibilidad de los controles por región.

[SES.1] Las listas de contactos de SES deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::SES::ContactList`

AWS Configregla: `tagged-ses-contactlist` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si una lista de contactos de Amazon SES tiene etiquetas con claves específicas definidas en el parámetro `requiredTagKeys`. El control falla si la lista de contactos no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si la lista de contactos no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para

sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte Etiquetar sus AWS recursos en el. Referencia general de AWS

Corrección

Para añadir etiquetas a una lista de contactos de Amazon SES, consulte TagResourcela referencia de la API v2 de Amazon SES.

[SES.2] Los conjuntos de configuración de SES deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::SES::ConfigurationSet`

AWS Configregla: `tagged-ses-configurationset` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que	Sin valor predeterminado

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
	recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.		cumplan los requisitos de AWS.	

Este control comprueba si un conjunto de configuración de Amazon SES tiene etiquetas con claves específicas definidas en el parámetro `requiredTagKeys`. El control falla si el conjunto de configuración no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si el conjunto de configuración no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte Etiquetar sus AWS recursos en el. Referencia general de AWS

Corrección

Para añadir etiquetas a un conjunto de configuraciones de Amazon SES, consulte TagResourcela referencia de la API v2 de Amazon SES.

[SES.3] Los conjuntos de configuración de SES deben tener el TLS habilitado para enviar correos electrónicos

Categoría: Proteger > Protección de datos > Cifrado de datos en tránsito

Gravedad: media

Tipo de recurso: `AWS::SES::ConfigurationSet`

Regla de AWS Config: ses-sending-tls-required

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un conjunto de configuraciones de Amazon SES requiere conexiones TLS. El control falla si la política TLS no está configurada `'REQUIRE'` para un conjunto de configuraciones.

De forma predeterminada, Amazon SES usa un TLS oportunista, lo que significa que los correos electrónicos se pueden enviar sin cifrar si no se puede establecer una conexión TLS con el servidor de correo receptor. Al aplicar el TLS para el envío de correos electrónicos, se garantiza que los mensajes solo se entreguen cuando se pueda establecer una conexión cifrada segura. Esto ayuda a proteger la confidencialidad e integridad del contenido del correo electrónico durante la transmisión entre Amazon SES y el servidor de correo del destinatario. Si no se puede establecer una conexión TLS segura, el mensaje no se entregará, lo que evitará la posible exposición de información confidencial.

> **Note**
>
> Si bien TLS 1.3 es el método de entrega predeterminado para Amazon SES, si no se aplica el requisito de TLS a través de los conjuntos de configuración, los mensajes podrían entregarse en texto sin formato si se produce un error en la conexión TLS. Para superar este control, debe configurar la política de TLS para que se ajuste a las opciones de entrega de su conjunto de `'REQUIRE'` configuraciones de SES. Cuando se requiere TLS, los mensajes solo se entregan si se puede establecer una conexión TLS con el servidor de correo receptor.

Corrección

Para configurar Amazon SES para que requiera conexiones TLS para un conjunto de configuraciones, consulte Amazon SES y los protocolos de seguridad en la Guía para desarrolladores de Amazon SES.

Controles de CSPM de Security Hub para Amazon SNS

Estos AWS Security Hub CSPM controles evalúan el servicio y los recursos del Amazon Simple Notification Service (Amazon SNS). Es posible que los controles no estén disponibles en todosRegiones de AWS. Para obtener más información, consulte Disponibilidad de los controles por región.

[SNS.1] Los temas de SNS deben cifrarse en reposo medianteAWS KMS

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6),, (1) NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (10), NIST.800-53.r5 SC-7 NIST.800-53.r5 SI-7 (6), 3.13.11, NIST.800-171.r2 3.13.16 NIST.800-171.r2

Categoría: Proteger > Protección de datos > Cifrado de datos en reposo

Gravedad: media

Tipo de recurso: `AWS::SNS::Topic`

Regla de AWS Config: `sns-encrypted-kms`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un tema de Amazon SNS está cifrado en reposo utilizando claves administradas en AWS Key Management Service (AWS KMS). Los controles fallan si el tema de SNS no utiliza una clave de KMS para el cifrado del servidor (SSE). De forma predeterminada, SNS almacena los mensajes y archivos mediante el cifrado de disco. Para pasar este control, debe optar por utilizar una clave KMS para el cifrado. Esto agrega una capa adicional de seguridad y brinda una mayor flexibilidad de control de acceso.

El cifrado de los datos en reposo reduce el riesgo de que un usuario no autenticado acceda a los datos almacenados en el disco. AWS Se requieren permisos de API para descifrar los datos antes de

que puedan leerse. Recomendamos cifrar temas de SNS con claves de KMS para tener una capa de seguridad adicional.

Corrección

Para habilitar SSE para un tema de SNS, consulte Habilitación del cifrado del servidor (SSE) para Amazon SNS en la Guía para desarrolladores de Amazon Simple Notification Service. Antes de poder usar SSE, también debe configurar AWS KMS key políticas que permitan el cifrado de temas y el cifrado y descifrado de mensajes. Para obtener más información, consulte Configuración de AWS KMS permisos en la Guía para desarrolladores de Amazon Simple Notification Service.

[SNS.2] El registro del estado de entrega debe estar habilitado para los mensajes de notificación enviados a un tema

> **Important**
>
> Security Hub CSPM retiró este control en abril de 2024. Para obtener más información, consulte Registro de cambios de los controles del CSPM de Security Hub.

Requisitos relacionados:, NIST.800-53.r5 AU-12 NIST.800-53.r5 AU-2

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: `AWS::SNS::Topic`

Regla de AWS Config: `sns-topic-message-delivery-notification-enabled`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si el registro está habilitado para el estado de entrega de los mensajes de notificación enviados a un tema de Amazon SNS para los puntos de conexión. Este control falla si la notificación del estado de entrega de los mensajes no está habilitada.

El registro es una parte importante del mantenimiento de la fiabilidad, la disponibilidad y el rendimiento de los servicios. El registro del estado de entrega de los mensajes aporta información operativa, como la siguiente:

- Saber si un mensaje se ha entregado al punto de enlace de Amazon SNS.
- Identificar la respuesta enviada desde el punto de enlace de Amazon SNS a Amazon SNS.
- Determinar el tiempo de permanencia del mensaje (el tiempo entre la marca de tiempo de publicación y la entrega a un punto de conexión de Amazon SNS).

Corrección

Para configurar el registro del estado de entrega de un tema, consulte el Estado de entrega de los mensajes de Amazon SNS en la Guía para desarrolladores de Amazon Simple Notification Service.

[SNS.3] Los temas de SNS deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::SNS::Topic`

AWS Configregla: `tagged-sns-topic` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	`No default value`

Este control comprueba si un tema de Amazon SNS tiene etiquetas con claves específicas definidas en el parámetro `requiredTagKeys`. El control falla si el tema no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si el tema no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte Etiquetar sus AWS recursos en el. Referencia general de AWS

Corrección

Para agregar etiquetas a un tema de SNS, consulte Configuración de etiquetas de temas de Amazon SNS en la Guía para desarrolladores del servicio de Amazon Simple Notification Service.

[SNS.4] Las políticas de acceso a los temas de SNS no deberían permitir el acceso público

Categoría: Proteger > Configuración de red segura > Recursos no accesibles públicamente

Gravedad: crítica

Tipo de recurso: `AWS::SNS::Topic`

Regla de AWS Config: sns-topic-no-public-access

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si la política de acceso a los temas de Amazon SNS permite el acceso público. Este control falla si la política de acceso a los temas de Amazon SNS permite el acceso público.

Puede utilizar una política de acceso de Amazon SNS con un tema determinado para restringir quién puede trabajar en ese tema (por ejemplo, quién puede publicar mensajes en el tema, quién se puede suscribir al tema, etcétera). Las políticas de SNS pueden conceder acceso a otros Cuentas de AWS usuarios o a los propios usuarios. Cuenta de AWS El uso de un carácter comodín (*) en el campo `Principal` de la política de temas y la falta de condiciones para limitar la política de temas pueden provocar la exfiltración de datos, la denegación del servicio o la inyección no deseada de mensajes en el servicio por parte de un atacante.

> **Note**
>
> Este control no evalúa condiciones de políticas que utilicen caracteres comodín o variables. Para generar un resultado `PASSED`, las condiciones de la política de acceso de Amazon SNS para un tema deben usar únicamente valores fijos, es decir, valores que no contengan caracteres comodín ni variables de la política. Para obtener información sobre variables de políticas, consulte Variables y etiquetas en la Guía del usuario de AWS Identity and Access Management.

Corrección

Para actualizar las políticas de acceso de un tema de SNS, consulte Información general sobre la administración del acceso en Amazon SNS en la Guía para desarrolladores del servicio Amazon Simple Notification Service.

Controles CSPM de Security Hub para Amazon SQS

Estos AWS Security Hub CSPM controles evalúan el servicio y los recursos del Amazon Simple Queue Service (Amazon SQS). Es posible que los controles no estén disponibles en todos. Regiones de AWS Para obtener más información, consulte Disponibilidad de los controles por región.

[SQS.1] Las colas de Amazon SQS deben cifrarse en reposo

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6)

Categoría: Proteger > Protección de datos > Cifrado de datos en reposo

Gravedad: media

Tipo de recurso: `AWS::SQS::Queue`

AWS Configregla: `sqs-queue-encrypted` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una cola de Amazon SQS está cifrada en reposo. El control falla si la cola no está cifrada con una SQS-managed clave (SSE-SQS) o una clave AWS Key Management Service (AWS KMS) (). SSE-KMS

El cifrado de los datos en reposo reduce el riesgo de que un usuario no autorizado acceda a los datos almacenados en el disco. Server-side El cifrado (SSE) protege el contenido de los mensajes de las colas de SQS mediante claves de SQS-managed cifrado (SSE-SQS) o AWS KMS claves (). SSE-KMS

Corrección

Para configurar el SSE para una cola de SQS, consulte Configuración del cifrado del servidor (SSE) para una cola (consola) en la Guía para desarrolladores de Amazon Simple Queue Service.

[SQS.2] Las colas de SQS deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::SQS::Queue`

AWS Configregla: `tagged-sqs-queue` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	`No default value`

Este control comprueba si una cola de Amazon SQS tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control falla si la cola no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y falla si la cola no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre

ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte Etiquetar sus AWS recursos en el. Referencia general de AWS

Corrección

Para agregar etiquetas a una cola existente mediante la consola de Amazon SQS, consulte Configuring cost allocation tags for an Amazon SQS queue (console) en la Guía para desarrolladores de Amazon Simple Queue Service.

[SQS.3] Las políticas de acceso a las colas de SQS no deberían permitir el acceso público

Categoría: Proteger > Gestión del acceso seguro > Recurso no accesible públicamente

Gravedad: crítica

Tipo de recurso: `AWS::SQS::Queue`

Regla de AWS Config: sqs-queue-no-public-access

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control verifica si una política de acceso de Amazon SQS permite el acceso público a una cola de SQS. El control falla si una política de acceso de SQS permite el acceso público a la cola.

Una política de acceso a Amazon SQS puede permitir el acceso público a una cola de SQS, lo que podría permitir que un usuario anónimo o cualquier identidad de AWS IAM autenticada accediera a la cola. Las políticas de acceso de SQS suelen permitir este acceso mediante el uso del carácter comodín (`*`) en el elemento `Principal` de la política o al no utilizar condiciones adecuadas para restringir el acceso a la cola, o ambas cosas. Si una política de acceso de SQS permite el acceso público, terceros podrían realizar tareas como recibir mensajes de la cola, enviar mensajes a la cola o modificar la política de acceso de la cola. Esto puede derivar en eventos como exfiltración de datos, denegación de servicio o inyección de mensajes en la cola por parte de un actor malintencionado.

> **Note**
>
> Este control no evalúa condiciones de políticas que utilicen caracteres comodín o variables. Para generar un resultado `PASSED`, las condiciones en la política de acceso de Amazon

SQS para una cola deben usar únicamente valores fijos, es decir, valores que no incluyan caracteres comodín ni variables de políticas. Para obtener información sobre variables de políticas, consulte Variables y etiquetas en la Guía del usuario de AWS Identity and Access Management.

Corrección

Para obtener información sobre cómo configurar la política de acceso de SQS para una cola de SQS, consulte Uso de políticas personalizadas con el lenguaje de políticas de acceso de Amazon SQS en la Guía del desarrollador de Amazon Simple Queue Service (Amazon SQS).

Controles CSPM de Security Hub para Step Functions

Estos AWS Security Hub CSPM controles evalúan el AWS Step Functions servicio y los recursos.

Es posible que estos controles no estén disponibles en todosRegiones de AWS. Para obtener más información, consulte Disponibilidad de los controles por región.

[StepFunctions.1] Step Functions indica que las máquinas deben tener el registro activado

Requisitos relacionados: PCI DSS v4.0. 1/104.4.2

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: `AWS::StepFunctions::StateMachine`

Regla de AWS Config: `step-functions-state-machine-logging-enabled`

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`logLevel`	Nivel mínimo de registro	Enum	`ALL`, `ERROR`, `FATAL`	Sin valor predeterminado

Este control comprueba si una máquina de AWS Step Functions estado tiene activado el registro. El control falla si una máquina de estados no tiene el registro activado. Si proporciona un valor personalizado para el parámetro `logLevel`, el control solo pasa si la máquina de estados tiene activado el nivel de registro especificado.

La monitorización le ayuda a mantener la fiabilidad, la disponibilidad y el rendimiento de Step Functions. Debe recopilar la mayor cantidad de datos de supervisión de los Servicios de AWS que utiliza para poder depurar más fácilmente los fallos multipunto. Tener una configuración de registro definida para sus máquinas de estado de Step Functions le permite realizar un seguimiento del historial de ejecución y los resultados en Amazon CloudWatch Logs. Si lo desea, puede realizar un seguimiento únicamente de los errores o eventos fatales.

Corrección

Para activar el registro en una máquina de estados de Step Functions, consulte Configurar el registro en la Guía para desarrolladores de AWS Step Functions.

[StepFunctions.2] Las actividades de Step Functions deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::StepFunctions::Activity`

AWS Configregla: `tagged-stepfunctions-activity` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si una AWS Step Functions actividad tiene etiquetas con las claves específicas definidas en el parámetro`requiredTagKeys`. El control lanza error si la actividad no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si la actividad no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte Etiquetar sus AWS recursos en el. Referencia general de AWS

Corrección

Para agregar etiquetas a una actividad de Step Functions, consulte Etiquetado en Step Functions en la Guía para desarrolladores de AWS Step Functions.

Controles CSPM de Security Hub para Systems Manager

Estos AWS Security Hub CSPM controles evalúan el servicio y los recursos AWS Systems Manager (SSM). Es posible que los controles no estén disponibles en todosRegiones de AWS. Para obtener más información, consulte Disponibilidad de los controles por región.

[SSM.1] Las instancias de Amazon EC2 deben administrarse medianteAWS Systems Manager

Requisitos relacionados: PCI DSS v3.2. 1/24., NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2), NIST.800-53.r5 CM-8 (1) NIST.800-53.r5 CM-8, (2), NIST.800-53.r5 CM-8 (3), NIST.800-53.r5 CM-8 (2), NIST.800-53.r5 SA-15 (8), NIST.800-53.r5 SA-15 (3) NIST.800-53.r5 SA-3 NIST.800-53.r5 SI-2

Categoría: Identificar - Inventario

Gravedad: media

Recurso evaluado: `AWS::EC2::Instance`

Recursos AWS Config de grabación necesarios: `AWS::EC2::Instance` `AWS::SSM::ManagedInstanceInventory`

Regla de AWS Config: ec2-instance-managed-by-systems-manager

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si las instancias EC2 de su cuenta detenidas y en ejecución están gestionadas porAWS Systems Manager. Systems Manager es un sistema Servicio de AWS que puede utilizar para ver y controlar su AWS infraestructura.

Para ayudarle a mantener la seguridad y el cumplimiento, Systems Manager analiza las instancias administradas detenidas y en ejecución. Una instancia administrada es una máquina configurada para utilizar Systems Manager. Luego, Systems Manager informa o toma medidas correctivas sobre cualquier infracción de política que detecte. Systems Manager también lo ayuda a configurar y mantener sus instancias administradas. Para obtener más información, consulte la Guía del usuario de AWS Systems Manager.

> **Note**
>
> Este control genera `FAILED` resultados para las instancias EC2 que son instancias de AWS Elastic Disaster Recovery Replication Server administradas porAWS. Una instancia de servidor de replicación es una instancia EC2 que se lanza automáticamente AWS Elastic Disaster Recovery para permitir la replicación continua de datos desde los servidores de origen. AWSelimina intencionadamente el agente Systems Manager (SSM) de estas instancias para mantener el aislamiento y evitar posibles rutas de acceso no deseadas.

Corrección

Para obtener información sobre la administración de instancias EC2 conAWS Systems Manager, consulte la administración de hosts de Amazon EC2 en AWS Systems Managerla Guía del usuario. En la sección de opciones de configuración de la AWS Systems Manager consola, puede conservar la configuración predeterminada o cambiarla según sea necesario según la configuración que prefiera.

[SSM.2] Las instancias de Amazon EC2 administradas por Systems Manager deben tener el estado de conformidad con los parches de CONFORMIDAD CON LOS PARCHES tras la instalación de un parche

Requisitos relacionados: NIST.800-53.r5 CM-8 (3), NIST.800-53.r5 SI-2 (2) NIST.800-53.r5 SI-2, (3), NIST.800-53.r5 SI-2 (4), NIST.800-53.r5 SI-2 NIST.800-53.r5 SI-2 (5), NIST.800-171.r2 3.7.1, PCI DSS v3.2. 1/62.2, PCI DSS v4.0. 1/22.2.1, PCI DSS v4.0. 1/6.3.3

Categoría: Detectar - Servicios de detección

Gravedad: alta

Tipo de recurso: `AWS::SSM::PatchCompliance`

Regla de AWS Config: ec2-managedinstance-patch-compliance-status-check

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si el estado de la conformidad de los parches de Systems Manager es `COMPLIANT` o `NON_COMPLIANT` después de instalar el parche en la instancia. El control falla si el estado de conformidad es `NON_COMPLIANT`. El control solo comprueba las instancias administradas por el Administrador de parches de Systems Manager.

Tener las instancias EC2 con parches según lo especificado por su organización reduce la superficie expuesta a ataques de su Cuentas de AWS.

Corrección

Systems Manager recomienda utilizar políticas de parches para configurar los parches para las instancias administradas. También puede utilizar los documentos de Systems Manager, tal y como se describe en el siguiente procedimiento, para aplicar un parche a una instancia.

Para solucionar parches no conformes

1. Abre la AWS Systems Manager consola en. https://console.aws.amazon.com/systems-manager/
2. En Administración de nodos, elija Ejecutar comando y, a continuación, elija Ejecutar comando.
3. Seleccione la opción para AWS- RunPatchBaseline.
4. Cambie la Operation (Operación) a Install (Instalar).
5. Seleccione Elegir las instancias manualmente y, a continuación, elija las instancias no conformes.
6. Seleccione Ejecutar.
7. Una vez completado el comando, para monitorear el nuevo estado de conformidad de las instancias con parches, elija Conformidad en el panel de navegación.

[SSM.3] Las instancias de Amazon EC2 administradas por Systems Manager deben tener el estado de conformidad de la asociación de COMPLIANT

Requisitos relacionados: NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2), (1) NIST.800-53.r5 CM-8, NIST.800-53.r5 CM-8 (3), NIST.800-53.r5 CM-8 NIST.800-53.r5 SI-2 (3), PCI DSS v3.2. 1/24.4, PCI DSS v4.0. 1/2.2.1, PCI DSS v4.0. 1/6.3.3

Categoría: Detectar - Servicios de detección

Gravedad: baja

Tipo de recurso: `AWS::SSM::AssociationCompliance`

Regla de AWS Config: ec2-managedinstance-association-compliance-status-check

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si el estado de conformidad de la AWS Systems Manager asociación es `COMPLIANT` o `NON_COMPLIANT` después de que la asociación se ejecute en una instancia. El control falla si el estado de conformidad de la asociación es `NON_COMPLIANT`.

Una asociación de State Manager es una configuración que se asigna a sus instancias administradas. La configuración define el estado que desea mantener en las instancias. Por ejemplo, una asociación puede especificar que el software antivirus debe estar instalado y ejecutándose en sus instancias, o bien que determinados puertos deben estar cerrados.

Después de crear una o varias asociaciones de administradores estatales, la información sobre el estado de la conformidad estará disponible inmediatamente. Puede ver el estado de conformidad en la consola o en respuesta a AWS CLI los comandos o las acciones correspondientes de la API de Systems Manager. En el caso de las asociaciones, Conformidad de la configuración muestra el estado de conformidad (`Compliant` o`Non-compliant`). También muestra el nivel de gravedad asignado a la asociación, como `Critical` o `Medium`.

Para obtener más información sobre el cumplimiento de las asociaciones de gerentes estatales, consulte Acerca del cumplimiento de las asociaciones de gerentes estatales en la Guía del usuario de AWS Systems Manager.

Corrección

Una asociación fallida puede estar relacionada con diferentes factores, como los destinos y los nombres de los documentos de Systems Manager. Para solucionar este problema, primero debe identificar e investigar la asociación consultando el historial de asociaciones. Para obtener instrucciones sobre cómo ver el historial de asociaciones, consulte Visualización del historial de asociaciones en la Guía del usuario de AWS Systems Manager.

Tras investigar, puede editar la asociación para corregir el problema identificado. Puede editar una asociación para especificar un nuevo nombre, la programación, el nivel de gravedad o los destinos. Tras editar una asociación, AWS Systems Manager crea una nueva versión. Para obtener instrucciones sobre cómo editar una asociación, consulte Edición y creación de una nueva versión de una asociación en la Guía del usuario de AWS Systems Manager.

[SSM.4] Los documentos SSM no deben ser públicos

Requisitos relacionados: NIST.800-53.r5 AC-21 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21),, NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9)

Categoría: Proteger > Configuración de red segura > Recursos no accesibles públicamente

Gravedad: crítica

Tipo de recurso: `AWS::SSM::Document`

Regla de AWS Config: ssm-document-not-public

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si AWS Systems Manager los documentos que son propiedad de una cuenta son públicos. El control falla si los documentos de Systems Manager que tienen `Self` como propietario son públicos.

Los documentos de Systems Manager que son públicos pueden permitir el acceso no deseado a sus documentos. Un documento público de Systems Manager puede exponer información valiosa sobre su cuenta, sus recursos y sus procesos internos.

A menos que el caso de uso requiera uso compartido público, recomendamos bloquear el uso compartido público para los documentos de Systems Manager que tengan `Self` como propietario.

Corrección

Para obtener información sobre cómo configurar el uso compartido de documentos de Systems Manager, consulte Uso compartido de un documento de SSM en la Guía del usuario de AWS Systems Manager.

[SSM.5] Los documentos SSM deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::SSM::Document`

Regla de AWS Config: ssm-document-tagged

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredKeyTags`	Una lista de claves de etiqueta que no son del sistema y que se deben asignar a un recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si un AWS Systems Manager documento tiene las claves de etiquetas especificadas por el `requiredKeyTags` parámetro. El control falla si el documento no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas por el parámetro `requiredKeyTags`.

Si no se especifican valores para el parámetro `requiredKeyTags`, el control solo verifica la existencia de una clave de etiqueta y falla si el documento no tiene ninguna. El control ignora las etiquetas del sistema, que se aplican automáticamente y tienen el prefijo `aws:`. El control no evalúa los documentos de Systems Manager que pertenecen a Amazon.

Una etiqueta es una etiqueta que se crea y se asigna a un AWS recurso. Cada etiqueta consta de una clave de etiqueta necesaria y un valor de etiqueta opcional. Utilice etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. También pueden ayudar a identificar, organizar, buscar y filtrar recursos. También pueden ayudar a rastrear propietarios de recursos para acciones y notificaciones. También puede usar etiquetas para implementar control de acceso basado en atributos (ABAC) como estrategia de autorización. Para obtener más información sobre estrategias ABAC, consulte Definición de permisos basados en atributos con autorización ABAC en la Guía del usuario de IAM. Para obtener más información sobre las etiquetas, consulte los AWSrecursos de etiquetado y la Guía del usuario del editor de etiquetas.

> **Note**
>
> No almacene información de identificación personal (PII) ni otra información confidencial en las etiquetas. Se puede acceder a las etiquetas desde muchos Servicios de AWS sitios. No están destinadas a usarse para datos privados o información confidencial.

Corrección

Para añadir etiquetas a un AWS Systems Manager documento, puede utilizar la AddTagsToResourceoperación de la AWS Systems Manager API o, si está utilizando laAWS CLI, ejecutar el comando add-tags-to-resource. También puede usar la consola de AWS Systems Manager.

[SSM.6] SSM Automation debería tener el registro habilitado CloudWatch

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: `AWS::::Account`

Regla de AWS Config: ssm-automation-logging-enabled

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si el CloudWatch registro de Amazon está habilitado para la automatización AWS Systems Manager (SSM). El control falla si el CloudWatch registro no está habilitado para SSM Automation.

SSM Automation es una AWS Systems Manager herramienta que le ayuda a crear soluciones automatizadas para implementar, configurar y administrar AWS los recursos a escala mediante manuales predefinidos o personalizados. Para cumplir requisitos operativos o de seguridad en la organización, podría necesitar proporcionar un registro de los scripts que ejecuta. Puede configurar SSM Automation para enviar el resultado de `aws:executeScript` las acciones de sus runbooks a un grupo de CloudWatch registros de Amazon Logs que especifique. Con CloudWatch Logs, puede monitorear, almacenar y acceder a los archivos de registro de varios archivos. Servicios de AWS

Corrección

Para obtener información sobre cómo habilitar el CloudWatch registro para SSM Automation, consulte Registrar los resultados de las acciones de automatización con CloudWatch registros en la Guía del AWS Systems Manager usuario.

[SSM.7] Los documentos SSM deben tener habilitada la configuración de bloqueo para compartir en público

Categoría: Proteger > Gestión del acceso seguro > Recurso no accesible públicamente

Gravedad: crítica

Tipo de recurso: `AWS::::Account`

Regla de AWS Config: ssm-automation-block-public-sharing

Tipo de programa: Periódico

Parámetros: ninguno

Este control verifica si la configuración para bloquear el uso compartido público está habilitada para los documentos de AWS Systems Manager. El control falla si la configuración para bloquear el uso compartido público está desactivada para los documentos de Systems Manager.

La configuración para bloquear el uso público de los documentos AWS Systems Manager (SSM) es una configuración a nivel de cuenta. Habilitar esta configuración puede evitar el acceso no deseado

a los documentos de SSM. Si habilita esta configuración, el cambio no afecta a los documentos de SSM que actualmente comparte con el público. A menos que el caso de uso requiera compartir documentos de SSM con el público, recomendamos habilitar la configuración para bloquear el uso compartido público. La configuración puede ser diferente para cada uno de ellos. Región de AWS

Corrección

Para obtener información sobre cómo habilitar la configuración para bloquear el uso compartido público de los documentos de AWS Systems Manager (SSM), consulte Bloqueo del uso compartido público de documentos de SSM en la Guía del usuario de AWS Systems Manager.

Controles CSPM de Security Hub paraAWS Transfer Family

Estos AWS Security Hub CSPM controles evalúan el AWS Transfer Family servicio y los recursos. Es posible que los controles no estén disponibles en todosRegiones de AWS. Para obtener más información, consulte Disponibilidad de los controles por región.

[Transfer.1]AWS Transfer Familylos flujos de trabajo deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::Transfer::Workflow`

AWS Configregla: `tagged-transfer-workflow` (regla CSPM de Security Hub personalizada)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredTagKeys`	Lista de claves de etiquetas que no corresponden al sistema que debe contener el	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que	`No default value`

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
	recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.		cumplan los requisitos de AWS.	

Este control comprueba si un AWS Transfer Family flujo de trabajo tiene etiquetas con las claves específicas definidas en el parámetro`requiredTagKeys`. El control lanza error si el flujo de trabajo no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si el flujo de trabajo no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

> **Note**
>
> No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetasServicios de AWS, entre ellasAWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte Etiquetar sus AWS recursos en el. Referencia general de AWS

Corrección

Para agregar etiquetas a un flujo de trabajo de Transfer Family (consola)

1. Abre la consola. AWS Transfer Family
2. En el panel de navegación, elija Workflows (Flujos de trabajo). Luego, seleccione el flujo de trabajo que desea etiquetar.
3. Elija Administrar etiquetas y luego agregue las etiquetas.

[Transfer.2] Los servidores Transfer Family no deben usar el protocolo FTP para la conexión de puntos finales

Requisitos relacionados: NIST.800-53.r5 CM-7, NIST.800-53.r5 IA-5 NIST.800-53.r5 SC-8, PCI DSS v4.0. 1/42.2.1

Categoría: Proteger > Protección de datos > Cifrado de datos en tránsito

Gravedad: media

Tipo de recurso: `AWS::Transfer::Server`

Regla de AWS Config: transfer-family-server-no-ftp

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si un AWS Transfer Family servidor utiliza un protocolo distinto del FTP para la conexión del punto final. El control lanza error si el servidor utiliza el protocolo FTP para que un cliente se conecte al punto de conexión del servidor.

El protocolo de transferencia de archivos (FTP) establece la conexión del punto de conexión mediante canales no cifrados, lo que hace que los datos enviados a través de estos canales sean vulnerables a la interceptación. El uso del protocolo de transferencia de archivos de Shell (SFTP), el protocolo de transferencia de archivos (FTPS) o el protocolo de declaración de aplicabilidad 2 (AS2) ofrece un nivel de seguridad adicional mediante el cifrado de los datos en tránsito y se pueden utilizar para ayudar a evitar posibles ataques de “man-in-the-middle” (MitM) o similares para espiar o manipular el tráfico de red.

Corrección

Para modificar el protocolo de un servidor de Transfer Family, consulte Edición de los protocolos de transferencia de archivos en la Guía del usuario de AWS Transfer Family.

[Transfer.3] Los conectores Transfer Family deben tener habilitado el registro

Requisitos relacionados: NIST.800-53.r5 AC-2 (12), NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 AU-9 (7) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-3 (8) NIST.800-53.r5 SI-4, NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8)

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: `AWS::Transfer::Connector`

Regla de AWS Config: transfer-connector-logging-enabled

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si el CloudWatch registro de Amazon está habilitado para un AWS Transfer Family conector. El control falla si el CloudWatch registro no está activado en el conector.

Amazon CloudWatch es un servicio de supervisión y observabilidad que proporciona visibilidad de sus AWS recursos, incluidos los AWS Transfer Family recursos. Para Transfer Family, CloudWatch proporciona auditoría y registro consolidados del progreso y los resultados del flujo de trabajo. Esto incluye varias métricas que Transfer Family define para los flujos de trabajo. Puede configurar Transfer Family para que registre automáticamente los eventos del conector CloudWatch. Para hacerlo, especifica un rol de registro para el conector. Para el rol de registro, crea un rol de IAM y una política de IAM basada en recursos que definen los permisos del rol.

Corrección

Para obtener información sobre cómo habilitar el CloudWatch registro para un conector Transfer Family, consulte Amazon CloudWatch logging for AWS Transfer Family servers en la Guía del AWS Transfer Family usuario.

[Transfer.4] Los acuerdos Transfer Family deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::Transfer::Agreement`

Regla de AWS Config: transfer-agreement-tagged

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredKeyTags`	Una lista de claves de etiqueta que no son del sistema y que se deben asignar a un recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si un AWS Transfer Family acuerdo tiene las claves de etiqueta especificadas en el `requiredKeyTags` parámetro. El control falla si el acuerdo no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas por el parámetro `requiredKeyTags`. Si no se especifican valores para el parámetro `requiredKeyTags`, el control solo verifica la existencia de una clave de etiqueta y falla si el acuerdo no tiene ninguna clave de etiqueta. El control ignora las etiquetas del sistema, que se aplican automáticamente y tienen el prefijo `aws:`.

Una etiqueta es una etiqueta que se crea y se asigna a un AWS recurso. Cada etiqueta consta de una clave de etiqueta necesaria y un valor de etiqueta opcional. Utilice etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. También pueden ayudar a identificar, organizar, buscar y filtrar recursos. También pueden ayudar a rastrear propietarios de recursos para acciones y notificaciones. También puede usar etiquetas para implementar control de acceso

basado en atributos (ABAC) como estrategia de autorización. Para obtener más información sobre estrategias ABAC, consulte Definición de permisos basados en atributos con autorización ABAC en la Guía del usuario de IAM. Para obtener más información sobre las etiquetas, consulte los AWSrecursos de etiquetado y la Guía del usuario del editor de etiquetas.

> **Note**
>
> No almacene información de identificación personal (PII) ni otra información confidencial en las etiquetas. Se puede acceder a las etiquetas desde muchos Servicios de AWS sitios. No están destinadas a usarse para datos privados o información confidencial.

Corrección

Para obtener información sobre cómo añadir etiquetas a un AWS Transfer Family acuerdo, consulte los métodos de etiquetado de recursos en la Guía del usuario de Tagging AWS Resources y Tag Editor.

[Transfer.5] Los certificados Transfer Family deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::Transfer::Certificate`

Regla de AWS Config: transfer-certificate-tagged

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredKeyTags`	Una lista de claves de etiqueta que no son del sistema y que se deben asignar a un	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que	Sin valor predeterminado

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
	recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.		cumplan los requisitos de AWS.	

Este control comprueba si un AWS Transfer Family certificado tiene las claves de etiqueta especificadas por el `requiredKeyTags` parámetro. El control falla si el certificado no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas por el parámetro `requiredKeyTags`. Si no se especifican valores para el parámetro `requiredKeyTags`, el control solo verifica la existencia de una clave de etiqueta y falla si el certificado no tiene ninguna. El control ignora las etiquetas del sistema, que se aplican automáticamente y tienen el prefijo `aws:`.

Una etiqueta es una etiqueta que se crea y se asigna a un AWS recurso. Cada etiqueta consta de una clave de etiqueta necesaria y un valor de etiqueta opcional. Utilice etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. También pueden ayudar a identificar, organizar, buscar y filtrar recursos. También pueden ayudar a rastrear propietarios de recursos para acciones y notificaciones. También puede usar etiquetas para implementar control de acceso basado en atributos (ABAC) como estrategia de autorización. Para obtener más información sobre estrategias ABAC, consulte Definición de permisos basados en atributos con autorización ABAC en la Guía del usuario de IAM. Para obtener más información sobre las etiquetas, consulte los AWSrecursos de etiquetado y la Guía del usuario del editor de etiquetas.

> **Note**
>
> No almacene información de identificación personal (PII) ni otra información confidencial en las etiquetas. Se puede acceder a las etiquetas desde muchos Servicios de AWS sitios. No están destinadas a usarse para datos privados o información confidencial.

Corrección

Para obtener información sobre cómo añadir etiquetas a un AWS Transfer Family certificado, consulte los métodos de etiquetado de recursos en la Guía del usuario de Tagging AWS Resources y Tag Editor.

[Transfer.6] Los conectores Transfer Family deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::Transfer::Connector`

Regla de AWS Config: transfer-connector-tagged

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredKeyTags`	Una lista de claves de etiqueta que no son del sistema y que se deben asignar a un recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si un AWS Transfer Family conector tiene las claves de etiqueta especificadas por el `requiredKeyTags` parámetro. El control falla si el conector no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas por el parámetro `requiredKeyTags`. Si no se especifican valores para el parámetro `requiredKeyTags`, el control solo verifica la existencia de una clave de etiqueta y falla si el conector no tiene ninguna. El control ignora las etiquetas del sistema, que se aplican automáticamente y tienen el prefijo `aws:`.

Una etiqueta es una etiqueta que se crea y se asigna a un AWS recurso. Cada etiqueta consta de una clave de etiqueta necesaria y un valor de etiqueta opcional. Utilice etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. También pueden ayudar a identificar, organizar, buscar y filtrar recursos. También pueden ayudar a rastrear propietarios de recursos para acciones y notificaciones. También puede usar etiquetas para implementar control de acceso basado en atributos (ABAC) como estrategia de autorización. Para obtener más información sobre estrategias ABAC, consulte Definición de permisos basados en atributos con autorización ABAC en la Guía del usuario de IAM. Para obtener más información sobre las etiquetas, consulte los AWSrecursos de etiquetado y la Guía del usuario del editor de etiquetas.

> **Note**
>
> No almacene información de identificación personal (PII) ni otra información confidencial en las etiquetas. Se puede acceder a las etiquetas desde muchos Servicios de AWS sitios. No están destinadas a usarse para datos privados o información confidencial.

Corrección

Para obtener información sobre cómo añadir etiquetas a un AWS Transfer Family conector, consulte los métodos de etiquetado de recursos en la Guía del usuario de Tagging AWS Resources y Tag Editor.

[Transfer.7] Los perfiles de Transfer Family deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::Transfer::Profile`

Regla de AWS Config: transfer-profile-tagged

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de CSPM de Security Hub
`requiredKeyTags`	Una lista de claves de etiqueta que no son del sistema y que se deben asignar a un recurso evaluado. Las claves de etiquetas distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan los requisitos de AWS.	Sin valor predeterminado

Este control comprueba si un AWS Transfer Family perfil tiene las claves de etiqueta especificadas por el `requiredKeyTags` parámetro. El control falla si el perfil no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas por el parámetro `requiredKeyTags`. Si no se especifican valores para el parámetro `requiredKeyTags`, el control solo verifica la existencia de una clave de etiqueta y falla si el perfil no tiene ninguna. El control ignora las etiquetas del sistema, que se aplican automáticamente y tienen el prefijo `aws:`. El control evalúa perfiles locales y perfiles de socios.

Una etiqueta es una etiqueta que se crea y se asigna a un AWS recurso. Cada etiqueta consta de una clave de etiqueta necesaria y un valor de etiqueta opcional. Utilice etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. También pueden ayudar a identificar, organizar, buscar y filtrar recursos. También pueden ayudar a rastrear propietarios de recursos para acciones y notificaciones. También puede usar etiquetas para implementar control de acceso basado en atributos (ABAC) como estrategia de autorización. Para obtener más información sobre estrategias ABAC, consulte Definición de permisos basados en atributos con autorización ABAC en la Guía del usuario de IAM. Para obtener más información sobre las etiquetas, consulte los AWSrecursos de etiquetado y la Guía del usuario del editor de etiquetas.

> **Note**
>
> No almacene información de identificación personal (PII) ni otra información confidencial en las etiquetas. Se puede acceder a las etiquetas desde muchos Servicios de AWS sitios. No están destinadas a usarse para datos privados o información confidencial.

Corrección

Para obtener información sobre cómo añadir etiquetas a un AWS Transfer Family perfil, consulte los métodos de etiquetado de recursos en la Guía del usuario de Tagging AWS Resources y Tag Editor.

Controles CSPM de Security Hub paraAWS WAF

Estos AWS Security Hub CSPM controles evalúan el AWS WAF servicio y los recursos. Es posible que los controles no estén disponibles en todosRegiones de AWS. Para obtener más información, consulte Disponibilidad de los controles por región.

[WAF.1]AWS WAFEl registro de ACL web global clásico debe estar habilitado

Requisitos relacionados: NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2 NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), (9) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 NIST.800-53.r5 SI-7 (8), PCI DSS v4.0. 1/104.4.2

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: `AWS::WAF::WebACL`

Regla de AWS Config: `waf-classic-logging-enabled`

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si el registro está habilitado para una ACL web AWS WAF global. Este control falla si el registro no está habilitado para la ACL web.

El registro es una parte importante del mantenimiento de la confiabilidad, la disponibilidad y el rendimiento de AWS WAF todo el mundo. Es un requisito empresarial y de conformidad en muchas organizaciones, y permite solucionar problemas de comportamiento de las aplicaciones. También proporciona información detallada sobre el tráfico que analiza la ACL web a la que se conecta AWS WAF.

Corrección

Para habilitar el registro de una ACL AWS WAF web, consulte Registrar la información del tráfico de una ACL web en la Guía para AWS WAF desarrolladores.

[WAF.2]AWS WAFLas reglas regionales clásicas deben tener al menos una condición

Requisitos relacionados: NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (21)

Categoría: Proteger - Configuración de red segura

Gravedad: media

Tipo de recurso: `AWS::WAFRegional::Rule`

Regla de AWS Config: `waf-regional-rule-not-empty`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una regla AWS WAF regional tiene al menos una condición. El control falla si no hay condiciones presentes en una regla.

Una regla de WAF Regional puede contener varias condiciones. Las condiciones de la regla permiten inspeccionar el tráfico y realizar una acción definida (permitir, bloquear o contar). Sin ninguna condición, el tráfico pasa sin inspección. Una regla de WAF Regional sin condiciones, pero con un nombre o etiqueta que sugiera permitir, bloquear o contar, podría llevar a suponer erróneamente que se está produciendo una de esas acciones.

Corrección

Para añadir una condición a una regla vacía, consulta Añadir y eliminar condiciones en una regla en la Guía para desarrolladores de AWS WAF.

[WAF.3]AWS WAFLos grupos de reglas regionales clásicos deben tener al menos una regla

Requisitos relacionados: NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (21)

Categoría: Proteger - Configuración de red segura

Gravedad: media

Tipo de recurso: `AWS::WAFRegional::RuleGroup`

Regla de AWS Config: `waf-regional-rulegroup-not-empty`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un grupo de reglas AWS WAF regionales tiene al menos una regla. El control falla si no hay reglas presentes en un grupo de reglas.

Un grupo de reglas de WAF Regionales puede contener varias reglas. Las condiciones de la regla permiten inspeccionar el tráfico y realizar una acción definida (permitir, bloquear o contar). Sin ninguna regla, el tráfico pasa sin inspección. Un grupo de reglas de WAF Regionales sin reglas, pero con un nombre o etiqueta que sugiera permitir, bloquear o contar, podría llevar a suponer erróneamente que se está produciendo una de esas acciones.

Corrección

Para agregar reglas y condiciones de reglas a un grupo de reglas vacío, consulte Agregar y eliminar reglas de un grupo de reglas AWS WAF clásico y Agregar y eliminar condiciones en una regla en la Guía para AWS WAF desarrolladores.

[WAF.4]AWS WAFLas ACL web regionales clásicas deben tener al menos una regla o grupo de reglas

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Categoría: Proteger - Configuración de red segura

Gravedad: media

Tipo de recurso: `AWS::WAFRegional::WebACL`

Regla de AWS Config: `waf-regional-webacl-not-empty`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una ACL AWS WAF Classic Regional web contiene reglas de WAF o grupos de reglas de WAF. Este control falla si una ACL web no contiene ninguna regla o grupo de reglas de WAF.

Una ACL web de WAF Regional puede contener una colección de reglas y grupos de reglas que inspeccionan y controlan las solicitudes web. Si una ACL web está vacía, el tráfico web puede pasar sin que el WAF lo detecte ni actúe en consecuencia, según la acción predeterminada.

Corrección

Para agregar reglas o grupos de reglas a una ACL web regional AWS WAF clásica vacía, consulte Edición de una ACL web en la Guía para AWS WAFdesarrolladores.

[WAF.6]AWS WAFLas reglas globales clásicas deben tener al menos una condición

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Categoría: Proteger - Configuración de red segura

Gravedad: media

Tipo de recurso: `AWS::WAF::Rule`

Regla de AWS Config: `waf-global-rule-not-empty`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una regla AWS WAF global contiene alguna condición. El control falla si no hay condiciones presentes en una regla.

Una regla de WAF global puede contener varias condiciones. Las condiciones de una regla permiten inspeccionar el tráfico y realizar una acción definida (permitir, bloquear o contar). Sin ninguna condición, el tráfico pasa sin inspección. Una regla de WAF global sin condiciones, pero con un nombre o etiqueta que sugiera permitir, bloquear o contar, podría llevar a suponer erróneamente que se está produciendo una de esas acciones.

Corrección

Para obtener instrucciones sobre cómo crear una regla y añadir condiciones, consulte Creación de una regla y adición de condiciones en la Guía para desarrolladores de AWS WAF.

[WAF.7]AWS WAFLos grupos de reglas globales clásicos deben tener al menos una regla

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Categoría: Proteger - Configuración de red segura

Gravedad: media

Tipo de recurso: `AWS::WAF::RuleGroup`

Regla de AWS Config: `waf-global-rulegroup-not-empty`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un grupo de reglas AWS WAF globales tiene al menos una regla. El control falla si no hay reglas presentes en un grupo de reglas.

Un grupo de reglas globales de WAF puede contener varias reglas. Las condiciones de la regla permiten inspeccionar el tráfico y realizar una acción definida (permitir, bloquear o contar). Sin ninguna regla, el tráfico pasa sin inspección. Un grupo de reglas globales de la WAF sin reglas, pero con un nombre o etiqueta que sugiera permitir, bloquear o contar, podría llevar a suponer erróneamente que se está produciendo una de esas acciones.

Corrección

Para obtener instrucciones sobre cómo agregar una regla a un grupo de reglas, consulte Creación de un grupo de reglas AWS WAF clásico en la Guía para AWS WAF desarrolladores.

[WAF.8]AWS WAFLas ACL web globales clásicas deben tener al menos una regla o grupo de reglas

Requisitos relacionados: NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (21)

Categoría: Proteger - Configuración de red segura

Gravedad: media

Tipo de recurso: `AWS::WAF::WebACL`

Regla de AWS Config: `waf-global-webacl-not-empty`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una ACL web AWS WAF global contiene al menos una regla de WAF o un grupo de reglas de WAF. El control falla si una ACL web no contiene ninguna regla o grupo de reglas de WAF.

Una ACL web global de WAF puede contener una colección de reglas y grupos de reglas que inspeccionan y controlan las solicitudes web. Si una ACL web está vacía, el tráfico web puede pasar sin que el WAF lo detecte ni actúe en consecuencia, según la acción predeterminada.

Corrección

Para agregar reglas o grupos de reglas a una ACL web AWS WAF global vacía, consulte Edición de una ACL web en la Guía para AWS WAFdesarrolladores. Para Filtrar, elija Global (CloudFront).

[WAF.10]AWS WAFLas ACL web deben tener al menos una regla o grupo de reglas

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Categoría: Proteger - Configuración de red segura

Gravedad: media

Tipo de recurso: `AWS::WAFv2::WebACL`

Regla de AWS Config: `wafv2-webacl-not-empty`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una lista de control de acceso web (ACL web) de la AWS WAF versión 2 contiene al menos una regla o un grupo de reglas. El control falla si una ACL web no contiene ninguna regla o grupo de reglas.

Una ACL web le proporciona un control detallado de todas las solicitudes web HTTP(S) a las que responde su recurso protegido. Una ACL web debe contener una colección de reglas y grupos de reglas que inspeccionen y controlen las solicitudes web. Si una ACL web está vacía, el tráfico web puede pasar sin que se detecte ni se actúe en consecuencia, AWS WAF según la acción predeterminada.

Corrección

Para añadir reglas o grupos de reglas a una ACL web de WAFV2 vacía, consulte Edición de una ACL web en la Guía para desarrolladores de AWS WAF.

[WAF.11]AWS WAFEl registro de ACL web debe estar habilitado

Requisitos relacionados: NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2 NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), (10) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SC-7 NIST.800-53.r5 SI-7 (8), PCI DSS v4.0. 1/104.4.2

Categoría: Identificar - Registro

Gravedad: baja

Tipo de recurso: `AWS::WAFv2::WebACL`

AWS Configregla: **`wafv2-logging-enabled`**

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si el registro está activado para una lista de control de acceso web (ACL web) de la AWS WAF versión 2. Este control falla si el registro está desactivado para la ACL web.

> **Note**
>
> Este control no comprueba si el registro de ACL AWS WAF web está habilitado para una cuenta a través de Amazon Security Lake.

El registro mantiene la confiabilidad, la disponibilidad y el rendimiento deAWS WAF. Además, el registro es un requisito empresarial y de conformidad en muchas organizaciones. Al registrar el tráfico analizado por su ACL web, puede solucionar problemas de comportamiento de las aplicaciones.

Corrección

Para activar el registro de una ACL AWS WAF web, consulte Administrar el registro de una ACL web en la Guía para AWS WAF desarrolladores.

[WAF.12]AWS WAFlas reglas deben tener CloudWatch las métricas habilitadas

Requisitos relacionados: NIST.800-53.r5 AC-4 (26),, NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2 NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4),

(10) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SC-7 NIST.800-53.r5 SI-7 (8), NIST.800-171.r2 3.14.6, 3.14.7 NIST.800-171.r2

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: `AWS::WAFv2::RuleGroup`

AWS Configregla: **`wafv2-rulegroup-logging-enabled`**

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una AWS WAF regla o un grupo de reglas tienen habilitadas CloudWatch las métricas de Amazon. El control falla si la regla o el grupo de reglas no tienen CloudWatch las métricas habilitadas.

La configuración de las CloudWatch métricas de AWS WAF las reglas y los grupos de reglas proporciona visibilidad del flujo de tráfico. Puede ver qué reglas de ACL se activan y qué solicitudes se aceptan y bloquean. Esta visibilidad puede ayudarle a identificar actividades maliciosas en los recursos asociados.

Corrección

Para habilitar CloudWatch las métricas en un grupo de AWS WAF reglas, invoca la UpdateRuleGroupAPI. Para habilitar CloudWatch las métricas en una AWS WAF regla, invoca la API UpdateWebACL. Establezca el campo `CloudWatchMetricsEnabled` como `true`. Cuando utiliza la AWS WAF consola para crear reglas o grupos de reglas, las CloudWatch métricas se habilitan automáticamente.

Controles CSPM de Security Hub para WorkSpaces

Estos AWS Security Hub CSPM controles evalúan el WorkSpaces servicio y los recursos de Amazon.

Es posible que estos controles no estén disponibles en todosRegiones de AWS. Para obtener más información, consulte Disponibilidad de los controles por región.

[WorkSpaces.1] los volúmenes de WorkSpaces usuarios deben cifrarse en reposo

Categoría: Proteger > Protección de datos > Cifrado de datos en reposo

Gravedad: media

Tipo de recurso: `AWS::WorkSpaces::Workspace`

Regla de AWS Config: `workspaces-user-volume-encryption-enabled`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un volumen de usuarios de Amazon WorkSpaces WorkSpace está cifrado en reposo. El control falla si el volumen WorkSpace de usuarios no está cifrado en reposo.

Los datos en reposo hacen referencia a los datos que se almacenan en un almacenamiento persistente y no volátil durante cualquier periodo de tiempo. El cifrado de datos en reposo permite proteger la confidencialidad de los datos, lo que reduce el riesgo de que un usuario no autorizado pueda acceder a ellos.

Corrección

Para cifrar un volumen de WorkSpaces usuarios, consulte Cifrar a WorkSpace en la Guía de WorkSpaces administración de Amazon.

[WorkSpaces.2] los volúmenes WorkSpaces raíz deben cifrarse en reposo

Categoría: Proteger > Protección de datos > Cifrado de datos en reposo

Gravedad: media

Tipo de recurso: `AWS::WorkSpaces::Workspace`

Regla de AWS Config: `workspaces-root-volume-encryption-enabled`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un volumen raíz de Amazon WorkSpaces WorkSpace está cifrado en reposo. El control falla si el volumen WorkSpace raíz no está cifrado en reposo.

Los datos en reposo hacen referencia a los datos que se almacenan en un almacenamiento persistente y no volátil durante cualquier periodo de tiempo. El cifrado de datos en reposo permite proteger la confidencialidad de los datos, lo que reduce el riesgo de que un usuario no autorizado pueda acceder a ellos.

Corrección

Para cifrar un volumen WorkSpaces raíz, consulte Cifrar a WorkSpace en la Guía de WorkSpaces administración de Amazon.

Permisos necesarios para configurar controles en el CSPM de Security Hub

Para ver información sobre los controles de seguridad y habilitar y deshabilitar los controles de seguridad en los estándares, la función AWS Identity and Access Management (IAM) que utilice para acceder al AWS Security Hub CSPM necesita permisos para realizar las siguientes operaciones de la API CSPM de Security Hub.

Para obtener los permisos necesarios, puede utilizar las políticas administrada por el CSPM de Security Hub. Como alternativa, puede actualizar las políticas de IAM personalizadas para incluir permisos para estas acciones.

- BatchGetSecurityControls— Devuelve información sobre un lote de controles de seguridad para la cuenta corriente y. Región de AWS
- ListSecurityControlDefinitions: Devuelve información sobre los controles de seguridad que se aplican a un estándar específico.
- ListStandardsControlAssociations: Identifica si un control de seguridad está activado o desactivado actualmente en cada uno de los estándares habilitados de la cuenta.
- BatchGetStandardsControlAssociations: En el caso de un lote de controles de seguridad, identifica si cada control está actualmente activado o desactivado según un estándar específico.
- BatchUpdateStandardsControlAssociations: Se utiliza para habilitar un control de seguridad en los estándares que incluyen el control, o para deshabilitar un control en los estándares. Se trata de un sustituto por lotes de la operación `UpdateStandardsControl` existente.
- BatchUpdateStandardsControlAssociations: se utiliza para habilitar o deshabilitar un lote de controles de seguridad en los estándares que incluyen los controles. Se trata de un sustituto por lotes de la operación `UpdateStandardsControl` existente.
- UpdateStandardsControl: se utiliza para habilitar o deshabilitar un único control de seguridad en los estándares que incluyen el control
- DescribeStandardsControl: devuelve detalles sobre los controles de seguridad específicos.

Además de las API anteriores, debe añadir permisos para llamar `BatchGetControlEvaluations` a su rol de IAM. Este permiso es necesario para ver el estado de habilitación y cumplimiento

de un control, el recuento de sus resultados y la puntuación general de seguridad de los controles en la consola del CSPM de Security Hub. Como solo se llama a la consola`BatchGetControlEvaluations`, este permiso no corresponde directamente a las API o AWS CLI comandos de CSPM de Security Hub documentados públicamente.

Habilitación de controles en el CSPM de Security Hub

En AWS Security Hub CSPM, un control es una salvaguarda dentro de un estándar de seguridad que ayuda a una organización a proteger la confidencialidad, la integridad y la disponibilidad de su información. Cada control CSPM de Security Hub está relacionado con un recurso específico. AWS Cuando habilita un control, el CSPM de Security Hub comienza a ejecutar comprobaciones de seguridad para el control, así como a generar resultados para este. Además, el CSPM de Security Hub tiene en cuenta todos los controles habilitados cuando calcula las puntuaciones de seguridad.

Puede elegir habilitar un control en todos los estándares de seguridad a los que se aplica. Como alternativa, puede configurar el estado de habilitación de forma diferente en los distintos estándares. Recomendamos la opción anterior, en la que el estado de habilitación de un control se alinea en todos los estándares habilitados. Para obtener instrucciones sobre cómo habilitar un control en todos los estándares a los que se aplica, consulte Habilitación de un control en todos los estándares. Para obtener instrucciones sobre cómo habilitar un control en un estándar específico, consulte Habilitación de un control en un estándar específico.

Si habilita la agregación entre regiones e inicia sesión en una región de agregación, la consola del CSPM de Security Hub muestra los controles que están disponibles en al menos una región vinculada. Si un control está disponible en una región vinculada, pero no en la región de agregación, no podrá habilitar ni deshabilitar ese control desde la región de agregación.

Puede habilitar y deshabilitar los controles en cada región mediante la consola CSPM de Security Hub, la API CSPM de Security Hub o. AWS CLI

Las instrucciones para habilitar y deshabilitar los controles varían en función de si se utiliza o no la configuración centralizada. En este tema se describen las diferencias. La configuración central está disponible para los usuarios que integran Security Hub CSPM y. AWS Organizations Recomendamos utilizar la configuración centralizada para simplificar el proceso de habilitación y deshabilitación de los controles en entornos de varias cuentas y regiones. Si utiliza la configuración centralizada, puede habilitar un control en varias cuentas y regiones mediante el uso de políticas de configuración. Si no utiliza la configuración centralizada, debe habilitar un control por separado en cada cuenta y región.

Habilitación de un control en todos los estándares

Recomendamos habilitar un control CSPM de AWS Security Hub en todos los estándares a los que se aplica el control. Si activa los resultados de control consolidados, recibirá un resultado por comprobación de control, incluso si un control pertenece a más de un estándar.

Cross-standard habilitación en entornos con varias cuentas y regiones

Para habilitar el control de seguridad en varias redes Regiones de AWS, debe Cuentas de AWS iniciar sesión en la cuenta de administrador delegada de CSPM de Security Hub y utilizar la configuración central. ???

En la configuración centralizada, el administrador delegado puede crear políticas de configuración del CSPM de Security Hub que habilitan los controles especificados en los estándares habilitados. A continuación, puede asociar la política de configuración a cuentas y unidades organizativas (OU) específicas o a la raíz. La política de configuración entra en vigencia en su región de origen (también denominada región de agregación) y en todas las regiones vinculadas.

Las políticas de configuración pueden personalizarse. Por ejemplo, puede optar por habilitar todos los controles en una unidad organizativa y puede optar por habilitar solo los controles de Amazon Elastic Compute Cloud (EC2) en otra unidad organizativa. El nivel de granularidad depende de los objetivos previstos en materia de cobertura de seguridad en su organización. Para instrucciones sobre cómo crear una política de configuración que habilite controles especificados en estándares, consulte Creación y asociación de políticas de configuración.

> **Note**
>
> El administrador delegado puede crear políticas de configuración para administrar los controles en todos los estándares excepto en el Service-Managed estándar:. AWS Control Tower Los controles de este estándar deben configurarse en el AWS Control Tower servicio.

Si desea que algunas cuentas configuren sus propios controles en lugar de hacerlo el administrador delegado, el administrador delegado puede designar esas cuentas como autoadministradas. Self-managed las cuentas deben configurar los controles por separado en cada región.

Cross-standard activación en una sola cuenta y región

Si no utiliza la configuración centralizada o tiene una cuenta autoadministrada, no podrá utilizar las políticas de configuración para habilitar de manera centralizada los controles en varias cuentas y

regiones. Sin embargo, puede seguir estos pasos para habilitar un control en una sola cuenta y región.

Security Hub CSPM console

Para habilitar un control en los estándares en una cuenta y región

1. Abra la consola AWS CSPM de Security Hub en. https://console.aws.amazon.com/securityhub/
2. En el panel de navegación, elija Controles.
3. Seleccione la pestaña Deshabilitado.
4. Seleccione la opción situada junto a un control.
5. Seleccione Habilitar el control (esta opción no aparece en los controles que ya están activados).
6. Repítalo en cada región en la que quiere habilitar el control.

Security Hub CSPM API

Para habilitar un control en los estándares en una cuenta y región

1. Invoque la API ListStandardsControlAssociations. Proporcione un ID de control de seguridad.

   Ejemplo de solicitud:

   ```
   {
       "SecurityControlId": "IAM.1"
   }
   ```

2. Invoque la API BatchUpdateStandardsControlAssociations. Proporcione el nombre de recurso de Amazon (ARN) de cualquier estándar en el que el control no esté habilitado. Para obtener los ARN estándar, ejecute `DescribeStandards`.
3. Defina el parámetro `AssociationStatus` equivalente a `ENABLED`. Si sigue estos pasos para un control que ya está habilitado, la API devuelve una respuesta con el código de estado HTTP 200.

   Ejemplo de solicitud:

   ```
   {
   ```

```
    "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
 "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0", "AssociationStatus": "ENABLED"}, {"SecurityControlId": "IAM.1",
 "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-
best-practices/v/1.0.0", "AssociationStatus": "ENABLED"}]
}
```

4. Repítalo en cada región en la que quiere habilitar el control.

AWS CLI

Para habilitar un control en los estándares en una cuenta y región

1. Ejecute el comando list-standards-control-associations. Proporcione un ID de control de seguridad.

```
aws securityhub  --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

2. Ejecute el comando batch-update-standards-control-associations. Proporcione el nombre de recurso de Amazon (ARN) de cualquier estándar en el que el control no esté habilitado. Para obtener los ARN estándar, ejecute el comando `describe-standards`.
3. Defina el parámetro `AssociationStatus` equivalente a `ENABLED`. Si sigue estos pasos para un control que ya está habilitado, el comando devuelve una respuesta con el código de estado HTTP 200.

```
aws securityhub  --region us-east-1 batch-update-standards-control-associations
 --standards-control-association-updates '[{"SecurityControlId": "CloudTrail.1",
 "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0", "AssociationStatus": "ENABLED"}, {"SecurityControlId": "CloudTrail.1",
 "StandardsArn": "arn:aws:securityhub:::standards/cis-aws-foundations-benchmark/
v/1.4.0", "AssociationStatus": "ENABLED"}]'
```

4. Repítalo en cada región en la que quiere habilitar el control.

Habilitación de un control en un estándar específico

Cuando habilita un estándar en AWS Security Hub CSPM, todos los controles que se le aplican se habilitan automáticamente en ese estándar (la excepción son los estándares administrados por

servicios). Puede deshabilitar y rehabilitar controles específicos dentro del estándar. Sin embargo, recomendamos alinear el estado de habilitación de un control en todos los estándares habilitados. Para obtener instrucciones sobre cómo habilitar un control en todos los estándares, consulte Habilitación de un control en todos los estándares.

La página de detalles de un estándar contiene la lista de los controles aplicables al estándar e información sobre los controles que están actualmente habilitados y deshabilitados en ese estándar.

En la página de detalles de los estándares, también puede habilitar controles en estándares específicos. Debe habilitar los controles de estándares específicos por separado en cada uno de ellos. Cuenta de AWS Región de AWS Cuando habilita un control en estándares específicos, solo afecta a la cuenta y a la región actuales.

Para habilitar un control en un estándar, primero debe habilitar al menos un estándar al que se aplique el control. Para obtener instrucciones sobre cómo habilitar un estándar, consulte Habilitación de un estándar de seguridad. Cuando habilita un control en uno o más estándares, el CSPM de Security Hub comienza a generar resultados para ese control. El CSPM de Security Hub incluye el estado del control en el cálculo del puntaje de seguridad general y de los puntajes de seguridad de los estándares. Incluso si habilita un control en varios estándares, recibirá un único resultado por control de seguridad en todos los estándares si activa los resultados de control consolidados. Para obtener más información, consulte Resultados de control consolidados.

Para habilitar un control en un estándar, el control debe estar disponible en su región actual. Para obtener más información, consulte Disponibilidad de controles por región.

Siga estos pasos para habilitar un control del CSPM de Security Hub en un estándar específico. En lugar de los siguientes pasos, también puede usar la acción de la API de `UpdateStandardsControl` para habilitar los controles en un estándar específico. Para obtener instrucciones sobre cómo habilitar un control en todos los estándares, consulte Cross-standard activación en una sola cuenta y región.

Security Hub CSPM console

Habilitación de un control en un estándar específico

1. Abra la consola CSPM de AWS Security Hub en. https://console.aws.amazon.com/securityhub/
2. Elija Estándares de seguridad en el panel de navegación.
3. Seleccione Ver resultados para el estándar correspondiente.

4. Seleccione un control.
5. Seleccione Habilitar el control (esta opción no aparece en los controles que ya están activados). Confirme seleccionando Habilitar.

Security Hub CSPM API

Habilitación de un control en un estándar específico

1. Ejecute `ListSecurityControlDefinitions` y proporcione un ARN estándar para obtener una lista de los controles disponibles para un estándar específico. Para obtener un ARN estándar, ejecute `DescribeStandards`. Esta API devuelve los identificadores de control de seguridad independientes del estándar, no los identificadores de control específicos del estándar.

   Ejemplo de solicitud:

   ```
   {
       "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/v/1.0.0"
   }
   ```

2. Ejecute `ListStandardsControlAssociations` y proporcione un identificador de control específico para devolver el estado de activación actual de un control en cada estándar.

   Ejemplo de solicitud:

   ```
   {
       "SecurityControlId": "IAM.1"
   }
   ```

3. Ejecute `BatchUpdateStandardsControlAssociations`. Indique el ARN del estándar en el que desee habilitar el control.
4. Defina el parámetro `AssociationStatus` equivalente a `ENABLED`.

   Ejemplo de solicitud:

   ```
   {
       "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
    "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0", "AssociationStatus": "ENABLED"}]
   ```

```
}
```

AWS CLI

Habilitación de un control en un estándar específico

1. Ejecute el comando `list-security-control-definitions` y proporcione un ARN estándar para obtener una lista de los controles disponibles para un estándar específico. Para obtener un ARN estándar, ejecute `describe-standards`. Este comando devuelve los identificadores de control de seguridad independientes del estándar, no los identificadores de control específicos del estándar.

```
aws securityhub --region us-east-1 list-security-control-definitions --
standards-arn "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0"
```

2. Ejecute el comando `list-standards-control-associations` y proporcione un identificador de control específico para devolver el estado de habilitación actual de un control en cada estándar.

```
aws securityhub  --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

3. Ejecute el comando `batch-update-standards-control-associations`. Indique el ARN del estándar en el que desee habilitar el control.
4. Defina el parámetro `AssociationStatus` equivalente a `ENABLED`.

```
aws securityhub  --region us-east-1 batch-update-standards-control-associations
 --standards-control-association-updates '[{"SecurityControlId": "CloudTrail.1",
 "StandardsArn": "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0", "AssociationStatus": "ENABLED"}]'
```

Habilitación de nuevos controles en estándares habilitados automáticamente

AWSSecurity Hub CSPM publica periódicamente nuevos controles y los añade a uno o más estándares. Puede elegir si quiere habilitar automáticamente nuevos controles en sus estándares habilitados.

Recomendamos usar la configuración centralizada del CSPM de Security Hub para habilitar automáticamente los nuevos controles de seguridad. Puede crear políticas de configuración que incluyan una lista de controles que se deben deshabilitar en los estándares. Todos los demás controles, incluidos los recién lanzados, están habilitados de manera predeterminada. Como alternativa, puede crear políticas que incluyan una lista de controles que se deben habilitar en los estándares. Todos los demás controles, incluidos los recién lanzados, están deshabilitados de manera predeterminada. Para obtener más información, consulte Descripción de la configuración central en el CSPM de Security Hub.

El CSPM de Security Hub no habilita controles nuevos cuando se agregan a un estándar que no haya habilitado.

Las siguientes instrucciones solo se aplican si no utiliza la configuración centralizada.

Elija el método de acceso que prefiera y siga los pasos para activar automáticamente los nuevos controles en los estándares habilitados.

> **Note**
>
> Cuando habilita controles nuevos de manera automática según estas instrucciones, podrá interactuar con los controles en la consola y también mediante programación inmediatamente después de su publicación. Sin embargo, los controles habilitados automáticamente tienen un estado predeterminado temporal de Desactivado. El CSPM de Security Hub puede tardar varios días en procesar la publicación de un control y asignarlo con el estado Habilitado en la cuenta. Durante este periodo de procesamiento, puede habilitar o desactivar manualmente cualquier control, y el CSPM de Security Hub mantendrá la selección que realice, independientemente de si tiene activada la habilitación automática de controles.

Security Hub CSPM console

Habilitación automática de nuevos controles

1. Abra la consola CSPM de AWS Security Hub en. https://console.aws.amazon.com/securityhub/
2. En el panel de navegación, elija Configuración y luego elija la pestaña General.
3. En Controles, seleccione Editar.
4. Active los Auto-enable nuevos controles en los estándares habilitados.

5. Seleccione Save.

Security Hub CSPM API

Habilitación automática de nuevos controles

1. Ejecute `UpdateSecurityHubConfiguration`.
2. Para activar automáticamente los nuevos controles para los estándares habilitados, establezca `AutoEnableControls` como `true`. Si no desea habilitar automáticamente los nuevos controles, establezca `AutoEnableControls` como falso.

AWS CLI

Habilitación automática de nuevos controles

1. Ejecute el comando `update-security-hub-configuration`.
2. Para activar automáticamente los nuevos controles para los estándares habilitados, especifique `--auto-enable-controls`. Si no desea habilitar automáticamente los nuevos controles, especifique `--no-auto-enable-controls`.

```
aws securityhub update-security-hub-configuration --auto-enable-controls | --no-auto-enable-controls
```

Comando de ejemplo:

```
aws securityhub update-security-hub-configuration --auto-enable-controls
```

Si no habilita automáticamente los controles nuevos, debe habilitarlos manualmente. Para obtener instrucciones, consulte Habilitación de controles en el CSPM de Security Hub.

Desactivación de controles en el CSPM de Security Hub

Para reducir el ruido de resultados, puede resultar útil desactivar los controles que no sean relevantes para el entorno. En AWS Security Hub CSPM, puede deshabilitar un control para todos los estándares de seguridad o solo para estándares específicos.

Si desactiva un control en todos los estándares, sucede lo siguiente:

- Los controles de seguridad del control ya no se realizan.
- No se generan resultados adicionales para el control.
- Los resultados existentes se dejan de actualizar para el control.
- Los resultados existentes del control se archivan de forma automática, por lo general dentro de un periodo de 3 a 5 días, según el mejor esfuerzo.
- El CSPM de Security Hub elimina cualquier AWS Config regla relacionada que haya creado para el control.

Si desactiva un control solo en estándares específicos, el CSPM de Security Hub deja de ejecutar las comprobaciones de seguridad para el control únicamente en esos estándares. Esto también excluye el control de los cálculos del puntaje de seguridad para cada uno de esos estándares. Si el control está habilitado en otros estándares, el CSPM de Security Hub retiene la regla asociada de AWS Config , si aplica, y continúa con la ejecución de las comprobaciones de seguridad para el control en los demás estándares. El CSPM de Security Hub también incluye el control cuando calcula el puntaje de seguridad para cada uno de los demás estándares, lo cual afecta el puntaje de seguridad general.

Si desactiva un estándar, todos los controles que se aplican al estándar se desactivan de forma automática para ese estándar. Sin embargo, los controles pueden permanecer habilitados en otros estándares. Cuando desactiva un estándar, el CSPM de Security Hub no lleva un seguimiento de qué controles se desactivaron para el estándar. En consecuencia, si vuelve a habilitar el mismo estándar, todos los controles que se aplican a él se habilitan de forma automática. Para obtener información acerca de la desactivación de un estándar, consulte Desactivación de un estándar.

La desactivación de un control no constituye una acción permanente. Suponga que desactiva un control y luego habilita un estándar que incluye ese control. El control queda habilitado para ese estándar. Cuando habilita un estándar en el CSPM de Security Hub, todos los controles que se aplican al estándar se habilitan de forma automática. Para obtener información sobre cómo se habilita un estándar, consulte Habilitación de un estándar.

Temas

- Deshabilitar un control en todos los estándares
- Deshabilitación de un control en un estándar específico
- Controles sugeridos para desactivar en el CSPM de Security Hub

Deshabilitar un control en todos los estándares

Recomendamos deshabilitar un control CSPM AWS de Security Hub en todos los estándares para mantener la alineación en toda la organización. Si usted desactiva un control solo en estándares específicos, aún recibirá resultados para el control si este está habilitado en otros estándares.

Cross-standard la desactivación en varias cuentas y regiones

Para deshabilitar un control de seguridad en varios anuncios Cuentas de AWS Regiones de AWS, debe usar una configuración central.

Cuando se usa la configuración centralizada, el administrador delegado puede crear políticas de configuración del CSPM de Security Hub que desactivan los controles especificados en los estándares habilitados. A continuación, puede asociar la política de configuración a cuentas específicas, unidades organizativas o a la raíz. La política de configuración entra en vigencia en su región de origen (también denominada región de agregación) y en todas las regiones vinculadas.

Las políticas de configuración pueden personalizarse. Por ejemplo, puede optar por deshabilitar todos los AWS CloudTrail controles de una OU y también puede optar por deshabilitar todos los controles de IAM de otra OU. El nivel de granularidad depende de los objetivos previstos en materia de cobertura de seguridad en su organización. Para instrucciones sobre cómo crear una política de configuración que deshabilite controles especificados en estándares, consulte Creación y asociación de políticas de configuración.

> **Note**
>
> El administrador delegado puede crear políticas de configuración para administrar los controles en todos los estándares excepto en el Service-Managed estándar: AWS Control Tower. Los controles de este estándar deben configurarse en el AWS Control Tower servicio.

Si desea que algunas cuentas configuren sus propios controles en lugar de hacerlo el administrador delegado, el administrador delegado puede designar esas cuentas como autoadministradas. Self-managed las cuentas deben configurar los controles por separado en cada región.

Cross-standard desactivación en una sola cuenta y región

Si no utiliza la configuración centralizada o tiene una cuenta autoadministrada, no podrá utilizar las políticas de configuración para deshabilitar de manera centralizada los controles en varias cuentas y regiones. Sin embargo, puede desactivar un control en una sola cuenta y región.

Security Hub CSPM console

Deshabilitación de un control en los estándares en una cuenta y región

1. Abra la consola AWS CSPM de Security Hub en. https://console.aws.amazon.com/securityhub/
2. En el panel de navegación, elija Controles.
3. Seleccione la opción situada junto a un control.
4. Elija la opción Desactivar el control. Esta opción no aparece para un control que ya esté desactivado.
5. Seleccione un motivo para deshabilitar el control y confírmelo seleccionando Deshabilitar.
6. Repítalo en cada región en la que quiere deshabilitar el control.

Security Hub CSPM API

Deshabilitación de un control en los estándares en una cuenta y región

1. Invoque la API ListStandardsControlAssociations. Proporcione un ID de control de seguridad.

   Ejemplo de solicitud:

   ```
   {
       "SecurityControlId": "IAM.1"
   }
   ```

2. Invoque la API BatchUpdateStandardsControlAssociations. Proporcione el ARN de cualquier estándar en el que esté habilitado el control. Para obtener los ARN estándar, ejecute `DescribeStandards`.
3. Defina el parámetro `AssociationStatus` equivalente a `DISABLED`. Si sigue estos pasos para un control que ya está deshabilitado, la API devuelve una respuesta con el código de estado HTTP 200.

   Ejemplo de solicitud:

   ```
   {
       "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
    "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-
   benchmark/v/1.2.0", "AssociationStatus": "DISABLED", "UpdatedReason": "Not
    applicable to environment"}, {"SecurityControlId": "IAM.1", "StandardsArn":
   ```

```
 "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/
v/1.0.0", "AssociationStatus": "DISABLED", "UpdatedReason": "Not applicable to
 environment"}}]
}
```

4. Repítalo en cada región en la que quiere deshabilitar el control.

AWS CLI

Deshabilitación de un control en los estándares en una cuenta y región

1. Ejecute el comando list-standards-control-associations. Proporcione un ID de control de seguridad.

```
aws securityhub  --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

2. Ejecute el comando batch-update-standards-control-associations. Proporcione el ARN de cualquier estándar en el que esté habilitado el control. Para obtener los ARN estándar, ejecute el comando `describe-standards`.
3. Defina el parámetro `AssociationStatus` equivalente a `DISABLED`. Si sigue estos pasos para un control que ya está deshabilitado, el comando devuelve una respuesta con el código de estado HTTP 200.

```
aws securityhub  --region us-east-1 batch-update-standards-control-associations
 --standards-control-association-updates '[{"SecurityControlId": "CloudTrail.1",
 "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0", "AssociationStatus": "DISABLED", "UpdatedReason": "Not applicable
 to environment"}, {"SecurityControlId": "CloudTrail.1", "StandardsArn":
 "arn:aws:securityhub:::standards/cis-aws-foundations-benchmark/v/1.4.0",
 "AssociationStatus": "DISABLED", "UpdatedReason": "Not applicable to
 environment"}]'
```

4. Repítalo en cada región en la que quiere deshabilitar el control.

Deshabilitación de un control en un estándar específico

Puede desactivar un control solo en estándares de seguridad específicos, en lugar de hacerlo en todos los estándares. Si el control se aplica a otros estándares habilitados, AWS Security Hub CSPM

continúa realizando comprobaciones de seguridad para el control y usted continúa recibiendo los resultados del control.

Sin embargo, recomendamos alinear el estado de habilitación de un control en todos los estándares habilitados a los que se aplica el control. Para obtener información sobre cómo desactivar un control en todos los estándares a los que aplica, consulte Deshabilitar un control en todos los estándares.

En la página de detalles de los estándares, también puede desactivar los controles de un estándar específico. Debe deshabilitar los controles de estándares específicos por separado en cada uno Cuenta de AWS y. Región de AWS Cuando desactiva un control en estándares específicos, esto afecta únicamente a la cuenta y a la región actuales.

Elija el método de su preferencia y siga estos pasos para desactivar un control en uno o más estándares específicos.

Security Hub CSPM console

Deshabilitación de un control en un estándar específico

1. Abra la consola CSPM de AWS Security Hub en. https://console.aws.amazon.com/securityhub/
2. Elija Estándares de seguridad en el panel de navegación. Seleccione Ver resultados para el estándar correspondiente.
3. Seleccione un control.
4. Elija la opción Desactivar el control. Esta opción no aparece para un control que ya esté desactivado.
5. Indique el motivo para deshabilitar el control y confirme seleccionando Deshabilitar.

Security Hub CSPM API

Deshabilitación de un control en un estándar específico

1. Ejecute `ListSecurityControlDefinitions` y proporcione un ARN estándar para obtener una lista de los controles disponibles para un estándar específico. Para obtener un ARN estándar, ejecute `DescribeStandards`. Esta API devuelve los identificadores de control de seguridad independientes del estándar, no los identificadores de control específicos del estándar.

   Ejemplo de solicitud:

```
{
    "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/v/1.0.0"
}
```

2. Ejecute `ListStandardsControlAssociations` y proporcione un identificador de control específico para devolver el estado de activación actual de un control en cada estándar.

   Ejemplo de solicitud:

```
{
    "SecurityControlId": "IAM.1"
}
```

3. Ejecute `BatchUpdateStandardsControlAssociations`. Proporcione el ARN del estándar en el que desea deshabilitar el control.
4. Defina el parámetro `AssociationStatus` equivalente a `DISABLED`. Si sigue estos pasos para un control que ya está deshabilitado, la API devuelve una respuesta con el código de estado HTTP 200.

   Ejemplo de solicitud:

```
{
    "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
 "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0", "AssociationStatus": "DISABLED",  "UpdatedReason": "Not applicable to environment"}]
}
```

AWS CLI

Deshabilitación de un control en un estándar específico

1. Ejecute el comando `list-security-control-definitions` y proporcione un ARN estándar para obtener una lista de los controles disponibles para un estándar específico. Para obtener un ARN estándar, ejecute `describe-standards`. Este comando devuelve los identificadores de control de seguridad independientes del estándar, no los identificadores de control específicos del estándar.

```
aws securityhub --region us-east-1 list-security-control-definitions --
standards-arn "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0"
```

2. Ejecute el comando `list-standards-control-associations` y proporcione un identificador de control específico para devolver el estado de habilitación actual de un control en cada estándar.

```
aws securityhub  --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

3. Ejecute el comando `batch-update-standards-control-associations`. Proporcione el ARN del estándar en el que desea deshabilitar el control.
4. Defina el parámetro `AssociationStatus` equivalente a `DISABLED`. Si sigue estos pasos para un control que ya está habilitado, el comando devuelve una respuesta con el código de estado HTTP 200.

```
aws securityhub  --region us-east-1 batch-update-standards-control-
associations --standards-control-association-updates '[{"SecurityControlId":
 "CloudTrail.1", "StandardsArn": "arn:aws:securityhub:us-east-1::standards/aws-
foundational-security-best-practices/v/1.0.0", "AssociationStatus": "DISABLED",
 "UpdatedReason": "Not applicable to environment"}]'
```

Controles sugeridos para desactivar en el CSPM de Security Hub

Recomendamos deshabilitar algunos controles CSPM AWS de Security Hub para reducir los costos de búsqueda de ruido y uso.

Controles que utilizan recursos globales

Algunos Servicios de AWS admiten recursos globales, lo que significa que puede acceder al recurso desde cualquier lugar. Región de AWS Para ahorrar costesAWS Config, puedes desactivar el registro de los recursos globales en todas las regiones excepto en una. Una vez hecho esto, Security Hub aún ejecutará comprobaciones de seguridad en todas las regiones en las que esté habilitado un control y se cobrará en función de la cantidad de comprobaciones por cuenta y región. En consecuencia, para reducir el ruido de los resultados y disminuir los costos del CSPM de Security

Hub, también debe desactivar los controles que involucren recursos globales en todas las regiones, excepto en la región que registra los recursos globales.

Si un control incluye recursos globales, pero solo está disponible en una región, si lo deshabilita en esa región, no podrá obtener resultados para el recurso subyacente. En ese caso, recomendamos que mantenga el control habilitado. Cuando se usa la agregación entre regiones, la región en la que el control se encuentra disponible debe ser la región de agregación o una de las regiones vinculadas. Los siguientes controles involucran recursos globales, pero solo están disponibles en una única región:

- Todos los CloudFront controles: disponibles solo en la región EE.UU. Este (Norte de Virginia)
- GlobalAccelerator.1— Disponible solo en la región EE.UU. Oeste (Oregón)
- Route53.2— Disponible solo en la región EE.UU. Este (Norte de Virginia)
- WAF.1, WAF.6, WAF.7, WAF.8 — Disponible solo en la región EE.UU. Este (Norte de Virginia)

> **Note**
>
> Si usa la configuración centralizada, el CSPM de Security Hub desactiva automáticamente los controles que implican recursos globales en todas las regiones, excepto en la región de origen. Los controles que elija habilitar a través de una política de configuración están habilitados en todas las regiones en las que están disponibles. Para limitar los resultados de estos controles a una sola región, puede actualizar la configuración de la AWS Config grabadora y desactivar el registro de recursos globales en todas las regiones, excepto en la región de origen.
> Si un control habilitado que implica recursos globales no es compatible en la región de origen, el CSPM de Security Hub intenta habilitarlo en una región vinculada donde sí se admita. Con la configuración centralizada, no se obtiene cobertura para un control que no está disponible ni en la región de origen ni en ninguna de las regiones vinculadas.
> Para obtener más información acerca de la configuración centralizada, consulte Descripción de la configuración central en el CSPM de Security Hub.

Para los controles cuya programación es de tipo periódica, es necesario desactivarlos en el CSPM de Security Hub para evitar cargos. Establecer el AWS Config parámetro en `false` no afecta `includeGlobalResourceTypes` a los controles periódicos de CSPM de Security Hub.

Los siguientes controles del CSPM de Security Hub usan recursos globales:

- [Account.1] La información de contacto de seguridad debe proporcionarse para unCuenta de AWS
- [Account.2]Cuentas de AWSdebe formar parte de unAWS Organizationsorganización
- [CloudFront.1] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado
- [CloudFront.3] CloudFront las distribuciones deben requerir el cifrado durante el tránsito
- [CloudFront.4] CloudFront las distribuciones deben tener configurada la conmutación por error de origen
- [CloudFront.5] CloudFront las distribuciones deben tener habilitado el registro
- [CloudFront.6] CloudFront las distribuciones deben tener WAF activado
- [CloudFront.7] CloudFront las distribuciones deben usar certificados personalizados SSL/TLS
- [CloudFront.8] CloudFront las distribuciones deben usar el SNI para atender las solicitudes HTTPS
- [CloudFront.9] CloudFront las distribuciones deben cifrar el tráfico para convertirlo en orígenes personalizados
- [CloudFront.10] CloudFront las distribuciones no deben usar protocolos SSL obsoletos entre ubicaciones de borde y orígenes personalizados
- [CloudFront.12] CloudFront las distribuciones no deben apuntar a orígenes de S3 inexistentes
- [CloudFront.13] CloudFront las distribuciones deben usar el control de acceso al origen
- [CloudFront.15] CloudFront las distribuciones deben usar la política de seguridad TLS recomendada
- [CloudFront.16] CloudFront las distribuciones deben usar el control de acceso de origen para los orígenes de las URL de las funciones de Lambda
- [GlobalAccelerator.1] Los aceleradores de Global Accelerator deben estar etiquetados
- [IAM.1] Las políticas de IAM no deberían permitir todos los privilegios administrativos «*»
- [IAM.2] Los usuarios de IAM no deberían tener políticas de IAM adjuntas
- [IAM.3] Las claves de acceso de los usuarios de IAM deben rotarse cada 90 días o menos
- [IAM.4] La clave de acceso del usuario raíz de IAM no debería existir
- [IAM.5] La MFA debe estar habilitada para todos los usuarios de IAM que tengan una contraseña de consola
- [IAM.6] La MFA de hardware debe estar habilitada para el usuario root
- [IAM.7] Las políticas de contraseñas para los usuarios de IAM deben tener configuraciones sólidas
- [IAM.8] Se deben eliminar las credenciales de usuario de IAM no utilizadas

- [IAM.9] La MFA debe estar habilitada para el usuario root
- [IAM.10] Las políticas de contraseñas para los usuarios de IAM deben tener configuraciones sólidas
- [IAM.11] Asegúrese de que la política de contraseñas de IAM requiera al menos una letra mayúscula
- [IAM.12] Asegúrese de que la política de contraseñas de IAM requiera al menos una letra minúscula
- [IAM.13] Asegúrese de que la política de contraseñas de IAM requiera al menos un símbolo
- [IAM.14] Asegúrese de que la política de contraseñas de IAM requiera al menos un número
- [IAM.15] Asegúrese de que la política de contraseñas de IAM exija una longitud de contraseña mínima de 14 o más
- [IAM.16] Asegúrese de que la política de contraseñas de IAM impida la reutilización de contraseñas
- [IAM.17] Asegúrese de que la política de contraseñas de IAM haga caducar las contraseñas en un plazo de 90 días o menos
- [IAM.18] Asegúrese de que se haya creado una función de soporte para gestionar los incidentes conAWS Support
- [IAM.19] La MFA debe estar habilitada para todos los usuarios de IAM
- [IAM.21] Las políticas de IAM gestionadas por el cliente que cree no deberían permitir acciones comodín en los servicios
- [IAM.22] Se deben eliminar las credenciales de usuario de IAM que no se hayan utilizado durante 45 días
- [IAM.24] Las funciones de IAM deben estar etiquetadas
- [IAM.25] Los usuarios de IAM deben estar etiquetados
- [IAM.26] SSL/TLS Los certificados caducados gestionados en IAM deben eliminarse
- [IAM.27] Las identidades de IAM no deberían tener la AWSCloudShellFullAccess política adjunta
- [KMS.1] Las políticas gestionadas por los clientes de IAM no deberían permitir acciones de descifrado en todas las claves de KMS
- [KMS.2] Los directores de IAM no deberían tener políticas integradas de IAM que permitan realizar acciones de descifrado en todas las claves de KMS
- [Route53.2] Las zonas alojadas públicas de Route 53 deberían registrar las consultas de DNS

- [WAF.1]AWS WAFEl registro de ACL web global clásico debe estar habilitado
- [WAF.6]AWS WAFLas reglas globales clásicas deben tener al menos una condición
- [WAF.7]AWS WAFLos grupos de reglas globales clásicos deben tener al menos una regla
- [WAF.8]AWS WAFLas ACL web globales clásicas deben tener al menos una regla o grupo de reglas

CloudTrail controles de registro

El CloudTrail.2control evalúa el uso de AWS Key Management Service (AWS KMS) para cifrar los registros de AWS CloudTrail seguimiento. Si registra estos registros en una cuenta de registro centralizada, debe habilitar este control solo en la cuenta y en el Región de AWS lugar donde se realiza el registro centralizado.

Si utiliza la configuración centralizada, el estado de habilitación de un control se alinea en la región de origen y en las regiones vinculadas. No puede deshabilitar un control en algunas regiones y habilitarlo en otras. En este caso, puede suprimir los hallazgos del CloudTrail.2 control para reducir el ruido de búsqueda.

CloudWatch controles de alarma

Si prefieres utilizar Amazon GuardDuty para la detección de anomalías en lugar de CloudWatch las alarmas de Amazon, puedes desactivar los siguientes controles, que se centran en CloudWatch las alarmas:

- [CloudWatch.1] Debe existir un registro, un filtro métrico y una alarma para el uso del usuario «raíz»
- [CloudWatch.2] Asegúrese de que existan un registro, un filtro métrico y una alarma para las llamadas a la API no autorizadas
- [CloudWatch.3] Asegúrese de que haya un registro, un filtro métrico y una alarma para iniciar sesión en la consola de administración sin MFA
- [CloudWatch.4] Asegúrese de que haya un registro, un filtro métrico y una alarma para los cambios en las políticas de IAM
- [CloudWatch.5] Asegúrese de que existan un registro, un filtro métrico y una alarma para los cambios CloudTrail de configuración
- [CloudWatch.6] Asegúrese de que existan un registro métrico, un filtro y una alarma para Consola de administración de AWS errores de autenticación

- [CloudWatch.7] Asegúrese de que haya un registro, un filtro métrico y una alarma para deshabilitar o programar la eliminación de las claves administradas por el cliente
- [CloudWatch.8] Asegúrese de que haya un registro, un filtro métrico y una alarma para los cambios en la política de buckets de S3
- [CloudWatch.9] Asegúrese de que existan un registro métrico, un filtro y una alarma para AWS Config cambios de configuración
- [CloudWatch.10] Asegúrese de que haya un registro, un filtro métrico y una alarma para los cambios en los grupos de seguridad
- [CloudWatch.11] Asegúrese de que existan un filtro métrico de registro y una alarma para los cambios en las listas de control de acceso a la red (NACL)
- [CloudWatch.12] Asegúrese de que haya un registro, un filtro métrico y una alarma para detectar los cambios en las pasarelas de red
- [CloudWatch.13] Asegúrese de que haya un registro, un filtro métrico y una alarma para los cambios en la tabla de rutas
- [CloudWatch.14] Asegúrese de que haya un registro, un filtro métrico y una alarma para los cambios en la VPC

Descripción de las comprobaciones de seguridad y las puntuaciones en el CSPM de Security Hub

Para cada control que habilite, AWS Security Hub CSPM ejecuta comprobaciones de seguridad. Una comprobación de seguridad produce un resultado que indica si un AWS recurso específico cumple con las reglas que incluye el control.

Algunas comprobaciones se ejecutan de forma periódica. Otras comprobaciones solo se ejecutan cuando se produce un cambio en el estado del recurso. Para obtener más información, consulte Programación para ejecutar comprobaciones de seguridad.

Muchas comprobaciones de seguridad utilizan reglas AWS Config administradas o personalizadas para establecer los requisitos de conformidad. Para ejecutar estas comprobaciones, debe configurar AWS Config y activar el registro de recursos para los recursos necesarios. Para obtener más información sobre la configuraciónAWS Config, consulteActivación y configuración AWS Config para Security Hub CSPM. Para obtener una lista de AWS Config los recursos que debe registrar para cada norma, consulteObligatorioAWS Configrecursos para hallazgos de control. Otros controles usan

funciones de Lambda personalizadas administradas por el CSPM de Security Hub y no requieren requisitos previos.

A medida que el CSPM de Security Hub ejecuta comprobaciones de seguridad, genera resultados y les asigna un estado de cumplimiento. Para obtener más información sobre el estado de conformidad, consulte Evaluación del estado de cumplimiento de los resultados del CSPM de Security Hub.

El CSPM de Security Hub usa el estado de cumplimiento de los resultados del control para determinar el estado general del control. Con base en el estado del control, el CSPM de Security Hub también calcula una puntuación de seguridad para todos los controles habilitados y para estándares específicos. Para obtener más información, consulte the section called “Estado de conformidad y el estado de control” y the section called “Calcular las puntuaciones de seguridad”.

Si activa los resultados consolidados de controles, el CSPM de Security Hub genera un único resultado incluso cuando un control se asocia con más de un estándar. Para obtener más información, consulte Resultados de control consolidados.

Temas

- ObligatorioAWS Configrecursos para hallazgos de control
- Programación para ejecutar comprobaciones de seguridad
- Generación y actualización de los resultados de control
- Evaluación del estado de cumplimiento y del estado del control
- Calcular las puntuaciones de seguridad

ObligatorioAWS Configrecursos para hallazgos de control

> **Note**
>
> Si utiliza Security Hub, CSPM y Security Hub, la configuración del registro de recursos se gestiona automáticamente. Security Hub crea un grabador de configuración vinculado a un servicio con todos los recursos relacionados con los controles compatibles con el CSPM de Security Hub AWS Config y obtiene información directa sobre ellos. Para obtener más información, consulte Uso del grabador de configuración vinculado a un servicio.

En AWS Security Hub CSPM, algunos controles utilizan AWS Config reglas vinculadas a servicios que detectan los cambios de configuración en los recursos. AWS Para que Security Hub CSPM genere resultados precisos para estos controles, debe habilitar AWS Config y activar el registro de recursos en. AWS Config Para obtener información sobre cómo Security Hub CSPM usa AWS Config las reglas y cómo habilitarlas y configurarlasAWS Config, consulte. Activación y configuración AWS Config para Security Hub CSPM Para obtener información detallada sobre el registro de recursos, consulte Uso del registrador de configuración en la Guía para desarrolladores de AWS Config.

Para recibir resultados de control precisos, debe activar el registro de AWS Config recursos para los controles habilitados con un tipo de programación activado por cambios. Algunos controles con un tipo de programación periódica también requieren registro de recursos. En esta página se enumeran los recursos requeridos para estos controles del CSPM de Security Hub.

Los controles CSPM de Security Hub pueden basarse en AWS Config reglas administradas o reglas CSPM personalizadas de Security Hub. Asegúrese de que no haya políticas AWS Identity and Access Management (de IAM) o políticas AWS Organizations administradas que impidan tener AWS Config permiso para registrar sus recursos. Los controles CSPM de Security Hub evalúan las configuraciones de los recursos directamente y no tienen en cuenta AWS Organizations las políticas.

> **Note**
>
> Si Regiones de AWS un control no está disponible, el recurso correspondiente no está disponible en. AWS Config Para obtener una lista de estos límites, consulte Límites regionales de los controles del CSPM de Security Hub.

Temas

- Recursos requeridos para todos los controles del CSPM de Security Hub
- Recursos necesarios para elAWSEstándar fundamental de mejores prácticas de seguridad
- Recursos necesarios para el CISAWSPunto de referencia fundamental
- Recursos necesarios para el estándar NIST SP 800-53 Revisión 5
- Recursos necesarios para el estándar NIST SP 800-171 Revisión 2
- Recursos necesarios para PCI DSS v3.2.1
- Recursos necesarios para elAWSEstándar de etiquetado de recursos

Recursos requeridos para todos los controles del CSPM de Security Hub

Para que Security Hub CSPM genere resultados para los controles activados por cambios que estén habilitados y usen una AWS Config regla, debe registrar los siguientes tipos de recursos en. AWS Config Esta tabla también indica qué controles evalúan un tipo específico de recurso. Un único control puede evaluar más de un tipo de recurso.

Servicio de AWS	Tipos de recurso	Controles relacionados
AWS Amplify	`AWS::Amplify::App`	Amplify.1
	`AWS::Amplify::Branch`	Amplify.2
Amazon API Gateway	`AWS::ApiGateway::Stage`	APIGateway.1 APIGateway.2 APIGateway.3 APIGateway.4 APIGateway.5
	`AWS::ApiGatewayV2::Stage`	APIGateway.1 APIGateway.9
	`AWS::ApiGateway::DomainName`	APIGateway.11
AWS AppConfig	`AWS::AppConfig::Application`	AppConfig.1
	`AWS::AppConfig::Co`	AppConfig.2

Servicio de AWS	Tipos de recurso	Controles relacionados
	`nfigurationProfile`	
	`AWS::AppConfig::Environment`	AppConfig.3
	`AWS::AppConfig::ExtensionAssociation`	AppConfig.4
Amazon AppFlow	`AWS::AppFlow::Flow`	AppFlow.1
AWS App Runner	`AWS::AppRunner::Service`	AppRunner.1
	`AWS::AppRunner::VpcConnector`	AppRunner.2
AWS AppSync	`AWS::AppSync::GraphQLApi`	AppSync.2 AppSync.4 AppSync.5
	`AWS::AppSync::ApiCache`	AppSync.1 AppSync.6
AWS Backup	`AWS::Backup::BackupPlan`	Backup.5
	`AWS::Backup::BackupVault`	Backup.3

Servicio de AWS	Tipos de recurso	Controles relacionados
	`AWS::Backup::RecoveryPoint`	Backup.1 Backup.2
	`AWS::Backup::ReportPlan`	Backup.4
AWS Batch	`AWS::Batch::ComputeEnvironment`	Batch.3 Batch.4
	`AWS::Batch::JobQueue`	Batch.1
	`AWS::Batch::SchedulingPolicy`	Batch.2
Amazon Bedrock	`AWS::Bedrock::DataSource`	Bedrock.1
Amazon Bedrock AgentCore	`AWS::BedrockAgentCore::BrowserCustom`	BedrockAgentCore.5 BedrockAgentCore.6
	`AWS::BedrockAgentCore::CodeInterpreterCustom`	BedrockAgentCore.7
	`AWS::BedrockAgentCore::Gateway`	BedrockAgentCore.2 BedrockAgentCore.4

Servicio de AWS	Tipos de recurso	Controles relacionados
	`AWS::BedrockAgentCore::Memory`	BedrockAgentCore.3
	`AWS::BedrockAgentCore::Runtime`	BedrockAgentCore.1
AWS Gestor de certificados(ACM)	`AWS::ACM::Certificate`	ACM.1 ACM.2 ACM.3
Amazon Athena	`AWS::Athena::DataCatalog`	Athena.2
	`AWS::Athena::WorkGroup`	Athena.3 Athena.4
AWS CloudFormation	`AWS::CloudFormation::Stack`	CloudFormation.2 CloudFormation.3 CloudFormation.4

Servicio de AWS	Tipos de recurso	Controles relacionados
Amazon CloudFront	`AWS::CloudFront::Distribution`	CloudFront.1 CloudFront.3 CloudFront.4 CloudFront.5 CloudFront.6 CloudFront.7 CloudFront.8 CloudFront.9 CloudFront.10 CloudFront.13 CloudFront.14 CloudFront.15 CloudFront.16 CloudFront.17
AWS CloudTrail	`AWS::CloudTrail::Trail`	CloudTrail.9
	`AWS::CloudTrail::EventDataStore`	CloudTrail.11
Amazon CloudWatch	`AWS::CloudWatch::Alarm`	CloudWatch.15 CloudWatch.17

Servicio de AWS	Tipos de recurso	Controles relacionados
AWS CodeArtifact	`AWS::CodeArtifact::Repository`	CodeArtifact.1
AWS CodeBuild	`AWS::CodeBuild::Project`	CodeBuild.1 CodeBuild.2 CodeBuild.3 CodeBuild.4
	`AWS::CodeBuild::ReportGroup`	CodeBuild.7
Amazon CodeGuru Profiler	`AWS::CodeGuruProfiler::ProfilingGroup`	CodeGuruProfiler.1
CodeGuru Revisor de Amazon	`AWS::CodeGuruReviewer::RepositoryAssociation`	CodeGuruReviewer.1
Amazon Cognito	`AWS::Cognito::IdentityPool`	Cognito.2

Servicio de AWS	Tipos de recurso	Controles relacionados
	`AWS::Cognito::UserPool`	Cognito.1 Cognito.3 Cognito.4 Cognito.5 Cognito.6
Amazon Connect Customer	`AWS::CustomerProfiles::ObjectType`	Connect.1
	`AWS::Connect::Instance`	Connect.2
AWS DataSync	`AWS::DataSync::Task`	DataSync.1 DataSync.2
Amazon Detective	`AWS::Detective::Graph`	Detective.1
AWS Database Migration Service(AWS DMS)	`AWS::DMS::Certificate`	DMS.2
	`AWS::DMS::Endpoint`	DMS.9 DMS.10 DMS.11 DMS.12
	`AWS::DMS::EventSubscription`	DMS.3

Servicio de AWS	Tipos de recurso	Controles relacionados
	`AWS::DMS::ReplicationInstance`	DMS.4 DMS.6 DMS.13
	`AWS::DMS::ReplicationSubnetGroup`	DMS.5
	`AWS::DMS::ReplicationTask`	DMS.7 DMS.8
Amazon DynamoDB	`AWS::DynamoDB::Table`	DynamoDB.1 DynamoDB.2 DynamoDB.5 DynamoDB.6
Amazon Elastic Compute Cloud (EC2)	`AWS::EC2::ClientVpnEndpoint`	EC2.51
	`AWS::EC2::CustomerGateway`	EC2.36
	`AWS::EC2::DHCPOptions`	EC2.174
	`AWS::EC2::EIP`	EC2.12 EC2.37

Servicio de AWS	Tipos de recurso	Controles relacionados
	`AWS::EC2::FlowLog`	EC2.48
	`AWS::EC2::Instance`	EC2.4 EC2.8 EC2.9 EC2.17 EC2.24 EC2.38 EMR.1 SSM.1
	`AWS::EC2::InternetGateway`	EC2.39
	`AWS::EC2::LaunchTemplate`	EC2.25 EC2.170 EC2.175 EC2.181
	`AWS::EC2::NatGateway`	EC2.40
	`AWS::EC2::NetworkAcl`	EC2.16 EC2.21 EC2.41

Servicio de AWS	Tipos de recurso	Controles relacionados
	`AWS::EC2::NetworkInterface`	EC2.22 EC2.35 EC2.180
	`AWS::EC2::PrefixList`	EC2.176
	`AWS::EC2::RouteTable`	EC2.42
	`AWS::EC2::SecurityGroup`	EC2.2 EC2.13 EC2.14 EC2.18 EC2.19 EC2.43
	`AWS::EC2::SnapshotBlockPublicAccess`	EC2.182
	`AWS::EC2::SpotFleet`	EC2.173
	`AWS::EC2::Subnet`	EC2.15 EC2.44 ElastiCache.7

Servicio de AWS	Tipos de recurso	Controles relacionados
	`AWS::EC2::TrafficMirrorFilter`	EC2.178
	`AWS::EC2::TrafficMirrorSession`	EC2.177
	`AWS::EC2::TrafficMirrorTarget`	EC2.179
	`AWS::EC2::TransitGateway`	EC2.23 EC2.52
	`AWS::EC2::TransitGatewayAttachment`	EC2.33
	`AWS::EC2::TransitGatewayRouteTable`	EC2.34
	`AWS::EC2::Volume`	EC2.3 EC2.45
	`AWS::EC2::VPC`	EC2.6 EC2.46

Servicio de AWS	Tipos de recurso	Controles relacionados
	`AWS::EC2::VPCBlockPublicAccessOptions`	EC2.172
	`AWS::EC2::VPCEndpointService`	EC2.47
	`AWS::EC2::VPCPeeringConnection`	EC2.49
	`AWS::EC2::VPNConnection`	EC2.20 EC2.171 EC2.183
	`AWS::EC2::VPNGateway`	EC2.50
Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup`	AutoScaling.1 AutoScaling.2 AutoScaling.6 AutoScaling.9 AutoScaling.10
	`AWS::AutoScaling::LaunchConfiguration`	AutoScaling.3 Autoscaling.5

Servicio de AWS	Tipos de recurso	Controles relacionados
Amazon EC2 Systems Manager (SSM)	`AWS::SSM::AssociationCompliance`	SSM.3
	`AWS::SSM::ManagedInstanceInventory`	SSM.1
	`AWS::SSM::PatchCompliance`	SSM.2
Amazon Elastic Container Registry (Amazon ECR)	`AWS::ECR::PublicRepository`	ECR.4
	`AWS::ECR::Repository`	ECR.2 ECR.3 ECR.5
Amazon Elastic Container Service (Amazon ECS)	`AWS::ECS::Cluster`	ECS.12 ECS.14
	`AWS::ECS::CapacityProvider`	ECS.19
	`AWS::ECS::Service`	ECS.2 ECS.10 ECS.13

Servicio de AWS	Tipos de recurso	Controles relacionados
	`AWS::ECS::TaskDefinition`	ECS.3 ECS.4 ECS.5 ECS.8 ECS.9 ECS.15 ECS.17 ECS.18 ECS.20 ECS.21
	`AWS::ECS::TaskSet`	ECS.16
Amazon Elastic File System (Amazon EFS)	`AWS::EFS::AccessPoint`	EFS.3 EFS.4 EFS.5
	`AWS::EFS::FileSystem`	EFS.7 EFS.8
Amazon Elastic Kubernetes Service (Amazon EKS)	`AWS::EKS::Cluster`	EKS.2 EKS.6 EKS.8

Servicio de AWS	Tipos de recurso	Controles relacionados
	`AWS::EKS::IdentityProviderConfig`	EKS.7
	`AWS::EKS::Nodegroup`	EKS.9
AWS Elastic Beanstalk	`AWS::ElasticBeanstalk::Environment`	ElasticBeanstalk.1 ElasticBeanstalk.2 ElasticBeanstalk.3
Elastic Load Balancing	`AWS::ElasticLoadBalancing::LoadBalancer`	ELB.2 ELB.3 ELB.5 ELB.7 ELB.8 ELB.9 ELB.10 ELB.14
	`AWS::ElasticLoadBalancingV2::Listener`	ELB.17 ELB.18

Servicio de AWS	Tipos de recurso	Controles relacionados
	`AWS::ElasticLoadBalancingV2::LoadBalancer`	ELB.1 ELB.4 ELB.5 ELB.6 ELB.12 ELB.13 ELB.16
ElasticSearch	`AWS::Elasticsearch::Domain`	ES.3 ES.4 ES.5 ES.6 ES.7 ES.8 ES.9
Amazon EMR	`AWS::EMR::SecurityConfiguration`	EMR.3 EMR.4
Amazon EventBridge	`AWS::Events::EventBus`	EventBridge.2 EventBridge.3
	`AWS::Events::Endpoint`	EventBridge.4

Servicio de AWS	Tipos de recurso	Controles relacionados
Amazon Fraud Detector	`AWS::FraudDetector::EntityType`	FraudDetector.1
	`AWS::FraudDetector::Label`	FraudDetector.2
	`AWS::FraudDetector::Outcome`	FraudDetector.3
	`AWS::FraudDetector::Variable`	FraudDetector.4
AWS Global Accelerator	`AWS::GlobalAccelerator::Accelerator`	GlobalAccelerator.1
AWS Glue	`AWS::Glue::Job`	Glue.1 Glue.4
	`AWS::Glue::MLTransform`	Glue.3
Amazon GuardDuty	`AWS::GuardDuty::Detector`	GuardDuty.4
	`AWS::GuardDuty::Filter`	GuardDuty.2
	`AWS::GuardDuty::IPSet`	GuardDuty.3

Servicio de AWS	Tipos de recurso	Controles relacionados
AWS Identity and Access Managemen t(YO SOY)	`AWS::IAM::Group`	IAM.27 KMS.2
	`AWS::IAM::Policy`	IAM.1 IAM.21 KMS.1
	`AWS::IAM::Role`	IAM.24 IAM.27 KMS.2
	`AWS::IAM::User`	IAM.2 IAM.3 IAM.5 IAM.8 IAM.19 IAM.22 IAM.25 IAM.27 KMS.2
AWS Identity and Access Management Access Analyzer	`AWS::AccessAnalyzer::Analyzer`	IAM.23

Servicio de AWS	Tipos de recurso	Controles relacionados
Amazon Interactive Video Service (Amazon IVS)	`AWS::IVS::PlaybackKeyPair`	IVS.1
	`AWS::IVS::RecordingConfiguration`	IVS.2
	`AWS::IVS::Channel`	IVS.3
AWS IoT	`AWS::IoT::Authorizer`	IoT.4
	`AWS::IoT::Dimension`	IoT.3
	`AWS::IoT::MitigationAction`	IoT.2
	`AWS::IoT::Policy`	IoT.6
	`AWS::IoT::RoleAlias`	IoT.5
	`AWS::IoT::SecurityProfile`	IoT.1
AWSEventos de IoT	`AWS::IoTEvents::AlarmModel`	IoTEvents.3

Servicio de AWS	Tipos de recurso	Controles relacionados
	`AWS::IoTEvents::DetectorModel`	IoTEvents.2
	`AWS::IoTEvents::Input`	IoTEvents.1
AWSIoT SiteWise	`AWS::IoTSiteWise::AssetModel`	IoTSiteWise.1
	`AWS::IoTSiteWise::Dashboard`	IoTSiteWise.2
	`AWS::IoTSiteWise::Gateway`	IoTSiteWise.3
	`AWS::IoTSiteWise::Portal`	IoTSiteWise.4
	`AWS::IoTSiteWise::Project`	IoTSiteWise.5
AWSIoT TwinMaker	`AWS::IoTTwinMaker::Entity`	IoTTwinMaker.4
	`AWS::IoTTwinMaker::Scene`	IoTTwinMaker.3

Servicio de AWS	Tipos de recurso	Controles relacionados
	`AWS::IoTTwinMaker::SyncJob`	IoTTwinMaker.1
	`AWS::IoTTwinMaker::Workspace`	IoTTwinMaker.2
AWSIoT Wireless	`AWS::IoTWireless::MulticastGroup`	IoTWireless.1
	`AWS::IoTWireless::ServiceProfile`	IoTWireless.2
	`AWS::IoTWireless::FuotaTask`	IoTWireless.3
Amazon Keyspaces (para Apache Cassandra)	`AWS::Cassandra::Keyspace`	Keyspaces.1
Amazon Kinesis	`AWS::Kinesis::Stream`	Kinesis.1 Kinesis.2 Kinesis.3
AWS Key Management Service(AWS KMS)	`AWS::KMS::Alias`	S3.17
	`AWS::KMS::Key`	KMS.3 KMS.5 S3.17

Servicio de AWS	Tipos de recurso	Controles relacionados
AWS Lambda	`AWS::Lambda::Function`	Lambda.1 Lambda.2 Lambda.3 Lambda.5 Lambda.6 Lambda.7
Amazon MSK	`AWS::MSK::Cluster`	MSK.1 MSK.2 MSK.4 MSK.6
	`AWS::KafkaConnect::Connector`	MSK.3 MSK.5
Amazon MQ	`AWS::AmazonMQ::Broker`	MQ.2 MQ.4 MQ.5 MQ.6
AWS Network Firewall	`AWS::NetworkFirewall::Firewall`	NetworkFirewall.1 NetworkFirewall.7 NetworkFirewall.9 NetworkFirewall.10

Servicio de AWS	Tipos de recurso	Controles relacionados
	`AWS::NetworkFirewall::FirewallPolicy`	NetworkFirewall.3 NetworkFirewall.4 NetworkFirewall.5 NetworkFirewall.8
	`AWS::NetworkFirewall::RuleGroup`	NetworkFirewall.6
OpenSearch Servicio Amazon	`AWS::OpenSearch::Domain`	Opensearch.1 Opensearch.2 Opensearch.3 Opensearch.4 Opensearch.5 Opensearch.6 Opensearch.7 Opensearch.8 Opensearch.9 Opensearch.10 Opensearch.11
AWS Privada CA	`AWS::ACMPCA::CertificateAuthority`	PCA.2

Servicio de AWS	Tipos de recurso	Controles relacionados
Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBCluster`	DocumentDB.1 DocumentDB.2 DocumentDB.4 DocumentDB.5 Neptune.1 Neptune.2 Neptune.4 Neptune.5 Neptune.7 Neptune.8 Neptune.9 RDS.7 RDS.12 RDS.14 RDS.15 RDS.16 RDS.24 RDS.27 RDS.28 RDS.34 RDS.35

Servicio de AWS	Tipos de recurso	Controles relacionados
		RDS.37 RDS.47 RDS.48
	`AWS::RDS::DBClusterSnapshot`	DocumentDB.3 Neptune.3 Neptune.6 RDS.1 RDS.4 RDS.29

Servicio de AWS	Tipos de recurso	Controles relacionados
	`AWS::RDS::DBInstance`	RDS.2 RDS.3 RDS.5 RDS.6 RDS.8 RDS.9 RDS.10 RDS.11 RDS.13 RDS.17 RDS.23 RDS.25 RDS.30 RDS.36 RDS.40
	`AWS::RDS::DBSecurityGroup`	RDS.31
	`AWS::RDS::DBSnapshot`	RDS.1 RDS.4 RDS.32

Servicio de AWS	Tipos de recurso	Controles relacionados
	`AWS::RDS::DBSubnetGroup`	RDS.33
	`AWS::RDS::EventSubscription`	RDS.19 RDS.20 RDS.21 RDS.22
	`AWS::RDS::GlobalCluster`	RDS.51
Amazon Redshift	`AWS::Redshift::Cluster`	Redshift.1 Redshift.2 Redshift.3 Redshift.4 Redshift.6 Redshift.7 Redshift.8 Redshift.10 Redshift.11 Redshift.18
	`AWS::Redshift::ClusterParameterGroup`	Redshift.2 Redshift.17

Servicio de AWS	Tipos de recurso	Controles relacionados
	`AWS::Redshift::ClusterSnapshot`	Redshift.13
	`AWS::Redshift::ClusterSubnetGroup`	Redshift.14 Redshift.16
	`AWS::Redshift::EventSubscription`	Redshift.12
Amazon Route 53	`AWS::Route53::HostedZone`	Route53.2
	`AWS::Route53::HealthCheck`	Route53.1
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::AccessPoint`	S3.19
	`AWS::S3::AccountPublicAccessBlock`	S3.2 S3.3

Servicio de AWS	Tipos de recurso	Controles relacionados
	`AWS::S3::Bucket`	CloudTrail.6 CloudTrail.7 S3.2 S3.3 S3.5 S3.6 S3.7 S3.8 S3.9 S3.10 S3.11 S3.12 S3.13 S3.14 S3.15 S3.17 S3.20
	`AWS::S3::MultiRegionAccessPoint`	S3.24

Servicio de AWS	Tipos de recurso	Controles relacionados
	`AWS::S3Express::DirectoryBucket`	S3.25
Amazon SageMaker AI	`AWS::SageMaker::AppImageConfig`	SageMaker.6
	`AWS::SageMaker::Image`	SageMaker.7
	`AWS::SageMaker::InferenceExperiment`	SageMaker.23 SageMaker.24
	`AWS::SageMaker::Model`	SageMaker.5 SageMaker.16 SageMaker.19
	`AWS::SageMaker::ModelExplainabilityJobDefinition`	SageMaker.20
	`AWS::SageMaker::ModelQualityJobDefinition`	SageMaker.25
	`AWS::SageMaker::MonitoringSchedule`	SageMaker.22

Servicio de AWS	Tipos de recurso	Controles relacionados
	`AWS::SageMaker::NotebookInstance`	SageMaker.2 SageMaker.3 SageMaker.21
	`AWS::SageMaker::FeatureGroup`	SageMaker.17 SageMaker.18
AWS Secrets Manager	`AWS::SecretsManager::Secret`	SecretsManager.1 SecretsManager.2 SecretsManager.5
AWS Service Catalog	`AWS::ServiceCatalog::Portfolio`	ServiceCatalog.1
Amazon Simple Email Service (Amazon SES)	`AWS::SES::ConfigurationSet`	SES.2 SES.3
	`AWS::SES::ContactList`	SES.1
Amazon Simple Notification Service (Amazon SNS)	`AWS::SNS::Topic`	SNS.1 SNS.3 SNS.4
Amazon Simple Queue Service (Amazon SQS)	`AWS::SQS::Queue`	SQS.1 SQS.2 SQS.3

Servicio de AWS	Tipos de recurso	Controles relacionados
AWS Step Functions	`AWS::StepFunctions::StateMachine`	StepFunctions.1
	`AWS::StepFunctions::Activity`	StepFunctions.2
AWS Systems Manager(SSM)	`AWS::SSM::Document`	SSM.5
AWS Transfer Family	`AWS::Transfer::Agreement`	Transfer.4
	`AWS::Transfer::Certificate`	Transfer.5
	`AWS::Transfer::Connector`	Transfer.3 Transfer.6
	`AWS::Transfer::Profile`	Transfer.7
	`AWS::Transfer::Workflow`	Transfer.1
AWS WAF	`AWS::WAF::Rule`	WAF.6
	`AWS::WAF::RuleGroup`	WAF.7
	`AWS::WAF::WebACL`	WAF.1 WAF.8

Servicio de AWS	Tipos de recurso	Controles relacionados
	`AWS::WAFRegional::Rule`	WAF.2
	`AWS::WAFRegional::RuleGroup`	WAF.3
	`AWS::WAFRegional::WebACL`	WAF.4
	`AWS::WAFv2::RuleGroup`	WAF.12
	`AWS::WAFv2::WebACL`	WAF.10 WAF.11
Amazon WorkSpaces	`AWS::WorkSpaces::WorkSpace`	WorkSpaces.1 WorkSpaces.2

Recursos necesarios para elAWSEstándar fundamental de mejores prácticas de seguridad

Para que Security Hub CSPM informe con precisión las conclusiones de los cambios, los controles activados que se aplican al estándar AWS Foundational Security Best Practices (v.1.0.0), están habilitados y utilizan una AWS Config regla, debe registrar los siguientes tipos de recursos. AWS Config Para obtener información sobre este estándar, consulte AWS Estándar fundamental de mejores prácticas de seguridad en Security Hub (CSPM).

Servicio de AWS	Tipos de recurso
Amazon API Gateway	`AWS::ApiGateway::DomainName` , `AWS::ApiGateway::Stage` , `AWS::ApiGatewayV2::Stage`

Servicio de AWS	Tipos de recurso
AWS AppSync	`AWS::AppSync::ApiCache`, `AWS::AppSync::GraphQLApi`
AWS Backup	`AWS::Backup::RecoveryPoint`
Amazon Bedrock	`AWS::Bedrock::DataSource`
Amazon Bedrock AgentCore	`AWS::BedrockAgentCore::BrowserCustom`, `AWS::BedrockAgentCore::CodeInterpreterCustom`, `AWS::BedrockAgentCore::Gateway`, `AWS::BedrockAgentCore::Runtime`
AWS Gestor de certificados(ACM)	`AWS::ACM::Certificate`
AWS CloudFormation	`AWS::CloudFormation::Stack`
Amazon CloudFront	`AWS::CloudFront::Distribution`
AWS CodeBuild	`AWS::CodeBuild::Project`, `AWS::CodeBuild::ReportGroup`
Amazon Cognito	`AWS::Cognito::IdentityPool`, `AWS::Cognito::UserPool`
AWS CloudTrail	`AWS::CloudTrail::EventDataStore`
Amazon Connect Customer	`AWS::Connect::Instance`
AWS DataSync	`AWS::DataSync::Task`
AWS Database Migration Service(AWS DMS)	`AWS::DMS::Endpoint`, `AWS::DMS::ReplicationInstance`, `AWS::DMS::ReplicationTask`
Amazon DynamoDB	`AWS::DynamoDB::Table`

Servicio de AWS	Tipos de recurso
Amazon EC2 Systems Manager (SSM)	`AWS::SSM::AssociationCompliance`, `AWS::SSM::ManagedInstanceInventory`, `AWS::SSM::PatchCompliance`
Amazon Elastic Compute Cloud (Amazon EC2)	`AWS::EC2::ClientVpnEndpoint`, `AWS::EC2::Instance`, `AWS::EC2::LaunchTemplate`, `AWS::EC2::NetworkAcl`, `AWS::EC2::NetworkInterface`, `AWS::EC2::SecurityGroup`, `AWS::EC2::SnapshotBlockPublicAccess`, `AWS::EC2::SpotFleet`, `AWS::EC2::Subnet`, `AWS::EC2::TransitGateway`, `AWS::EC2::VPCBlockPublicAccessOptions`, `AWS::EC2::VPNConnection`, `AWS::EC2::Volume`
Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup`, `AWS::AutoScaling::LaunchConfiguration`
Amazon Elastic Container Registry (Amazon ECR)	`AWS::ECR::Repository`
Amazon Elastic Container Service (Amazon ECS)	`AWS::ECS::CapacityProvider`, `AWS::ECS::Cluster`, `AWS::ECS::Service`, `AWS::ECS::TaskDefinition`, `AWS::ECS::TaskSet`
Amazon Elastic File System (Amazon EFS)	`AWS::EFS::AccessPoint`, `AWS::EFS::FileSystem`
Amazon Elastic Kubernetes Service (Amazon EKS)	`AWS::EKS::Cluster`, `AWS::EKS::Nodegroup`

Servicio de AWS	Tipos de recurso
AWS Elastic Beanstalk	`AWS::ElasticBeanstalk::Environment`
Elastic Load Balancing	`AWS::ElasticLoadBalancing::LoadBalancer` , `AWS::ElasticLoadBalancingV2::Listener` , `AWS::ElasticLoadBalancingV2::LoadBalancer`
ElasticSearch	`AWS::Elasticsearch::Domain`
Amazon EMR	`AWS::EMR::SecurityConfiguration`
AWS Glue	`AWS::Glue::Job` , `AWS::Glue::MLTransform`
AWS Identity and Access Management(YO SOY)	`AWS::IAM::Group` , `AWS::IAM::Policy` , `AWS::IAM::Role` , `AWS::IAM::User`
Amazon Kinesis	`AWS::Kinesis::Stream`
AWS Key Management Service(AWS KMS)	`AWS::KMS::Key`
AWS Lambda	`AWS::Lambda::Function`
Amazon Managed Streaming para Apache Kafka (Amazon MSK)	`AWS::MSK::Cluster` , `AWS::KafkaConnect::Connector`
AWS Network Firewall	`AWS::NetworkFirewall::Firewall` , `AWS::NetworkFirewall::FirewallPolicy` , `AWS::NetworkFirewall::RuleGroup`
OpenSearch Servicio Amazon	`AWS::OpenSearch::Domain`

Servicio de AWS	Tipos de recurso
Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBCluster`, `AWS::RDS::DBClusterSnapshot`, `AWS::RDS::DBInstance`, `AWS::RDS::DBProxy`, `AWS::RDS::DBSnapshot`, `AWS::RDS::EventSubscription`, `AWS::RDS::GlobalCluster`
Amazon Redshift	`AWS::Redshift::Cluster`, `AWS::Redshift::ClusterSubnetGroup`
Amazon Redshift sin servidor	`AWS::RedshiftServerless::Workgroup`
Amazon Route 53	`AWS::Route53::HostedZone`
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::AccessPoint`, `AWS::S3::AccountPublicAccessBlock`, `AWS::S3::Bucket`, `AWS::S3::MultiRegionAccessPoint`, `AWS::S3Express::DirectoryBucket`
Amazon SageMaker AI	`AWS::SageMaker::FeatureGroup`, `AWS::SageMaker::InferenceExperiment`, `AWS::SageMaker::Model`, `AWS::SageMaker::ModelExplainabilityJobDefinition`, `AWS::SageMaker::ModelQualityJobDefinition`, `AWS::SageMaker::MonitoringSchedule`, `AWS::SageMaker::NotebookInstance`
Amazon Simple Notification Service (Amazon SNS)	`AWS::SNS::Topic`
Amazon Simple Queue Service (Amazon SQS)	`AWS::SQS::Queue`

Servicio de AWS	Tipos de recurso
AWS Secrets Manager	`AWS::SecretsManager::Secret`
AWS Step Functions	`AWS::StepFunctions::StateMachine`
AWS Transfer Family	`AWS::Transfer::Connector`
AWS WAF	`AWS::WAF::Rule` , `AWS::WAF::RuleGroup` , `AWS::WAF::WebACL` , `AWS::WAFRegional::Rule` , `AWS::WAFRegional::RuleGroup` , `AWS::WAFRegional::WebACL` , `AWS::WAFv2::RuleGroup` , `AWS::WAFv2::WebACL`
Amazon WorkSpaces	`AWS::WorkSpaces::WorkSpace`

Recursos necesarios para el CISAWSPunto de referencia fundamental

Para ejecutar comprobaciones de seguridad para los controles habilitados que se aplican al Center for Internet Security (CIS) AWS Foundations Benchmark, Security Hub CSPM sigue los pasos de auditoría exactos prescritos para las comprobaciones o utiliza reglas AWS Config gestionadas específicas. Para información sobre este estándar en el CSPM de Security Hub, consulte CIS AWS Aspectos básicos y comparativos del CSPM de Security Hub.

Recursos necesarios para CIS v5.0.0

Para que Security Hub CSPM informe con precisión de las conclusiones de los controles activados por cambios de CIS v5.0.0 habilitados que utilizan una AWS Config regla, debe registrar los siguientes tipos de recursos en. AWS Config

Servicio de AWS	Tipos de recurso
Amazon Elastic Compute Cloud (Amazon EC2)	`AWS::EC2::Instance` , `AWS::EC2::NetworkAcl` , `AWS::EC2::SecurityGroup` , `AWS::EC2::VPC`
Amazon Elastic File System (Amazon EFS)	`AWS::EFS::FileSystem`

Servicio de AWS	Tipos de recurso
AWS Identity and Access Management(IAM)	`AWS::IAM::Group` , `AWS::IAM::User` , `AWS::IAM::Role`
Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBInstance` , `AWS::RDS::DBCluster`
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::Bucket`

Recursos necesarios para CIS v3.0.0

Para que Security Hub CSPM informe con precisión de las conclusiones de los controles activados por cambios de CIS v3.0.0 habilitados que utilizan una AWS Config regla, debe registrar los siguientes tipos de recursos en. AWS Config

Servicio de AWS	Tipos de recurso
Amazon Elastic Compute Cloud (Amazon EC2)	`AWS::EC2::Instance` , `AWS::EC2::NetworkAcl` , `AWS::EC2::Security Group` , `AWS::EC2::VPC`
AWS Identity and Access Management(IAM)	`AWS::IAM::Group` , `AWS::IAM::User` , `AWS::IAM::Role`
Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBInstance`
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::Bucket`

Recursos de necesarios para CIS v1.4.0

Para que Security Hub CSPM informe con precisión de las conclusiones de los controles activados por cambios en el CIS v1.4.0 habilitados que utilizan una AWS Config regla, debe registrar los siguientes tipos de recursos en. AWS Config

Servicio de AWS	Tipos de recurso
Amazon Elastic Compute Cloud (Amazon EC2)	`AWS::EC2::NetworkAcl` , `AWS::EC2::SecurityGroup`
AWS Identity and Access Management(IAM)	`AWS::IAM::Policy` , `AWS::IAM::User`
Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBInstance`
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::Bucket`

Recursos de necesarios para CIS v1.2.0

Para que Security Hub CSPM informe con precisión de las conclusiones de los controles activados por cambios en el CIS v1.2.0 habilitados que utilizan una AWS Config regla, debe registrar los siguientes tipos de recursos en. AWS Config

Servicio de AWS	Tipos de recurso
Amazon Elastic Compute Cloud (Amazon EC2)	`AWS::EC2::SecurityGroup`
AWS Identity and Access Management(IAM)	`AWS::IAM::Policy` , `AWS::IAM::User`

Recursos necesarios para el estándar NIST SP 800-53 Revisión 5

Para que Security Hub CSPM informe con precisión las conclusiones de los cambios, los controles activados que se aplican al estándar NIST SP 800-53 revisión 5, están habilitados y utilizan una AWS Config regla, debe registrar los siguientes tipos de recursos. AWS Config Para obtener información sobre este estándar, consulte Revisión 5 de NIST SP 800-53 en el CSPM de Security Hub.

Servicio de AWS	Tipos de recurso
Amazon API Gateway	`AWS::ApiGateway::Stage` , `AWS::ApiGatewayV2::Stage`
AWS AppSync	`AWS::AppSync::GraphQLApi`

Servicio de AWS	Tipos de recurso
AWS Backup	`AWS::Backup::RecoveryPoint`
Amazon Bedrock AgentCore	`AWS::BedrockAgentCore::Gateway`, `AWS::BedrockAgentCore::Memory`
AWS Gestor de certificados(ACM)	`AWS::ACM::Certificate`
AWS CloudFormation	`AWS::CloudFormation::Stack`
Amazon CloudFront	`AWS::CloudFront::Distribution`
Amazon CloudWatch	`AWS::CloudWatch::Alarm`
AWS CodeBuild	`AWS::CodeBuild::Project`
AWS Database Migration Service(AWS DMS)	`AWS::DMS::Endpoint`, `AWS::DMS::ReplicationInstance`, `AWS::DMS::ReplicationTask`
Amazon DynamoDB	`AWS::DynamoDB::Table`
Amazon Elastic Compute Cloud (Amazon EC2)	`AWS::EC2::ClientVpnEndpoint`, `AWS::EC2::EIP`, `AWS::EC2::Instance`, `AWS::EC2::LaunchTemplate`, `AWS::EC2::NetworkAcl`, `AWS::EC2::NetworkInterface`, `AWS::EC2::SecurityGroup`, `AWS::EC2::Subnet`, `AWS::EC2::TransitGateway`, `AWS::EC2::VPNConnection`, `AWS::EC2::Volume`
Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup`, `AWS::AutoScaling::LaunchConfiguration`
Amazon Elastic Container Registry (Amazon ECR)	`AWS::ECR::Repository`

Servicio de AWS	Tipos de recurso
Amazon Elastic Container Service (Amazon ECS)	`AWS::ECS::Cluster` , `AWS::ECS::Service` , `AWS::ECS::TaskDefinition`
Amazon Elastic File System (Amazon EFS)	`AWS::EFS::AccessPoint`
Amazon Elastic Kubernetes Service (Amazon EKS)	`AWS::EKS::Cluster`
AWS Elastic Beanstalk	`AWS::ElasticBeanstalk::Environment`
Elastic Load Balancing	`AWS::ElasticLoadBalancing::LoadBalancer` , `AWS::ElasticLoadBalancingV2::Listener` , `AWS::ElasticLoadBalancingV2::LoadBalancer`
Amazon ElasticSearch	`AWS::Elasticsearch::Domain`
Amazon EMR	`AWS::EMR::SecurityConfiguration`
Amazon EventBridge	`AWS::Events::Endpoint` , `AWS::Events::EventBus`
AWS Glue	`AWS::Glue::Job`
AWS Identity and Access Management(YO SOY)	`AWS::IAM::Group` , `AWS::IAM::Policy` , `AWS::IAM::Role` , `AWS::IAM::User`
AWS Key Management Service(AWS KMS)	`AWS::KMS::Alias` , `AWS::KMS::Key`
Amazon Kinesis	`AWS::Kinesis::Stream`
AWS Lambda	`AWS::Lambda::Function`
Amazon Managed Streaming para Apache Kafka (Amazon MSK)	`AWS::MSK::Cluster`

Servicio de AWS	Tipos de recurso
Amazon MQ	`AWS::AmazonMQ::Broker`
AWS Network Firewall	`AWS::NetworkFirewall::Firewall`, `AWS::NetworkFirewallPolicy`, `AWS::NetworkFirewall::RuleGroup`
OpenSearch Servicio Amazon	`AWS::OpenSearch::Domain`
Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBCluster`, `AWS::RDS::DBClusterSnapshot`, `AWS::RDS::DBInstance`, `AWS::RDS::DBSnapshot`, `AWS::RDS::EventSubscription`
Amazon Redshift	`AWS::Redshift::Cluster`, `AWS::Redshift::ClusterSubnetGroup`
Amazon Route 53	`AWS::Route53::HostedZone`
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::AccessPoint`, `AWS::S3::AccountPublicAccessBlock`, `AWS::S3::Bucket`
AWS Service Catalog	`AWS::ServiceCatalog::Portfolio`
Amazon Simple Notification Service (Amazon SNS)	`AWS::SNS::Topic`
Amazon Simple Queue Service (Amazon SQS)	`AWS::SQS::Queue`
Amazon EC2 Systems Manager (SSM)	`AWS::SSM::AssociationCompliance`, `AWS::SSM::ManagedInstanceInventory`, `AWS::SSM::PatchCompliance`
Amazon SageMaker AI	`AWS::SageMaker::FeatureGroup`, `AWS::SageMaker::NotebookInstance`

Servicio de AWS	Tipos de recurso
AWS Secrets Manager	`AWS::SecretsManager::Secret`
AWS Transfer Family	`AWS::Transfer::Connector`
AWS WAF	`AWS::WAF::Rule` , `AWS::WAF::RuleGroup` , `AWS::WAF::WebACL` , `AWS::WAFRegional::Rule` , `AWS::WAFRegional::RuleGroup` , `AWS::WAFRegional::WebACL` , `AWS::WAFv2::RuleGroup` , `AWS::WAFv2::WebACL`

Recursos necesarios para el estándar NIST SP 800-171 Revisión 2

Para que Security Hub CSPM informe con precisión las conclusiones de los cambios, los controles activados que se aplican al estándar NIST SP 800-171 revisión 2, están habilitados y utilizan una AWS Config regla, debe registrar los siguientes tipos de recursos. AWS Config Para obtener información sobre este estándar, consulte Revisión 2 de NIST SP 800-171 en el CSPM de Security Hub.

Servicio de AWS	Tipos de recurso
AWS Gestor de certificados (ACM)	`AWS::ACM::Certificate`
Amazon API Gateway	`AWS::ApiGateway::Stage`
Amazon CloudFront	`AWS::CloudFront::Distribution`
Amazon CloudWatch	`AWS::CloudWatch::Alarm`
Amazon Elastic Compute Cloud (Amazon EC2)	`AWS::EC2::ClientVpnEndpoint` , `AWS::EC2::NetworkAcl` , `AWS::EC2::SecurityGroup` , `AWS::EC2::VPC` , `AWS::EC2::VPNConnection`
Elastic Load Balancing	`AWS::ElasticLoadBalancing::LoadBalancer`

Servicio de AWS	Tipos de recurso
AWS Identity and Access Management(YO SOY)	`AWS::IAM::Policy` , `AWS::IAM::User`
AWS Key Management Service (AWS KMS)	`AWS::KMS::Alias` , `AWS::KMS::Key`
AWS Network Firewall	`AWS::NetworkFirewall::FirewallPolicy` , `AWS::NetworkFirewall::RuleGroup`
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::Bucket`
Amazon Simple Notification Service (Amazon SNS)	`AWS::SNS::Topic`
AWS Systems Manager (SSM)	`AWS::SSM::PatchCompliance`
AWS WAF	`AWS::WAFv2::RuleGroup`

Recursos necesarios para PCI DSS v3.2.1

Para que el CSPM de Security Hub informe con precisión los resultados, debe registrar los siguientes tipos de recursos en AWS Config. Esto se aplica a los controles que: (1) se aplican a la versión 3.2.1 del estándar Payment Card Industry Data Security Standard (PCI DSS), (2) están habilitados y (3) usan una regla de AWS Config. Para obtener información sobre este estándar, consulte PCI DSS en el CSPM de Security Hub.

Servicio de AWS	Tipos de recurso
AWS CodeBuild	`AWS::CodeBuild::Project`
Amazon Elastic Compute Cloud (Amazon EC2)	`AWS::EC2::EIP` , `AWS::EC2::Instance` , `AWS::EC2::SecurityGroup`
Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup`
AWS Identity and Access Management(IAM)	`AWS::IAM::Policy` , `AWS::IAM::User`

Servicio de AWS	Tipos de recurso
AWS Lambda	`AWS::Lambda::Function`
OpenSearch Servicio Amazon	`AWS::OpenSearch::Domain`
Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBClusterSnapshot` , `AWS::RDS::DBInstance` , `AWS::RDS::DBSnapshot`
Amazon Redshift	`AWS::Redshift::Cluster`
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::AccountPublicAccessBlock` , `AWS::S3::Bucket`
Amazon EC2 Systems Manager (SSM)	`AWS::SSM::AssociationCompliance` , `AWS::SSM::ManagedInstanceInventory` , `AWS::SSM::PatchCompliance`

Recursos necesarios para elAWSEstándar de etiquetado de recursos

Todos los controles que se aplican al estándar de etiquetado de AWS recursos se activan mediante cambios y utilizan una AWS Config regla. Para que Security Hub CSPM informe con precisión de los hallazgos de estos controles, debe registrar los siguientes tipos de recursos en. AWS Config Para obtener información sobre este estándar, consulte AWS Estándar de etiquetado de recursos en Security Hub CSPM.

Servicio de AWS	Tipos de recurso
AWS Amplify	`AWS::Amplify::App` , `AWS::Amplify::Branch`
Amazon AppFlow	`AWS::AppFlow::Flow`
AWS App Runner	`AWS::AppRunner::Service` , `AWS::AppRunner::VpcConnector`

Servicio de AWS	Tipos de recurso
AWS AppConfig	`AWS::AppConfig::Application`, `AWS::AppConfig::ConfigurationProfile`, `AWS::AppConfig::Environment`, `AWS::AppConfig::ExtensionAssociation`
AWS AppSync	`AWS::AppSync::GraphQLApi`
Amazon Athena	`AWS::Athena::DataCatalog`, `AWS::Athena::WorkGroup`
AWS Backup	`AWS::Backup::BackupPlan`, `AWS::Backup::BackupVault`, `AWS::Backup::RecoveryPlan`, `AWS::Backup::ReportPlan`
AWS Batch	`AWS::Batch::ComputeEnvironment`, `AWS::Batch::JobQueue`, `AWS::Batch::SchedulingPolicy`
AWS Gestor de certificados(ACM)	`AWS::ACM::Certificate`
AWS CloudFormation	`AWS::CloudFormation::Stack`
Amazon CloudFront	`AWS::CloudFront::Distribution`
AWS CloudTrail	`AWS::CloudTrail::Trail`
AWS CodeArtifact	`AWS::CodeArtifact::Repository`
Amazon CodeGuru	`AWS::CodeGuruProfiler::ProfilingGroup`, `AWS::CodeGuruReviewer::RepositoryAssociation`
Amazon Connect Customer	`AWS::CustomerProfiles::ObjectType`

Servicio de AWS	Tipos de recurso
AWS Database Migration Service(AWS DMS)	`AWS::DMS::Certificate`, `AWS::DMS::EventSubscription` `AWS::DMS::ReplicationInstance`, `AWS::DMS::ReplicationSubnetGroup`
AWS DataSync	`AWS::DataSync::Task`
Amazon Detective	`AWS::Detective::Graph`
Amazon DynamoDB	`AWS::DynamoDB::Trail`
Amazon Elastic Compute Cloud (EC2)	`AWS::EC2::CustomerGateway`, `AWS::EC2::DHCPOptions`, `AWS::EC2::EIP`, `AWS::EC2::FlowLog`, `AWS::EC2::Instance`, `AWS::EC2::InternetGateway`, `AWS::EC2::LaunchTemplate`, `AWS::EC2::NatGateway`, `AWS::EC2::NetworkAcl`, `AWS::EC2::NetworkInterface`, `AWS::EC2::PrefixList`, `AWS::EC2::RouteTable`, `AWS::EC2::SecurityGroup`, `AWS::EC2::Subnet`, `AWS::EC2::TrafficMirrorFilter`, `AWS::EC2::TrafficMirrorSession`, `AWS::EC2::TrafficMirrorTarget`, `AWS::EC2::TransitGateway`, `AWS::EC2::TransitGatewayAttachment`, `AWS::EC2::TransitGatewayRouteTable`, `AWS::EC2::Volume`, `AWS::EC2::VPC`, `AWS::EC2::VPCEndpointService`, `AWS::EC2::VPCPeeringConnection`, `AWS::EC2::VPNGateway`

Servicio de AWS	Tipos de recurso
Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup`
Amazon Elastic Container Registry (Amazon ECR)	`AWS::ECR::PublicRepository`
Amazon Elastic Container Service (Amazon ECS)	`AWS::ECS::Cluster` , `AWS::ECS::Service` , `AWS::ECS::TaskDefinition`
Amazon Elastic File System (Amazon EFS)	`AWS::EFS::AccessPoint`
Amazon Elastic Kubernetes Service (Amazon EKS)	`AWS::EKS::Cluster` , `AWS::EKS::IdentityProviderConfig`
AWS Elastic Beanstalk	`AWS::ElasticBeanstalk::Environment`
ElasticSearch	`AWS::Elasticsearch::Domain`
Amazon EventBridge	`AWS::Events::EventBus`
Amazon Fraud Detector	`AWS::FraudDetector::EntityType` , `AWS::FraudDetector::Label` `AWS::FraudDetector::Outcome` , `AWS::FraudDetector::Variable`
AWS Global Accelerator	`AWS::GlobalAccelerator::Accelerator`
AWS Glue	`AWS::Glue::Job`
Amazon GuardDuty	`AWS::GuardDuty::Detector` , `AWS::GuardDuty::Filter` , `AWS::GuardDuty::IPSet`

Servicio de AWS	Tipos de recurso
AWS Identity and Access Management(YO SOY)	`AWS::IAM::Role` , `AWS::IAM::User`
AWS Identity and Access Management Access Analyzer(Analizador de acceso IAM)	`AWS::AccessAnalyzer::Analyzer`
AWS IoT	`AWS::IoT::Authorizer` , `AWS::IoT::Dimension` , `AWS::IoT::MitigationAction` , `AWS::IoT::Policy` , `AWS::IoT::RoleAlias` , `AWS::IoT::SecurityProfile`
AWS IoTEventos	`AWS::IoTEvents::AlarmModel` , `AWS::IoTEvents::DetectorModel` , `AWS::IoTEvents::Input`
AWS IoTSiteWise	`AWS::IoTSiteWise::Dashboard` , `AWS::IoTSiteWise::Gateway` , `AWS::IoTSiteWise::Portal` , `AWS::IoTSiteWise::Project`
AWS IoTTwinMaker	`AWS::IoTTwinMaker::Entity` , `AWS::IoTTwinMaker::Scene` , `AWS::IoTTwinMaker::SyncJob` , `AWS::IoTTwinMaker::Workspace`
AWS IoTinalámbrico	`AWS::IoTWireless::FuotaTask` , `AWS::IoTWireless::MulticastGroup` , `AWS::IoTWireless::ServiceProfile`
Amazon Interactive Video Service (Amazon IVS)	`AWS::IVS::Channel` , `AWS::IVS::PlaybackKeyPair` , `AWS::IVS::RecordingConfiguration`
Amazon Keyspaces (para Apache Cassandra)	`AWS::Cassandra::Keyspace`

Servicio de AWS	Tipos de recurso
Amazon Kinesis	`AWS::Kinesis::Stream`
AWS Lambda	`AWS::Lambda::Function`
Amazon MQ	`AWS::AmazonMQ::Broker`
AWS Network Firewall	`AWS::NetworkFirewall::Firewall`, `AWS::NetworkFirewall::FirewallPolicy`
OpenSearch Servicio Amazon	`AWS::OpenSearch::Domain`
AWS Autoridad de certificación privada	`AWS::ACMPCA::CertificateAuthority`
Amazon Relational Database Service	`AWS::RDS::DBCluster`, `AWS::RDS::DBClusterSnapshot`, `AWS::RDS::DBInstance`, `AWS::RDS::DBSecurityGroup`, `AWS::RDS::DBSnapshot`, `AWS::RDS::DBSubnetGroup`
Amazon Redshift	`AWS::Redshift::Cluster`, `AWS::Redshift::ClusterParameterGroup`, `AWS::Redshift::ClusterSnapshot`, `AWS::Redshift::ClusterSubnetGroup`, `AWS::Redshift::EventSubscription`
Amazon Route 53	`AWS::Route53::HealthCheck`
Amazon SageMaker AI	`AWS::SageMaker::AppImageConfig`, `AWS::SageMaker::Image`
AWS Secrets Manager	`AWS::SecretsManager::Secret`
Amazon Simple Email Service (Amazon SES)	`AWS::SES::ConfigurationSet`, `AWS::SES::ContactList`

Servicio de AWS	Tipos de recurso
Amazon Simple Notification Service (Amazon SNS)	`AWS::SNS::Topic`
Amazon Simple Queue Service (Amazon SQS)	`AWS::SQS::Queue`
AWS Step Functions	`AWS::StepFunctions::Activity`
AWS Systems Manager(SSM)	`AWS::SSM::Document`
AWS Transfer Family	`AWS::Transfer::Agreement` , `AWS::Transfer::Certificate` , `AWS::Transfer::Connector` , `AWS::Transfer::Profile` , `AWS::Transfer::Workflow`

Programación para ejecutar comprobaciones de seguridad

Tras activar un estándar de seguridad, AWS Security Hub CSPM comienza a ejecutar todas las comprobaciones en un plazo de dos horas. La mayoría de las comprobaciones comienzan a ejecutarse en 25 minutos. El CSPM de Security Hub ejecuta comprobaciones mediante la evaluación de la regla subyacente de un control. Hasta que un control complete su primera ejecución de comprobaciones, su estado es Sin datos.

Al habilitar un nuevo estándar, Security Hub CSPM puede tardar hasta 24 horas en generar resultados para los controles que utilizan la misma regla subyacente AWS Config vinculada a servicios que los controles habilitados de otros estándares habilitados. Por ejemplo, si habilita el Lambda.1control en el estándar AWS Foundational Security Best Practices (FSBP), Security Hub CSPM crea la regla vinculada al servicio y, por lo general, genera resultados en cuestión de minutos. Después de esto, si habilita el Lambda.1 control en el Estándar de seguridad de datos del sector de tarjetas de pago (PCI DSS), Security Hub CSPM puede tardar hasta 24 horas en generar resultados para el control, ya que utiliza la misma regla vinculada al servicio.

Después de la comprobación inicial, la programación de cada control puede ser periódica o activada por cambios. En el caso de un control que se basa en una AWS Config regla administrada, la descripción del control incluye un enlace a la descripción de la regla en la Guía para desarrolladores. AWS Config Esa descripción especifica si la regla se activa por cambios o si es periódica.

Controles de seguridad periódicos

Los controles de seguridad periódicos se ejecutan automáticamente en las 12 o 24 horas posteriores a la última ejecución. El CSPM de Security Hub determina la periodicidad, y usted no puede cambiarla. Los controles periódicos reflejan una evaluación en el momento en que se ejecuta la comprobación.

Si actualiza el estado de flujo de trabajo de un resultado de control periódico y, a continuación, en la siguiente comprobación, el estado de cumplimiento del resultado sigue siendo el mismo, el estado de flujo de trabajo permanece en su estado modificado. Por ejemplo, si se produce un error al buscar el KMS.4control (la AWS KMS keyrotación debe estar habilitada) y, a continuación, se corrige el hallazgo, Security Hub CSPM cambia el estado del flujo de trabajo de a. `NEW` `RESOLVED` Si desactiva la rotación de claves de KMS antes de la siguiente comprobación periódica, el estado del flujo de trabajo del resultado se mantiene como `RESOLVED`.

Las comprobaciones que utilizan funciones de Lambda personalizadas del CSPM de Security Hub son periódicas.

Change-triggered controles de seguridad

Change-triggered las comprobaciones de seguridad se ejecutan cuando el recurso asociado cambia de estado. AWS Configle permite elegir entre el registro continuo de los cambios en el estado del recurso y el registro diario. Si elige el registro diario, AWS Config entrega los datos de configuración de los recursos al final de cada período de 24 horas si se producen cambios en el estado de los recursos. Si no hay cambios, no se entrega ningún dato. Esto podría retrasar la generación de resultados del CSPM de Security Hub hasta que finalice un período de 24 horas. Independientemente del período de grabación que haya elegido, el CSPM de Security Hub comprueba al menos una vez cada 24 horas para asegurarse de que no AWS Config se haya omitido ninguna actualización de recursos.

Por lo general, el CSPM de Security Hub utiliza reglas activadas por cambios siempre que es posible. Para que un recurso utilice una regla activada por cambios, debe ser compatible con los elementos de configuración. AWS Config

Generación y actualización de los resultados de control

AWSSecurity Hub CSPM genera y actualiza las conclusiones de control cuando realiza comprobaciones con los controles de seguridad. Los resultados de control utilizan el Formato de resultados de seguridad de AWS.

El CSPM de Security Hub normalmente cobra por cada comprobación de seguridad de un control. Sin embargo, si varios controles utilizan la misma AWS Config regla, Security Hub CSPM solo cobrará una vez por cada comprobación que se ajuste a la regla. Por ejemplo, varios controles utilizan la AWS Config `iam-password-policy` regla en el estándar CIS AWS Foundations Benchmark y en el estándar AWS Foundational Security Best Practices. Cada vez que el CSPM de Security Hub ejecuta una comprobación con esa regla, genera un resultado de control independiente para cada control relacionado, pero cobra solo una vez por la comprobación.

Si el tamaño de un resultado de control excede el máximo de 240 KB, el CSPM de Security Hub elimina el objeto `Resource.Details` del resultado. En el caso de los controles respaldados por AWS Config recursos, puede revisar los detalles de los recursos mediante la AWS Config consola.

Temas

- Resultados de control consolidados
- Generación, actualización y archivado de resultados de control
- Automatización y supresión de resultados de control
- Detalles de cumplimiento para los resultados de control
- ProductFields detalles de los hallazgos de control
- Niveles de gravedad correspondientes a los resultados de control

Resultados de control consolidados

Si la cuenta tiene habilitados los resultados consolidados de control, el CSPM de Security Hub genera un único resultado (o una actualización del resultado) por cada comprobación de seguridad de un control, incluso cuando ese control corresponde a varios estándares habilitados. Para ver una lista de los controles y los estándares a los que se aplican, consulte Referencia de controles para el CSPM de Security Hub. Recomendamos habilitar los resultados de control consolidados para reducir el ruido de resultados.

Si habilitó el CSPM de Security Hub Cuenta de AWS antes del 23 de febrero de 2023, puede habilitar los hallazgos de control consolidados siguiendo las instrucciones que aparecen más adelante en esta sección. Si habilita el CSPM de Security Hub el 23 de febrero de 2023 o después de esa fecha, los resultados consolidados de control se habilitan automáticamente para la cuenta.

Si utiliza la integración del CSPM de Security Hub con AWS Organizations o invitó cuentas de miembro mediante un proceso manual, los resultados consolidados de control se habilitan para las cuentas de miembro solo si están habilitados para la cuenta de administrador. Si la característica

está desactivada para la cuenta de administrador, también lo estará para las cuentas de miembro. Este comportamiento se aplica a las cuentas de miembros nuevas y existentes. Además, si el administrador utiliza la configuración centralizada para administrar el CSPM de Security Hub para varias cuentas, no puede usar las políticas de configuración centralizada para habilitar o desactivar los resultados consolidados de control para las cuentas.

Si desactiva los resultados consolidados de control para la cuenta, el CSPM de Security Hub genera o actualiza un resultado de control independiente por cada estándar habilitado que incluya un control. Por ejemplo, si habilita cuatro estándares que comparten un control, recibe cuatro resultados independientes después de una comprobación de seguridad para ese control. Si habilita los resultados de control consolidados, solo recibirá un resultado.

Cuando habilita los resultados consolidados de control, el CSPM de Security Hub genera nuevos resultados que no dependen de ningún estándar y archiva los resultados anteriores que sí estaban asociados a estándares. Algunos campos y valores de los resultados de control cambiarán, lo que podría afectar los flujos de trabajo existentes. Para obtener información sobre estos cambios, consulte Resultados de control consolidados: cambios en ASFF. Habilitar los resultados consolidados de control también podría afectar los resultados que los productos de terceros integrados reciben del CSPM de Security Hub. Si utiliza la solución Automated Security Response en la AWS versión 2.0.0, tenga en cuenta que admite los resultados de control consolidados.

Para habilitar o deshabilitar los resultados de control consolidados, debe iniciar sesión en una cuenta de administrador o en una cuenta independiente.

> **Note**
>
> Después de habilitar los resultados consolidados de control, el CSPM de Security Hub puede tardar hasta 24 horas en generar nuevos resultados consolidados y archivar los resultados existentes que dependían de estándares. De forma similar, después de desactivar los resultados consolidados de control, el CSPM de Security Hub puede tardar hasta 24 horas en generar nuevos resultados basados en estándares y archivar los resultados consolidados existentes. Durante estos periodos, es posible que vea una combinación de resultados que no dependen de estándares y resultados basados en estándares en la cuenta.

Security Hub CSPM console

Para habilitar o desactivar los resultados consolidados de control

1. Abra la consola CSPM de AWS Security Hub en. https://console.aws.amazon.com/securityhub/
2. En el panel de navegación, en Configuración, seleccione General.
3. En la sección Controles, elija Editar.
4. Use el conmutador Resultados consolidados de control para habilitar o desactivar los resultados consolidados de control.
5. Seleccione Save.

Security Hub CSPM API

Para habilitar o desactivar los resultados consolidados de control mediante programación utilice la operación UpdateSecurityHubConfiguration de la API del CSPM de Security Hub. O bien, si está utilizando elAWS CLI, ejecute el update-security-hub-configurationcomando.

Para el parámetro `control-finding-generator`, especifique `SECURITY_CONTROL` para habilitar los resultados consolidados de control. Para desactivar los resultados consolidados de control, especifique `STANDARD_CONTROL`.

Por ejemplo, el siguiente AWS CLI comando habilita los hallazgos de control consolidados.

```
$ aws securityhub  --region us-east-1 update-security-hub-configuration --control-finding-generator SECURITY_CONTROL
```

El siguiente AWS CLI comando desactiva las conclusiones de control consolidadas.

```
$ aws securityhub  --region us-east-1 update-security-hub-configuration --control-finding-generator STANDARD_CONTROL
```

Generación, actualización y archivado de resultados de control

El CSPM de Security Hub ejecuta comprobaciones de seguridad según una programación. La primera vez que Security Hub CSPM ejecuta una comprobación de seguridad para un control, genera un nuevo hallazgo para cada AWS recurso que el control comprueba. Cada vez que el

CSPM de Security Hub ejecuta posteriormente una comprobación de seguridad para el control, actualiza los resultados existentes para reflejar los resultados de la comprobación. Esto significa que puede utilizar los datos de resultados individuales para hacer un seguimiento de cómo cambia el cumplimiento de determinados recursos con respecto a controles específicos.

Por ejemplo, si el estado de cumplimiento de un recurso cambia de `FAILED` a `PASSED` para un control determinado, el CSPM de Security Hub no genera un resultado nuevo. En su lugar, el CSPM de Security Hub actualiza el resultado existente para el control y el recurso. En el resultado, el CSPM de Security Hub cambia el valor del campo de estado de cumplimiento `Compliance.Status` a `PASSED`. El CSPM de Security Hub también actualiza los valores de otros campos adicionales para reflejar los resultados de la comprobación. Por ejemplo, la etiqueta de gravedad, el estado del flujo de trabajo y las marcas de tiempo que indican cuándo el CSPM de Security Hub ejecutó la comprobación más recientemente y actualizó el resultado.

Al reportar cambios en el estado de cumplimiento, el CSPM de Security Hub podría actualizar cualquiera de los siguientes campos en un resultado de control:

- `Compliance.Status`: el nuevo estado de cumplimiento del recurso para el control especificado.
- `FindingProviderFields.Severity.Label`: la nueva representación cualitativa de la gravedad del resultado, como `LOW`, `MEDIUM` o `HIGH`.
- `FindingProviderFields.Severity.Original`: la nueva representación cuantitativa de la gravedad del resultado, como `0` para un recurso conforme.
- `FirstObservedAt`: cuándo cambió por última vez el estado de cumplimiento del recurso.
- `LastObservedAt`: cuándo el CSPM de Security Hub ejecutó más recientemente la comprobación de seguridad para el control y el recurso especificados.
- `ProcessedAt`: cuándo el CSPM de Security Hub comenzó más recientemente a procesar el resultado.
- `ProductFields.PreviousComplianceStatus`: el estado de cumplimiento anterior (`Compliance.Status`) del recurso para el control especificado.
- `UpdatedAt`: cuándo el CSPM de Security Hub actualizó más recientemente el resultado.
- `Workflow.Status`: el estado de la investigación del resultado, basado en el nuevo estado de cumplimiento del recurso para el control especificado.

Si el CSPM de Security Hub actualiza un campo depende principalmente de los resultados de la comprobación de seguridad más reciente para el control y el recurso correspondientes. Por ejemplo, si el estado de cumplimiento de un recurso cambia de `PASSED` a `FAILED` para un control

determinado, el CSPM de Security Hub cambia el estado del flujo de trabajo del resultado a `NEW`. Para hacer seguimiento a las actualizaciones de resultados individuales, puede consultar el historial de un resultado. Para obtener detalles sobre campos individuales en los resultados, consulte el Formato de resultados de seguridad de AWS (ASFF).

En ciertos casos excepcionales, el CSPM de Security Hub genera resultados nuevos cuando un control ejecuta comprobaciones posteriores, en lugar de actualizar los resultados existentes. Esto puede ocurrir si hay un problema con la AWS Config regla que respalda un control. Si esto ocurre, el CSPM de Security Hub archiva el resultado existente y genera un resultado nuevo para cada comprobación. En los nuevos resultados, el estado de cumplimiento es `NOT_AVAILABLE` y el estado del registro es `ARCHIVED`. Tras solucionar el problema con la AWS Config regla, Security Hub CSPM genera nuevas conclusiones y comienza a actualizarlas para realizar un seguimiento de los cambios posteriores en el estado de conformidad de los recursos individuales.

Además de generar y actualizar resultados de control, el CSPM de Security Hub archiva automáticamente los resultados de control que cumplen ciertos criterios. El CSPM de Security Hub archiva un resultado si el control está desactivado, el recurso especificado se elimina o el recurso especificado deja de existir. Un recurso puede dejar de existir porque el servicio asociado ya no se utiliza. Más específicamente, el CSPM de Security Hub archiva automáticamente un resultado de control si cumple el siguiente criterio:

- El resultado no se ha actualizado durante 3 a 5 días. Tenga en cuenta que este archivado basado en ese intervalo de tiempo se realiza solo cuando es posible y no está garantizado.
- Se devolvió la AWS Config evaluación asociada `NOT_APPLICABLE` para determinar el estado de conformidad del recurso especificado.

Para determinar si un resultado está archivado, puede consultar el campo `RecordState` del resultado. Si un resultado está archivado, el valor de este campo es `ARCHIVED`.

El CSPM de Security Hub almacena los resultados de control archivados durante 30 días. Después de 30 días, los resultados caducan y el CSPM de Security Hub los elimina de forma permanente. Para determinar si un resultado de control archivado ha caducado, el CSPM de Security Hub basa su cálculo en el valor del campo `UpdatedAt` del resultado.

Para almacenar resultados de control archivados por más de 30 días, puede exportarlos a un bucket de S3. Puedes hacerlo mediante una acción personalizada con una EventBridge regla de Amazon. Para obtener más información, consulte Uso EventBridge para respuesta y remediación automatizadas.

> **Note**
>
> Antes del 3 de julio de 2025, el CSPM de Security Hub generaba y actualizaba los resultados de control de manera distinta cuando el estado de cumplimiento de un recurso cambiaba para un control. Anteriormente, el CSPM de Security Hub creaba un resultado de control nuevo y archivaba el resultado existente para un recurso. Por lo tanto, podría tener varios resultados archivados para un control y recurso en particular hasta que dichos resultados caducaran (después de 30 días).

Automatización y supresión de resultados de control

Puede usar reglas de automatización del CSPM de Security Hub para actualizar o suprimir resultados de control específicos. Aún si suprime un resultado, podrá acceder a este. Sin embargo, la supresión indica que considera que no es necesario realizar ninguna acción para abordar el resultado.

La supresión de resultados puede reducir el ruido que estos generan. Por ejemplo, podría suprimir resultados de control que se generan en cuentas de prueba. O bien, podría suprimir resultados relacionados con recursos específicos. Para obtener más información sobre cómo actualizar o suprimir resultados automáticamente, consulte Descripción de las reglas de automatización en el CSPM de Security Hub.

Las reglas de automatización son adecuadas cuando desea actualizar o suprimir resultados de control específicos. Sin embargo, si un control no es relevante para la organización o caso de uso, recomendamos desactivar el control. Si desactiva un control, el CSPM de Security Hub no ejecuta comprobaciones de seguridad para ese control y no se cobra por él.

Detalles de cumplimiento para los resultados de control

En las conclusiones generadas por las comprobaciones de seguridad de los controles, el objeto de conformidad y los campos del formato de comprobación de AWS seguridad (ASFF) proporcionan los detalles de conformidad de los recursos individuales comprobados por un control. Esto incluye la siguiente información:

- `AssociatedStandards`: los estándares habilitados en los que el control está habilitado.
- `RelatedRequirements`: los requisitos relacionados correspondientes al control en todos los estándares habilitados. Estos requisitos derivan de marcos de seguridad de terceros aplicables al

control, como el estándar Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago (PCI DSS) o el estándar NIST SP 800-171 Revisión 2.

- `SecurityControlId`: el identificador del control en los estándares que el CSPM de Security Hub admite.
- `Status`: el resultado de la comprobación más reciente que el CSPM de Security Hub ejecutó para el control. Los resultados de comprobaciones anteriores se retienen en el historial del resultado.
- `StatusReasons`: una matriz que enumera los motivos del valor especificado en el campo `Status`. Para cada motivo, esto incluye un código de motivo y una descripción.

En la siguiente tabla aparecen los códigos de motivo y las descripciones que un resultado podría incluir en la matriz `StatusReasons`. Los pasos de remediación varían según el control que haya generado un resultado con un código de motivo específicado. Para consultar la guía de remediación de un control, consulte la Referencia de controles para el CSPM de Security Hub.

Código de motivo	Compliance status (Estado de conformidad)	Description (Descripción)
`CLOUDTRAIL_METRIC_FILTER_NOT_VALID`	`FAILED`	El registro CloudTrail multirregional no tiene un filtro métrico válido.
`CLOUDTRAIL_METRIC_FILTERS_NOT_PRESENT`	`FAILED`	Los filtros métricos no están presentes en el sendero multirregional. CloudTrail
`CLOUDTRAIL_MULTI_REGION_NOT_PRESENT`	`FAILED`	La cuenta no tiene un registro multirregional CloudTrail con la configuración requerida.
`CLOUDTRAIL_REGION_INVAILD`	`WARNING`	Multi-Region CloudTrail los senderos no están en la región actual.
`CLOUDWATCH_ALARM_ACTIONS_NOT_VALID`	`FAILED`	No hay acciones de alarma válidas presentes.
`CLOUDWATCH_ALARMS_NOT_PRESENT`	`FAILED`	CloudWatch las alarmas no existen en la cuenta.

Código de motivo	Compliance status (Estado de conformidad)	Description (Descripción)
`CONFIG_ACCESS_DENIED`	`NOT_AVAILABLE` AWS Configel estado es `ConfigError`	AWS Configacceso denegado. Compruebe que AWS Config está activado y que se le han concedido los permisos suficientes.
`CONFIG_EVALUATIONS_EMPTY`	`PASSED`	AWS Configevaluó sus recursos en función de la regla. La regla no se aplicaba a los AWS recursos incluidos en su ámbito, se eliminaron los recursos especificados o se eliminaron los resultados de la evaluación.
`CONFIG_RECORDER_CUSTOM_ROLE`	`FAILED`(para Config.1)	La AWS Config grabadora utiliza una función de IAM personalizada en lugar de la función AWS Config vinculada al servicio, y el parámetro `includeConfigServiceLinkedRoleCheck` personalizado for Config.1 no está establecido en. `false`
`CONFIG_RECORDER_DISABLED`	`FAILED`(para) Config.1	AWS Configno está activado con la grabadora de configuración encendida.

Código de motivo	Compliance status (Estado de conformidad)	Description (Descripción)
`CONFIG_RECORDER_MISSING_REQUIRED_RESOURCE_TYPES`	`FAILED`(para Config.1)	AWS Configno registra todos los tipos de recursos que correspon den a los controles CSPM de Security Hub habilitados. Active la grabación de los siguientes recursos: . *`Resources that aren't being recorded`*
`CONFIG_RETURNS_NOT_APPLICABLE`	`NOT_AVAILABLE`	El estado de cumplimiento se `NOT_AVAILABLE` debe a que AWS Config devolvió el estado de No aplicable. AWS Configno indica el motivo del estado. Estas son algunas de las posibles razones del estado de No aplicable: • El recurso se ha eliminado del ámbito de aplicación de la AWS Config regla. • Se ha eliminado la AWS Config regla. • Se ha eliminado el recurso. • La lógica de la AWS Config regla puede generar un estado de No aplicable.

Código de motivo	Compliance status (Estado de conformidad)	Description (Descripción)
`CONFIG_RULE_EVALUATION_ERROR`	`NOT_AVAILABLE` AWS Configel estado es `ConfigError`	Este código de motivo se utiliza para varios tipos diferentes de errores de evaluación. La descripción proporciona la información específica del motivo. El tipo de error puede ser uno de los siguientes: • Incapacidad de realizar la evaluación debido a la falta de permisos. La descripción proporciona el permiso específico que falta. • Un valor ausente o no válido para un parámetro. La descripción proporciona el parámetro y los requisitos para el valor del parámetro. • Error al leer en un bucket de S3. La descripción identifica el bucket y proporciona el error específico. • Falta una AWS suscripción. • Un tiempo de espera general en la evaluación. • Una cuenta suspendida.
`CONFIG_RULE_NOT_FOUND`	`NOT_AVAILABLE` AWS Configel estado es `ConfigError`	La AWS Config regla está en proceso de creación.

Código de motivo	Compliance status (Estado de conformidad)	Description (Descripción)
`INTERNAL_SERVICE_ERROR`	`NOT_AVAILABLE`	Se ha producido un error desconocido.
`LAMBDA_CUSTOM_RUNTIME_DETAILS_NOT_AVAILABLE`	`FAILED`	El CSPM de Security Hub no puede realizar una comprobación en un tiempo de ejecución de Lambda personalizado.
`S3_BUCKET_CROSS_ACCOUNT_CROSS_REGION`	`WARNING`	El resultado está en un estado `WARNING` porque el bucket de S3 asociado a esta regla se encuentra en una región o cuenta diferente. Esta regla no admite comprobaciones entre regiones ni entre cuentas. Se recomienda deshabilitar este control en esta región o cuenta. Ejecútelo solo en la región o cuenta donde se encuentra el recurso.
`SNS_SUBSCRIPTION_NOT_PRESENT`	`FAILED`	Los filtros de métricas de CloudWatch Logs no tienen una suscripción a Amazon SNS válida.

Código de motivo	Compliance status (Estado de conformidad)	Description (Descripción)
`SNS_TOPIC_CROSS_ACCOUNT`	`WARNING`	El resultado se encuentra en un estado de `WARNING`. El tema de SNS asociado a esta regla es propiedad de otra cuenta. La cuenta actual no puede obtener la información de la suscripción. La cuenta propietaria del tema de SNS debe conceder a la cuenta actual el permiso `sns:ListSubscriptionsByTopic` para el tema de SNS.
`SNS_TOPIC_CROSS_ACCOUNT_CROSS_REGION`	`WARNING`	El resultado se encuentra en un estado de `WARNING`, porque el tema de SNS asociado a esta regla se encuentra en una región o cuenta diferente. Esta regla no admite comprobaciones entre regiones ni entre cuentas. Se recomienda deshabilitar este control en esta región o cuenta. Ejecútelo solo en la región o cuenta donde se encuentra el recurso.
`SNS_TOPIC_INVALID`	`FAILED`	El tema de SNS asociado a esta regla no es válido.
`THROTTLING_ERROR`	`NOT_AVAILABLE`	La operación de la API relevante superó la tasa permitida.

ProductFields detalles de los hallazgos de control

En los resultados generados por las comprobaciones de seguridad de los controles, el ProductFieldsatributo del formato de búsqueda de AWS seguridad (ASFF) puede incluir los siguientes campos.

`ArchivalReasons:0/Description`

Describe por qué el CSPM de Security Hub archivó un resultado.

Por ejemplo, el CSPM de Security Hub archiva los resultados existentes cuando se desactiva un control o un estándar, o cuando se habilita o desactiva la funcionalidad de resultados consolidados de control.

`ArchivalReasons:0/ReasonCode`

Especifica por qué el CSPM de Security Hub archivó un resultado.

Por ejemplo, el CSPM de Security Hub archiva los resultados existentes cuando se desactiva un control o un estándar, o cuando se habilita o desactiva la funcionalidad de resultados consolidados de control.

`PreviousComplianceStatus`

El estado de cumplimiento previo (`Compliance.Status`) del recurso para el control especificado, según la actualización más reciente del resultado. Si el estado de cumplimiento del recurso no cambió durante la actualización más reciente, este valor es igual al valor del campo `Compliance.Status` del resultado. Para obtener una lista de los posibles valores, consulte Evaluación del estado de cumplimiento y del estado del control.

`StandardsGuideArn` o `StandardsArn`

El ARN del estándar asociado con el control.

Para el estándar CIS AWS Foundations Benchmark, el campo es`StandardsGuideArn`. Para los estándares PCI DSS y AWS Foundational Security Best Practices, el campo es. `StandardsArn`

Estos campos se eliminan en favor de `Compliance.AssociatedStandards` si habilita los resultados de control consolidados.

`StandardsGuideSubscriptionArn` o `StandardsSubscriptionArn`

El ARN de la suscripción de la cuenta al estándar.

Para el estándar CIS AWS Foundations Benchmark, el campo es`StandardsGuideSubscriptionArn`. Para los estándares PCI DSS y AWS Foundational Security Best Practices, el campo es. `StandardsSubscriptionArn`

Estos campos se eliminan si habilita los resultados de control consolidados.

`RuleId` o `ControlId`

El identificador del control.

Para la versión 1.2.0 del estándar CIS AWS Foundations Benchmark, el campo es`RuleId`. Para otros estándares, incluidas las versiones posteriores del estándar de Indicador de referencia de AWS de CIS, el campo es `ControlId`.

Estos campos se eliminan en favor de `Compliance.SecurityControlId` si habilita los resultados de control consolidados.

`RecommendationUrl`

La URL de la información de remediación del control. Este campo se elimina a favor de `Remediation.Recommendation.Url` si habilita los resultados de control consolidados.

`RelatedAWSResources:0/name`

El nombre del recurso asociado a el resultado.

`RelatedAWSResource:0/type`

El tipo de recurso asociado con el control.

`StandardsControlArn`

El ARN del control. Este campo se elimina si habilita los resultados de control consolidados.

`aws/securityhub/ProductName`

Para los resultados de control, el nombre del producto es `Security Hub`.

`aws/securityhub/CompanyName`

Para los resultados de control, el nombre de la empresa es `AWS`.

`aws/securityhub/annotation`

Una descripción del problema descubierto por el control.

`aws/securityhub/FindingId`

El identificador del resultado.

Este campo no hace referencia a un estándar si habilita los resultados de control consolidados.

Niveles de gravedad correspondientes a los resultados de control

La gravedad asignada a un control del CSPM de Security Hub indica la importancia del control. La gravedad de un control determina la etiqueta de gravedad asignada a los resultados del control.

Criterios de gravedad

La gravedad de un control se determina en función de la evaluación de los siguientes criterios:

- ¿Cómo de difícil es para un agente de amenazas aprovechar la debilidad de la configuración asociada al control? La dificultad viene determinada por el grado de sofisticación o complejidad que se requiere para utilizar la debilidad para llevar a cabo un escenario de amenaza.
- ¿Qué posibilidades hay de que la debilidad comprometa sus recursos Cuentas de AWS o sus recursos? Si sus recursos se Cuentas de AWS ven comprometidos, la confidencialidad, la integridad o la disponibilidad de sus datos o AWS infraestructura se ven afectadas de alguna manera. La probabilidad de que se ponga en peligro indica la probabilidad de que el escenario de amenaza provoque una interrupción o una violación de sus recursos Servicios de AWS o de sus recursos.

Como ejemplo, fíjese en las siguientes debilidades de configuración:

- Las claves de acceso de los usuarios no se renuevan cada 90 días.
- Existe la clave de usuario raíz de IAM.

Ambas debilidades son igualmente difíciles de aprovechar para un adversario. En ambos casos, el adversario puede utilizar el robo de credenciales o algún otro método para adquirir una clave de usuario. Luego pueden usarla para acceder a sus recursos de forma no autorizada.

Sin embargo, la probabilidad de que se ponga en peligro es mucho mayor si el autor de la amenaza adquiere la clave de acceso del usuario raíz, ya que esto le da un mayor acceso. Como resultado, la debilidad clave del usuario raíz es más grave.

La gravedad no tiene en cuenta la criticidad del recurso subyacente. El nivel de importancia crítica se define como el nivel de importancia de los recursos que están asociados con el resultado. Por ejemplo, un recurso asociado a una aplicación crítica para la misión es más importante que uno

asociado a pruebas que no son de producción. Para recopilar información sobre la criticidad de los recursos, utilice el `Criticality` campo del formato de búsqueda de AWS seguridad (ASFF).

La siguiente tabla muestra la dificultad de explotación y la probabilidad de que las etiquetas de seguridad se vean comprometidas.

	Compromiso muy probable	Compromiso probable	Compromiso poco probable	Compromiso muy poco probable
Muy fácil de explotar	Critico	Critico	Alto	Medio
Algo fácil de explotar	Critico	Alto	Medio	Medio
Algo difícil de explotar	Alto	Medio	Medio	Bajo
Muy difícil de explotar	Medio	Medio	Bajo	Bajo

Definiciones de gravedad

Las etiquetas de gravedad se definen de la siguiente manera.

Crítico: el problema debe solucionarse de inmediato para evitar una escalada.

Por ejemplo, un bucket de S3 abierto se considera un hallazgo de gravedad crítica. Debido a que muchos agentes exploran buckets S3 abiertos, es probable que otros detecten los datos de un bucket de S3 expuesto y accedan a ellos.

En general, los recursos que son de acceso público se consideran problemas de seguridad críticos. Debe tratar los resultados críticos con la máxima urgencia. También debe tener en cuenta la criticidad del recurso.

Alto: el problema debe abordarse con prioridad a corto plazo.

Por ejemplo, si un grupo de seguridad de VPC predeterminado está abierto al tráfico entrante y saliente, se considera de gravedad alta. Es bastante fácil para un actor de amenazas

comprometer un VPC mediante este método. También es probable que el actor de la amenaza pueda interrumpir o exfiltrar los recursos una vez que estén en el VPC.

El CSPM de Security Hub recomienda que trate un resultado de alta gravedad como una prioridad a corto plazo. Debe tomar medidas correctivas de inmediato. También debe tener en cuenta la criticidad del recurso.

Medio: el tema debe abordarse como una prioridad a medio plazo.

Por ejemplo, la falta de cifrado de los datos en tránsito se considera un resultado de gravedad media. Se requiere un sofisticado ataque de intermediarios para aprovechar esta debilidad. Es decir, es algo difícil. Es probable que algunos datos se vean comprometidos si el escenario de amenaza tiene éxito.

El CSPM de Security Hub recomienda que investigue el recurso implicado tan pronto como le sea posible. También debe tener en cuenta la criticidad del recurso.

Bajo: el problema no requiere acción por sí solo.

Por ejemplo, la falta de recopilación de información forense se considera de gravedad baja. Este control puede ayudar a evitar futuros compromisos, pero la ausencia de análisis forense no conduce directamente a un compromiso.

No es necesario tomar medidas inmediatas ante los resultados de baja gravedad, pero pueden proporcionar un contexto si los correlacionas con otros problemas.

Informativo: no se encontró ningún punto débil en la configuración.

En otras palabras, el estado es `PASSED`, `WARNING` o `NOT AVAILABLE`.

No se recomienda ninguna acción. Los resultados informativos ayudan a los clientes a demostrar que están en un estado de conformidad.

Evaluación del estado de cumplimiento y del estado del control

El `Compliance.Status` campo del formato de comprobación de AWS seguridad describe el resultado de una comprobación de control. AWSSecurity Hub CSPM utiliza el estado de conformidad de los hallazgos de control para determinar un estado de control general. El estado del control se muestra en la página de detalles de un control en la consola del CSPM de Security Hub.

Evaluación del estado de cumplimiento de los resultados del CSPM de Security Hub

El estado de conformidad para cada resultado se asigna uno de los siguientes valores:

- PASSED: indica que el control superó la comprobación de seguridad correspondiente al resultado. Esto establece de forma automática el Workflow.Status del CSPM de Security Hub en RESOLVED.
- FAILED: indica que el control no superó la comprobación de seguridad correspondiente al resultado.
- WARNING: indica que el CSPM de Security Hub no puede determinar si el recurso se encuentra en un estado PASSED o FAILED. Por ejemplo, si el registro de recursos de AWS Config no se encuentra activado para el tipo de recurso correspondiente.
- NOT_AVAILABLE— Indica que la comprobación no se puede completar porque se ha producido un error en el servidor, se ha eliminado el recurso o se ha producido el resultado de la AWS Config evaluación. NOT_APPLICABLE Si el resultado AWS Config de la evaluación fueNOT_APPLICABLE, Security Hub CSPM archiva automáticamente el hallazgo.

Si el estado de cumplimiento de un resultado cambia de PASSED a FAILED, WARNING o NOT_AVAILABLE, y Workflow.Status era NOTIFIED o RESOLVED, el CSPM de Security Hub cambia de forma automática Workflow.Status a NEW.

Si no cuenta con recursos correspondientes a un control, el CSPM de Security Hub genera un resultado PASSED a nivel de la cuenta. Si cuenta con un recurso correspondiente a un control y luego elimina ese recurso, el CSPM de Security Hub crea un resultado NOT_AVAILABLE y lo archiva de inmediato. Después de 18 horas, recibe un resultado PASSED porque ya no cuenta con recursos correspondientes al control.

Obtención del estado de control a partir del estado de conformidad

El CSPM de Security Hub deriva un estado general del control a partir del estado de cumplimiento de los resultados del control. Al determinar el estado del control, el CSPM de Security Hub ignora los resultados con RecordState de ARCHIVED, y los resultados con Workflow.Status de SUPPRESSED.

El estado de control tiene asignado uno de los siguientes valores:

- Aprobado: indica que todos los resultados tienen un estado de conformidad como PASSED.
- Con fallos: indica que al menos un resultado tiene un estado de conformidad como FAILED.
- Desconocido: indica que al menos un resultado tiene un estado de conformidad como WARNING o NOT_AVAILABLE. Ningún resultado tiene un estado de conformidad como FAILED.

- Sin datos: indica que no hay ningún resultado para el control. Por ejemplo, un control recién habilitado presenta este estado hasta que el CSPM de Security Hub empieza a generar resultados para dicho control. Un control también presenta este estado si todos sus resultados son `SUPPRESSED` o si no se encuentra disponible en la Región de AWS actual.
- Desactivado: indica que el control está desactivado en la cuenta actual y en la región. No se están realizando controles de seguridad para este control en la cuenta y la región actuales. Sin embargo, los resultados de un control desactivado pueden tener un valor para el estado de conformidad hasta 24 horas después de la desactivación.

Para una cuenta de administrador, el estado del control refleja su estado para la cuenta de administrador y para las cuentas de miembro. En concreto, el estado general de un control aparece como Con fallos si el control tiene uno o más resultados fallidos en la cuenta del administrador o en cualquiera de las cuentas de los miembros. Si estableció una región de agregación, el estado de control de la región de agregación refleja el estado de control de dicha región y las regiones vinculadas. En concreto, el estado general de un control aparece como Con fallos si el control tiene uno o más resultados fallidos en la región de agregación o en cualquiera de las regiones vinculadas.

El CSPM de Security Hub normalmente genera el estado inicial del control dentro de los 30 minutos posteriores a su primera visita a la página Resumen o a la página de Estándares de seguridad en la consola del CSPM de Security Hub. El registro de recursos de AWS Config debe estar configurado para que aparezca el estado de control. Una vez generados los estados de control por primera vez, el CSPM de Security Hub los actualiza cada 24 horas con base en los resultados del periodo anterior. Una marca de tiempo en la página de detalles de control indica cuándo se actualizó por última vez el estado de control.

> **Note**
>
> Después de habilitar un control por primera vez, el proceso puede tardar hasta 24 horas para que se generen los estados de control en las regiones de China y en la AWS GovCloud (US) Region.

Calcular las puntuaciones de seguridad

En la consola CSPM de AWS Security Hub, la página de resumen y la página de controles muestran un resumen de la puntuación de seguridad para todos los estándares habilitados. En la

página Estándares de seguridad, el CSPM de Security Hub también muestra una puntuación de seguridad entre 0 y 100 por ciento para cada estándar habilitado.

Cuando habilita por primera vez el CSPM de Security Hub, este calcula la puntuación de seguridad resumida y las puntuaciones de seguridad por estándar dentro de los primeros 30 minutos después de su visita inicial a la página Resumen o a la página Estándares de seguridad en la consola. Las puntuaciones se generan únicamente para los estándares que están habilitados cuando visita esas páginas en la consola. Además, debe configurar el registro de recursos de AWS Config para que aparezcan las puntuaciones La puntuación de seguridad resumida es el promedio de las puntuaciones de seguridad estándar. Para revisar una lista de los estándares que están habilitados actualmente, puede utilizar el GetEnabledStandards funcionamiento de la API CSPM de Security Hub.

Tras la primera generación de puntuaciones, el CSPM de Security Hub actualiza las puntuaciones de seguridad cada 24 horas. El CSPM de Security Hub muestra una marca de tiempo que indica cuándo se actualizó por última vez la puntuación de seguridad. Tenga en cuenta que la generación inicial de puntuaciones de seguridad puede tardar hasta 24 horas en las regiones de China y en AWS GovCloud (US) Regions.

Si activa los resultados de control consolidados, es posible que las puntuaciones de seguridad tarden hasta 24 horas en actualizarse. Además, al habilitar una nueva región de agregación o actualizar las regiones vinculadas, se restablecen las puntuaciones de seguridad existentes. El CSPM de Security Hub puede tardar hasta 24 horas en generar nuevas puntuaciones de seguridad que incluyan los datos de las regiones actualizadas.

Método de cálculo de las puntuaciones de seguridad

La puntuación de seguridad representa la proporción de controles superados frente a los controles habilitados. La puntuación se muestra como un porcentaje redondeado hacia arriba o hacia abajo hasta el número entero más cercano.

El CSPM de Security Hub calcula una puntuación de seguridad resumida que abarca todos los estándares que tiene habilitados. El CSPM de Security Hub también calcula una puntuación de seguridad para cada estándar habilitado. Para calcular la puntuación, los controles habilitados incluyen los controles con los estados Aprobado, Con fallos y Desconocido. Los controles cuyo estado es Sin datos se excluyen del cálculo de la puntuación.

El CSPM de Security Hub omite los resultados archivados y suprimidos al calcular el estado de los controles. Esto puede afectar a las puntuaciones de seguridad. Por ejemplo, si suprime todos los

resultados fallidos de un control, su estado pasa a ser Aprobado, lo que a su vez puede mejorar sus puntuaciones de seguridad. Para obtener más información sobre el estado de control, consulte Evaluación del estado de cumplimiento y del estado del control.

Ejemplo de puntuación:

Standard	Controles superados	Controles con errores	Controles desconocidos	Puntuación estándar
AWS Mejores prácticas básicas de seguridad v1.0.0	168	22	0	88%
CIS AWS Foundations Benchmark v1.4.0	8	29	0	22%
CIS AWS Foundations Benchmark v1.2.0	6	35	0	15%
Publicación especial 800-53 del NIST, revisión 5	159	56	0	74%
PCI DSS v3.2.1	28	17	0	62%

Al calcular la puntuación de seguridad resumida, el CSPM de Security Hub contabiliza cada control una sola vez, incluso si pertenece a varios estándares. Por ejemplo, si ha habilitado un control que se aplica a tres estándares habilitados, solo cuenta como un control habilitado a efectos de puntuación.

En este ejemplo, aunque el número total de controles habilitados en todos los estándares es 528, el CSPM de Security Hub cuenta cada control único solo una vez para fines de puntuación. Es

probable que el número de controles habilitados únicos sea inferior a 528. Si suponemos que el número de controles habilitados únicos es 515 y el número de controles únicos aprobados es 357, la puntuación resumida es del 69 %. Esta puntuación se calcula dividiendo el número de controles únicos aprobados entre el número de controles únicos habilitados.

Puede obtener una puntuación resumida distinta de la puntuación estándar, incluso si solo habilitó un estándar en su cuenta dentro de la región actual. Esto puede suceder si inició sesión con una cuenta de administrador y las cuentas de miembro tienen estándares adicionales o estándares diferentes habilitados. Esto también puede suceder si consulta la puntuación desde la región de agregación y existen estándares adicionales o distintos habilitados en regiones vinculadas.

Puntuaciones de seguridad para las cuentas de administrador

Si ha iniciado sesión en una cuenta de administrador, la puntuación de seguridad resumida y la puntuación estándar representan los estados de control de la cuenta de administrador y de todas las cuentas de los miembros.

Si el estado de un control es Con fallos incluso en la cuenta de un miembro, su estado es Con fallos en la cuenta de administrador y afecta a las puntuaciones de la cuenta de administrador.

Si ha iniciado sesión en una cuenta de administrador y está consultando las puntuaciones de una región de agregación, las puntuaciones de seguridad representan los estados de control de todas las cuentas de los miembros y de todas las regiones vinculadas.

Puntuaciones de seguridad si ha establecido una región de agregación

Si ha establecido una agregación Región de AWS, la puntuación de seguridad resumida y la puntuación estándar tienen en cuenta los estados de control en general
regiones vinculadas.

Si el estado de un control es Con fallos incluso en una región vinculada, su estado es Con fallos en la región de agregación y afecta a las puntuaciones de la región de agregación.

Si ha iniciado sesión en una cuenta de administrador y está consultando las puntuaciones de una Región de agregación, las puntuaciones de seguridad representan los estados de control de todas las cuentas de los miembros y de todas las regiones vinculadas.

Categorías de controles en el CSPM de Security Hub

A cada control se le asigna una categoría. La categoría de un control refleja la función de seguridad a la que se aplica el control.

El valor de la categoría contiene la categoría, la subcategoría dentro de la categoría y, opcionalmente, un clasificador dentro de la subcategoría. Por ejemplo:

- Identificación > Inventario
- Proteger > Protección de datos > Cifrado de datos en tránsito

Estas son las descripciones de las categorías, subcategorías y clasificadores disponibles.

Identificar

Desarrollar la comprensión organizativa para administrar el riesgo de ciberseguridad para sistemas, activos, datos y capacidades.

Inventario

¿Ha implementado el servicio las estrategias correctas de etiquetado de recursos? ¿Las estrategias de etiquetado incluyen al propietario del recurso?

¿Qué recursos utiliza el servicio? ¿Son recursos aprobados para este servicio?

¿Tiene visibilidad del inventario aprobado? Por ejemplo, ¿utiliza servicios como Amazon EC2 Systems Manager y Service Catalog?

Registro

¿Ha habilitado de forma segura todos los registros relevantes para el servicio? Los ejemplos de archivos de registros incluyen los siguientes:

- Registros de flujo de Amazon VPC
- Registros de acceso de Elastic Load Balancing
- CloudFront Registros de Amazon
- Amazon CloudWatch Logs
- Registro de Amazon Relational Database Service
- Registros de indexación lentos de Amazon OpenSearch Service
- X-Ray rastreo
- AWS Directory Serviceregistros
- AWS Configartículos
- Snapshots

Protección

Desarrollar y aplicar las protecciones adecuadas para garantizar la prestación de servicios de infraestructura críticos y prácticas de codificación seguras.

Gestión segura del acceso

- ¿Utiliza el servicio las prácticas de menos privilegios en sus políticas de IAM o de recursos?
- ¿Las contraseñas y los secretos son lo suficientemente complejos? ¿Se rotan apropiadamente?
- ¿Utiliza el servicio la autenticación multifactor (MFA)?
- ¿El servicio evita el usuario raíz?
- ¿Las políticas basadas en recursos permiten el acceso público?

Configuración de red segura

- ¿El servicio evita el acceso público y no seguro a la red remota?
- ¿El servicio utiliza la VPC correctamente? Por ejemplo, ¿se requieren trabajos para ejecutarse en la VPC?
- ¿El servicio segmenta y aísla adecuadamente los recursos confidenciales?

Protección de datos

- Cifrado de datos en reposo: ¿el servicio cifra los datos en reposo?
- Cifrado de datos en tránsito: ¿el servicio cifra los datos en tránsito?
- Integridad de los datos: ¿el servicio valida la integridad de los datos?
- Protección contra la eliminación de datos: ¿protege el servicio los datos contra la eliminación accidental?
- Administración/Uso de datos: ¿Utiliza servicios como Amazon Macie para rastrear la ubicación de sus datos confidenciales?

Protección de API

- ¿El servicio se utiliza AWS PrivateLink para proteger las operaciones de la API del servicio?

Servicios de protección

¿Los servicios de protección adecuados están bien ubicados? ¿Proporcionan la cantidad correcta de cobertura?

Los servicios de protección le ayudan a desviar los ataques y compromisos dirigidos al servicio. Algunos ejemplos de servicios de protección AWS incluyenAWS Control Tower, AWS WAFAWS Shield Advanced, Vanta, Secrets Manager, IAM Access Analyzer y. AWS Resource Access Manager

Desarrollo seguro

¿Utiliza prácticas de codificación seguras?

¿Evita vulnerabilidades como el Top Ten de Open Web Application Security Project (OWASP)?

Detect

Desarrolle e implemente las actividades apropiadas para identificar la ocurrencia de un evento de ciberseguridad.

Servicios de detección

¿Existen los servicios de detección correctos?

¿Proporcionan la cantidad correcta de cobertura?

Algunos ejemplos de servicios de AWS detección incluyen Amazon GuardDuty, AWS Security Hub CSPM, Amazon Inspector, Amazon DetectiveAWS IoT Device Defender, Amazon CloudWatch Alarms y. AWS Trusted Advisor

Respuesta

Desarrolle e implemente las actividades apropiadas para tomar medidas relacionadas con la detección de un evento de ciberseguridad.

Acciones de respuesta

¿Responde rápidamente a los eventos de seguridad?

¿Tiene hallazgos críticos o de alta gravedad activos?

Forenses

¿Puede adquirir datos forenses de forma segura para el servicio? Por ejemplo, ¿adquiere instantáneas de Amazon EBS asociadas con verdaderos resultados positivos?

¿Has creado una cuenta forense?

Recuperar

Desarrolle e implemente las actividades apropiadas para mantener planes de resiliencia y restaurar cualquier capacidad o servicio que se haya visto afectado debido a un evento de ciberseguridad.

Resiliencia

¿La configuración del servicio admite conmutaciones por error elegantes, escalado elástico y alta disponibilidad?

¿Has establecido copias de seguridad?

Cómo revisar los detalles de los controles en el CSPM de Security Hub

Al seleccionar un control en la página Controles o en la página de detalles estándar de la consola de CSPM de Security Hub, accederá a la página de detalles del control.

En la parte superior de la página de detalles del control se indica el estado de control. El estado de control resume el rendimiento de un control en función del estado de conformidad de los resultados del control. Por lo general, el CSPM de Security Hub genera el estado de control inicial 30 minutos después de la primera visita a la página Resumen o a la página Estándares de seguridad de la consola del CSPM de Security Hub. Los estados solo están disponibles para los controles que están habilitados al visitar esas páginas.

La página de detalles del control también muestra un desglose del estado de cumplimiento de los resultados del control durante las últimas 24 horas. Para obtener más información sobre el estado de control y el estado de conformidad, consulte Evaluación del estado de cumplimiento y del estado del control.

AWS Config el registro de recursos debe configurarse para que aparezca el estado del control. Una vez que se generan por primera vez los estados de control, el CSPM de Security Hub los actualiza cada 24 horas según los resultados de las 24 horas anteriores.

Las cuentas de administrador ven un estado de control agregado en la cuenta de administrador y en las cuentas de los miembros. Si ha establecido una región de agregación, el estado de control incluye los resultados de todas las regiones vinculadas. Para obtener más información sobre el estado de control, consulte the section called “Estado de conformidad y el estado de control”.

También puede activar o desactivar el control desde la página de detalles de control.

> **Note**
>
> Una vez activado un control, pueden pasar hasta 24 horas hasta que se generen los estados de control por primera vez en las regiones de China y de AWS GovCloud (US) Regions.

La pestaña Estándares y requisitos enumera los estándares para los que se puede habilitar un control y los requisitos relacionados con el control desde diferentes marcos de cumplimiento.

La pestaña Comprobaciones muestra los resultados activos del control correspondientes a las últimas 24 horas. Los resultados del control se generan y se actualizan cuando el CSPM de Security Hub ejecuta las comprobaciones de seguridad del control. La lista que aparece en esta pestaña no incluye los resultados archivados.

Para cada resultado, la lista proporciona acceso a los detalles del resultado, como el estado de cumplimiento y el recurso relacionado. También puede configurar el estado del flujo de trabajo de cada resultado y enviar los resultados a acciones personalizadas. Para obtener más información, consulte Revisión y administración de resultados de controles.

Visualización de detalles de un control

Elija su método de acceso preferido y siga estos pasos para revisar los detalles de un control. Los detalles se aplican a la cuenta corriente y a la región e incluyen lo siguiente:

- El título y la descripción del control.
- Un enlace a la guía de remediación para los resultados de control con errores.
- La gravedad del control.
- Estado del control.

En la consola también puede revisar una lista de resultados recientes del control. Para hacerlo mediante programación, puede usar la operación GetFindings de la API del CSPM de Security Hub.

Security Hub CSPM console

1. Abra la consola CSPM de AWS Security Hub en. https://console.aws.amazon.com/securityhub/
2. En el panel de navegación, elija Control.
3. Seleccione un control.

Security Hub CSPM API

1. Ejecute `ListSecurityControlDefinitions` y proporcione uno o más ARN estándar para obtener una lista de los identificadores de control para ese estándar. Para obtener los ARN estándar, ejecute `DescribeStandards`. Si no proporciona un ARN estándar, esta API devuelve todos los identificadores de control del CSPM de Security Hub. Esta API devuelve los identificadores de control de seguridad independientes de los estándares, no los identificadores de control basados en estándares que existían antes de las versiones de estas características.

   Ejemplo de solicitud:

   ```
   {
       "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/v/1.0.0"
   }
   ```

2. Ejecute `BatchGetSecurityControls` para obtener información sobre uno o más controles de la actual Cuenta de AWS y. Región de AWS

   Ejemplo de solicitud:

   ```
   {
       "SecurityControlIds": ["Config.1", "IAM.1"]
   }
   ```

AWS CLI

1. Ejecute el comando `list-security-control-definitions` y proporcione uno o más ARN estándar para obtener una lista de los identificadores de control. Para obtener los ARN estándar, ejecute el comando `describe-standards`. Si no proporciona un ARN estándar,

este comando devuelve todos los identificadores de control del CSPM de Security Hub. Este comando devuelve los identificadores de control de seguridad independientes de los estándares, no los identificadores de control basados en estándares que existían antes de las versiones de estas características.

```
aws securityhub --region us-east-1 list-security-control-definitions --
standards-arn "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0"
```

2. Ejecute el comando batch-get-security-controls para obtener detalles sobre uno o más controles de en las Región de AWS y Cuenta de AWS actuales.

```
aws securityhub --region us-east-1 batch-get-security-controls --security-
control-ids '["Config.1", "IAM.1"]'
```

Filtrado y ordenación de controles en el CSPM de Security Hub

En la consola CSPM de AWS Security Hub, puede usar la página de controles para revisar una tabla de los controles que están disponibles en la actualidad. Región de AWS La excepción es una región de agregación. Si configuró una región de agregació e inicia sesión en esa región, la consola muestra los controles que están disponibles en la región de agregación o en una o más regiones vinculadas.

Para enfocarse en un subconjunto específico de controles, puede ordenar y filtrar la tabla de controles. Las opciones Filtrar por junto a la tabla pueden ayudarle a enfocarse rápidamente en estos subconjuntos específicos:

- Todos los controles habilitados, que son controles habilitados en al menos un estándar habilitado.
- Todos los controles desactivados, que son controles desactivados en todos los estándares.
- Todos los controles habilitados que tienen un estado de control específico, como Fallido. La opción Sin datos muestra únicamente los controles que no tienen resultados en este momento. Para obtener información sobre el estado del control, consulte Evaluación del estado de cumplimiento y del estado del control.

Además de las opciones Filtrar por, puede filtrar la tabla. Para ello, ingrese los criterios de filtro en el cuadro Filtrar controles que está sobre la tabla. Por ejemplo, puede filtrar por ID de control o gravedad.

De forma predeterminada, los controles con un estado Fallido aparecen primero, en orden descendente según la gravedad. Para cambiar el orden, elija un encabezado de columna diferente.

> **Tip**
>
> Si tiene flujos de trabajo automatizados basados en los resultados del control, recomendamos usar `SecurityControlId` o `SecurityControlArn`, que son campos ASFF, como filtros, en lugar de usar los campos `Title` o `Description`. Estos últimos campos pueden cambiar ocasionalmente, mientras que el ID del control y el ARN son identificadores estáticos.

Si inicia sesión en una cuenta de administrador del CSPM de Security Hub, los controles Habilitados incluyen aquellos que están habilitados en al menos una cuenta de miembro. Si configuró una región de agregación, los controles Habilitados incluyen aquellos que están habilitados en al menos una región vinculada.

Si selecciona la opción junto a un control habilitado, se abre un panel que muestra los estándares en los que dicho control permanece habilitado en este momento. También puede ver los estándares en los que el control está actualmente desactivado. Desde este panel, puede desactivar un control en todos los estándares. Para obtener más información, consulte Desactivación de controles en el CSPM de Security Hub. En las cuentas de administrador, la información del panel refleja la configuración de todas las cuentas de miembro.

Para recuperar una lista de controles mediante programación, puede usar la operación ListSecurityControlDefinitions de la API del CSPM de Security Hub. Para recuperar los detalles de controles individuales, puede usar la operación BatchGetSecurityControls.

Comprensión de los parámetros de control en el CSPM de Security Hub

Algunos controles del CSPM AWS de Security Hub utilizan parámetros que afectan a la forma en que se evalúa el control. Por lo general, dichos controles se evalúan con los valores predeterminados de parámetros que define el CSPM de Security Hub. Sin embargo, para un subconjunto de estos controles, puede modificar los valores de los parámetros. Cuando modifica el valor de un parámetro de control, el CSPM de Security Hub evalúa el control con el valor que especifique. Si el recurso que

subyace el control cumple el valor personalizado, el CSPM de Security Hub genera un resultado `PASSED`. Si el recurso no cumple el valor personalizado, el CSPM de Security Hub genera un resultado `FAILED`.

Al personalizar los parámetros de control, puede ajustar las prácticas recomendadas de seguridad que supervisa y recomienda el CSPM de Security Hub para alinearlas con los requisitos empresariales y expectativas de seguridad. En lugar de suprimir los resultados de un control, puede personalizar uno o varios de sus parámetros para obtener los resultados que se adapten a sus necesidades de seguridad.

Estos son algunos ejemplos de casos de uso para modificar los parámetros de control y establecer valores personalizados:

- [CloudWatch.16] — Los grupos de CloudWatch registro deben conservarse durante un período de tiempo específico

  Puede especificar el periodo de retención.
- [IAM.7] — Las políticas de contraseñas para los usuarios de IAM deben tener configuraciones sólidas

  Puede especificar parámetros relacionados con la seguridad de la contraseña.
- [EC2.18] — Los grupos de seguridad solo deben permitir el tráfico entrante sin restricciones a los puertos autorizados

  Puede especificar qué puertos están autorizados para permitir el tráfico entrante sin restricciones.
- [Lambda.5] — Las funciones de VPC Lambda deben funcionar en varias zonas de disponibilidad

  Puede especificar el número mínimo de zonas de disponibilidad que generará un resultado válido.

En esta sección, se describen los aspectos que se deben tener en cuenta al modificar los parámetros de control.

Efecto de la modificación de los valores de parámetros de control

Al cambiar el valor de un parámetro, también se desencadena un nuevo control de seguridad que evalúa el control en función del nuevo valor. El CSPM de Security Hub genera entonces nuevos resultados del control con base en el nuevo valor. Durante las actualizaciones periódicas de los resultados del control, el CSPM de Security Hub también usa el nuevo valor del parámetro. Si modifica los valores de un parámetro de control pero no habilita ningún estándar que incluya ese

control, el CSPM de Security Hub no ejecuta comprobaciones de seguridad con los nuevos valores. Debe habilitar al menos un estándar pertinente para que el CSPM de Security Hub evalúe el control con base en el nuevo valor del parámetro.

Un control puede tener uno o varios parámetros personalizables. Entre los tipos de datos posibles para cada parámetro de control se encuentran los siguientes:

- Booleano
- Double
- Enum
- EnumList
- Entero
- IntegerList
- Cadena
- StringList

Los valores personalizados de los parámetros se aplican a los estándares habilitados. No puede personalizar los parámetros de un control que no sea compatible en su región actual. Para obtener una lista de los límites regionales para los controles individuales, consulte Límites regionales de los controles del CSPM de Security Hub.

En algunos controles, los valores de los parámetros aceptables deben estar dentro de un rango especificado para ser válidos. En estos casos, el CSPM de Security Hub proporciona el intervalo aceptable.

El CSPM de Security Hub selecciona los valores predeterminados de los parámetros y en ocasiones puede actualizarlos. Después de personalizar un parámetro de control, su valor sigue siendo el valor que especificó para el parámetro, a menos que lo cambie. Es decir, el parámetro deja de adoptar las actualizaciones del valor predeterminado del CSPM de Security Hub, incluso si el valor personalizado coincide con el valor predeterminado vigente definido por el CSPM de Security Hub. Este es un ejemplo del control [ACM.1] — Los ACM-issued certificados se importan y se deben renovar después de un período de tiempo específico:

```
{
    "SecurityControlId": "ACM.1",
    "Parameters": {
        "daysToExpiration": {
```

```
            "ValueType": "CUSTOM",
            "Value": {
                "Integer": 30
            }
        }
    }
}
```

En el ejemplo anterior, el parámetro `daysToExpiration` tiene un valor personalizado de `30`. El valor predeterminado actual para este parámetro también es `30`. Si el CSPM de Security Hub cambia el valor predeterminado a `14`, el parámetro de este ejemplo no adopta ese cambio. Retendrá un valor de `30`.

Si desea adoptar las actualizaciones del valor predeterminado del CSPM de Security Hub para un parámetro, establezca el campo `ValueType` en `DEFAULT`, en lugar de `CUSTOM`. Para obtener más información, consulte Reversión a los parámetros de control predeterminados en una sola cuenta y región.

Controles que admiten parámetros personalizados

Para obtener una lista de los controles de seguridad que admiten parámetros personalizados, consulte la página Controls de la consola del CSPM de Security Hub o la Referencia de controles para el CSPM de Security Hub. Para recuperar esta lista mediante programación, puede utilizar la operación ListSecurityControlDefinitions. En la respuesta, el objeto `CustomizableProperties` indica qué controles admiten parámetros personalizables.

Revisión de los valores actuales de los parámetros de control

Puede resultar útil conocer el valor actual de un parámetro de control antes de modificarlo.

Puede revisar los valores actuales de los parámetros de control individuales de su cuenta. Si utiliza la configuración central, el administrador delegado de CSPM de AWS Security Hub también puede revisar los valores de los parámetros que se especifican en una política de configuración.

Elija el método que prefiera y siga los pasos para revisar los valores actuales de los parámetros de control.

Security Hub CSPM console

Para revisar los valores actuales de los parámetros de control (consola)

1. Abra la consola AWS CSPM de Security Hub en. https://console.aws.amazon.com/securityhub/
2. En el panel de navegación, elija Controles. Elija un control.
3. Elija la pestaña Parámetros. Esta pestaña muestra los valores actuales de los parámetros del control.

Security Hub CSPM API

Para revisar los valores actuales de los parámetros de control (API)

Invoque la API BatchGetSecurityControls y proporcione uno o varios identificadores o ARN de control de seguridad. El objeto `Parameters` de la respuesta muestra los valores actuales de los parámetros de los controles especificados.

Por ejemplo, el siguiente AWS CLI comando muestra los valores de los parámetros actuales para `APIGatway.1``CloudWatch.15`, y. `IAM.7` Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$ aws securityhub batch-get-security-controls \
--region us-east-1 \
--security-control-ids '["APIGateway.1", "CloudWatch.15", "IAM.7"]'
```

Elija el método que prefiera para ver los valores actuales de los parámetros en una política de configuración centralizada.

Security Hub CSPM console

Para revisar los valores actuales de los parámetros de control en una política de configuración (consola)

1. Abra la consola CSPM de AWS Security Hub en. https://console.aws.amazon.com/securityhub/

Inicie sesión con las credenciales de la cuenta de administrador delegado del CSPM de Security Hub en la región de origen.

2. En el panel de navegación, seleccione Configuración y Configuración.
3. En la pestaña Políticas, seleccione la política de configuración y, a continuación, elija Ver detalles. A continuación, aparecen los detalles de la política, incluidos los valores actuales de los parámetros.

Security Hub CSPM API

Para revisar los valores actuales de los parámetros de control en una política de configuración (API)

1. Invoque la API GetConfigurationPolicy desde la cuenta de administrador delegado de la región de origen.
2. Proporcione el ARN o el ID de la política de configuración cuyos detalles quiere ver. La respuesta incluye los valores actuales de los parámetros.

Por ejemplo, el siguiente AWS CLI comando recupera los valores de los parámetros de control actuales de la política de configuración especificada. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$ aws securityhub get-configuration-policy \
--region us-east-1 \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Los resultados de control también incluyen los valores actuales de los parámetros de control. En la AWS Formato de búsqueda de seguridad (ASFF), estos valores aparecen en el campo `Parameters` del objeto `Compliance`. Para revisar los resultados en la consola del CSPM de Security Hub, elija Resultados en el panel de navegación. Para revisar los resultados mediante programación, utilice la operación GetFindings de la API del CSPM de Security Hub.

Personalización de los valores de los parámetros de control

Las instrucciones para personalizar los parámetros de control varían en función de si utiliza la configuración ??? central en el CSPM de Security Hub. AWS La configuración central es una función que el administrador delegado de CSPM de Security Hub puede usar para configurar las capacidades de CSPM de Security Hub en todas Regiones de AWS las cuentas y unidades organizativas (OU).

Si su organización utiliza la configuración central, el administrador delegado puede crear políticas de configuración que incluyan parámetros de control personalizados. Estas políticas se pueden asociar a cuentas de miembros y unidades organizativas administradas de manera centralizada y entran en vigencia en su región de origen y en todas las regiones vinculadas. El administrador delegado también puede designar una o varias cuentas como autoadministradas, lo que permite al propietario de la cuenta configurar sus propios parámetros por separado en cada región. Si su organización no utiliza la configuración centralizada, debe personalizar los parámetros de control por separado en cada cuenta y región.

Recomendamos utilizar la configuración centralizada porque permite alinear los valores de los parámetros de control en las distintas partes de la organización. Por ejemplo, todas sus cuentas de prueba podrían usar determinados valores de parámetros y todas las cuentas de producción podrían utilizar valores diferentes.

Personalización de parámetros de control en varias cuentas y regiones

Si es el administrador delegado del CSPM de Security Hub para una organización que usa la configuración centralizada, seleccione el método de su preferencia y siga los pasos para personalizar los parámetros de control en varias cuentas y regiones.

Security Hub CSPM console

Para personalizar los valores de un parámetro de control en varias cuentas y regiones (consola)

1. Abra la consola CSPM AWS de Security Hub en. https://console.aws.amazon.com/securityhub/

   Asegúrese de que haya iniciado sesión en la región de origen.
2. En el panel de navegación, seleccione Configuración y Configuración.
3. Elija la pestaña Policies.

4. Para crear una nueva política de configuración que incluya parámetros personalizados, elija Crear política. Para especificar los parámetros personalizados en una política de configuración existente, seleccione la política y, luego, elija Editar.

   Para crear una política de configuración nueva con valores de parámetros de control personalizados

   1. En la sección Política personalizada, elija los estándares y controles de seguridad que quiere habilitar.
   2. Seleccione Personalizar los parámetros de control.
   3. Seleccione un control y, a continuación, especifique valores personalizados para uno o varios parámetros.
   4. Para personalizar los parámetros de más controles, elija Personalizar un control adicional.
   5. En la sección Cuentas, seleccione las cuentas o unidades organizativas a las que quiere aplicar la política.
   6. Elija Siguiente.
   7. Elija Crear y aplicar política. Tanto en su región de origen como en todas regiones vinculadas, esta acción anula los ajustes de configuración existentes de las cuentas y unidades organizativas asociadas a esta política de configuración. Las cuentas y las unidades organizativas se pueden asociar a una política de configuración mediante una aplicación directa o la herencia de un elemento principal.

   Para personalizar los valores de un parámetro de control en una política de configuración existente

   1. En la sección Controles, en Política personalizada, especifique los nuevos valores personalizados de parámetros que quiera.
   2. Si es la primera vez que personaliza los parámetros de control en esta política, seleccione Personalizar los parámetros de control y, a continuación, seleccione el control que quiere personalizar. Para personalizar los parámetros de más controles, elija Personalizar un control adicional.
   3. En la sección Cuentas, compruebe las cuentas o unidades organizativas a las que quiere aplicar la política.
   4. Elija Siguiente.

5. Revise los cambios y compruebe que sean correctos. Cuando termine, elija Guardar y aplicar política. Tanto en su región de origen como en todas regiones vinculadas, esta acción anula los ajustes de configuración existentes de las cuentas y unidades organizativas asociadas a esta política de configuración. Las cuentas y las unidades organizativas se pueden asociar a una política de configuración mediante una aplicación directa o la herencia de un elemento principal.

Security Hub CSPM API

Para personalizar los valores de un parámetro de control en varias cuentas y regiones (API)

Para crear una política de configuración nueva con valores de parámetros de control personalizados

1. Invoque la API CreateConfigurationPolicy desde la cuenta de administrador delegado de la región de origen.
2. Para el objeto `SecurityControlCustomParameters`, indique el identificador de cada control que quiere personalizar.
3. Para el objeto `Parameters`, indique el nombre de cada parámetro que quiere personalizar. Para cada parámetro que personalice, indique `CUSTOM` en `ValueType`. En `Value`, indique el tipo de datos del parámetro y el valor personalizado. El campo `Value` no puede estar vacío cuando el valor de `ValueType` es `CUSTOM`. Si la solicitud omite un parámetro que el control admite, ese parámetro conserva su valor actual. Para encontrar los parámetros, los tipos de datos y los valores válidos admitidos para un control, invoque la API GetSecurityControlDefinition.

Para personalizar los valores de un parámetro de control en una política de configuración existente

1. Invoque la API UpdateConfigurationPolicy desde la cuenta de administrador delegado de la región de origen.
2. En el campo `Identifier`, indique el nombre de recurso de Amazon (ARN) o el identificador de la política de configuración que quiera actualizar.
3. Para el objeto `SecurityControlCustomParameters`, indique el identificador de cada control que quiere personalizar.

4. Para el objeto `Parameters`, indique el nombre de cada parámetro que quiere personalizar. Para cada parámetro que personalice, indique `CUSTOM` en `ValueType`. En `Value`, indique el tipo de datos del parámetro y el valor personalizado. Si la solicitud omite un parámetro que el control admite, ese parámetro conserva su valor actual. Para encontrar los parámetros, los tipos de datos y los valores válidos admitidos para un control, invoque la API GetSecurityControlDefinition.

Por ejemplo, el siguiente AWS CLI comando crea una nueva política de configuración con un valor personalizado para el `daysToExpiration` parámetro de. `ACM.1` Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$ aws securityhub create-configuration-policy \
--region us-east-1 \
--name "SampleConfigurationPolicy" \
--description "Configuration policy for production accounts" \
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,
 "EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-
foundational-security-best-practices/v/1.0.0","arn:aws:securityhub:::ruleset/
cis-aws-foundations-benchmark/v/1.2.0"],"SecurityControlsConfiguration":
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2"],
 "SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters":
 {"daysToExpiration": {"ValueType": "CUSTOM", "Value": "Integer": 15}}}]}}}'
```

Personalización de parámetros de control en una sola cuenta y región

Si no utiliza la configuración centralizada o tiene una cuenta autoadministrada, puede personalizar los parámetros de control de su cuenta en una región a la vez.

Elija el método que prefiera y siga los pasos para personalizar los parámetros de control. Los cambios se aplican solo a su cuenta en la región actual. Para personalizar los parámetros de control en otras regiones, repita los siguientes pasos en cada cuenta o región adicional en la que quiere personalizar los parámetros. El mismo control puede utilizar valores de parámetros diferentes en regiones distintas.

Security Hub CSPM console

Para personalizar los valores de un parámetro de control en una cuenta y región (consola)

1. Abra la consola CSPM de AWS Security Hub en. https://console.aws.amazon.com/securityhub/
2. En el panel de navegación, elija Controles. En la tabla, elija un control que admita parámetros personalizados y cuyos parámetros quiere cambiar. La columna Parámetros personalizados indica qué controles los admiten.
3. En la página de detalles del control, seleccione la pestaña Parámetros y, a continuación, elija Editar.
4. Especifique los valores de los parámetros que quiere cambiar.
5. De manera opcional, en la sección Motivo del cambio, seleccione un motivo para personalizar los parámetros.
6. Seleccione Save.

Security Hub CSPM API

Para personalizar los valores de un parámetro de control en una cuenta y región (API)

1. Invoque la API UpdateSecurityControl.
2. En `SecurityControlId`, indique el identificador del control que quiere personalizar.
3. Para el objeto `Parameters`, indique el nombre de cada parámetro que quiere personalizar. Para cada parámetro que personalice, indique `CUSTOM` en `ValueType`. En `Value`, indique el tipo de datos del parámetro y el valor personalizado. Si la solicitud omite un parámetro que el control admite, ese parámetro conserva su valor actual. Para encontrar los parámetros, los tipos de datos y los valores válidos admitidos para un control, invoque la API GetSecurityControlDefinition.
4. De manera opcional, en `LastUpdateReason`, indique un motivo para personalizar los parámetros de control.

Por ejemplo, el siguiente AWS CLI comando define un valor personalizado para el `daysToExpiration` parámetro de. `ACM.1` Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$ aws securityhub update-security-control \
```

```
--region us-east-1 \
--security-control-id ACM.1 \
--parameters '{"daysToExpiration": {"ValueType": "CUSTOM", "Value": {"Integer":
 15}}}' \
--last-update-reason "Internal compliance requirement"
```

Reversión de los valores predeterminados de los parámetros de control

Un parámetro de control puede tener un valor predeterminado que defina AWS Security Hub CSPM. En ocasiones, el CSPM de Security Hub actualiza el valor predeterminado de un parámetro para alinearlo con la evolución de las prácticas recomendadas de seguridad. Si no ha especificado un valor personalizado para un parámetro de control, el control hace un seguimiento automático de esas actualizaciones y utiliza el nuevo valor predeterminado.

Puede volver a utilizar los valores predeterminados del parámetro para un control. Las instrucciones para revertir parámetros dependen de si usa la configuración centralizada en el CSPM de Security Hub. La configuración central es una función que el administrador delegado de CSPM de Security Hub puede usar para configurar las capacidades de CSPM de Security Hub en todas las cuentas y unidades Regiones de AWS organizativas (OU).

> **Note**
>
> No todos los parámetros de control tienen un valor predeterminado del CSPM de Security Hub. En esos casos, cuando `ValueType` se establece en `DEFAULT`, no existe un valor predeterminado específico que utilice el CSPM de Security Hub. En su lugar, el CSPM de Security Hub omite el parámetro si no hay un valor personalizado.

Reversión a los parámetros de control predeterminados en varias cuentas y regiones

Si utiliza la configuración centralizada, puede revertir los parámetros de control para varias cuentas y unidades organizativas administradas de manera centralizada en la región de origen y las regiones vinculadas.

Elija el método que prefiera y siga los pasos para revertir a los valores predeterminados de los parámetros en varias cuentas y regiones mediante la configuración centralizada.

Security Hub CSPM console

Para revertir los valores predeterminados de los parámetros de control en varias cuentas y regiones (consola)

1. Abra la consola CSPM AWS de Security Hub en. https://console.aws.amazon.com/securityhub/

   Inicie sesión con las credenciales de la cuenta de administrador delegado del CSPM de Security Hub en la región de origen.
2. En el panel de navegación, seleccione Configuración y Configuración.
3. Elija la pestaña Policies.
4. Seleccione una política y, a continuación, elija Editar.
5. En Política personalizada, la sección Controles muestra una lista de controles para los que especificó parámetros personalizados.
6. Busque el control que tenga uno o varios valores de parámetros que revertir. A continuación, elija Eliminar para revertir a los valores predeterminados.
7. En la sección Cuentas, compruebe las cuentas o unidades organizativas a las que quiere aplicar la política.
8. Elija Siguiente.
9. Revise los cambios y compruebe que sean correctos. Cuando termine, elija Guardar y aplicar política. Tanto en su región de origen como en todas regiones vinculadas, esta acción anula los ajustes de configuración existentes de las cuentas y unidades organizativas asociadas a esta política de configuración. Las cuentas y las unidades organizativas se pueden asociar a una política de configuración mediante una aplicación directa o la herencia de un elemento principal.

Security Hub CSPM API

Para revertir los valores predeterminados de los parámetros de control en varias cuentas y regiones (API)

1. Invoque la API UpdateConfigurationPolicy desde la cuenta de administrador delegado de la región de origen.
2. En el campo `Identifier`, indique el nombre de recurso de Amazon (ARN) o el identificador de la política que quiere actualizar.

3. Para el objeto `SecurityControlCustomParameters`, indique el identificador de cada control para revertir uno o varios parámetros.
4. En el objeto `Parameters`, para cada parámetro que quiere revertir, indique `DEFAULT` en el campo `ValueType`. Si `ValueType` está establecido en `DEFAULT`, no es necesario proporcionar un valor para el campo `Value`. Si se incluye un valor en la solicitud, el CSPM de Security Hub lo ignora. Si la solicitud omite un parámetro que el control admite, ese parámetro conserva su valor actual.

> **Warning**
>
> Si omite un objeto de control del campo `SecurityControlCustomParameters`, el CSPM de Security Hub revierte todos los parámetros personalizados del control a sus valores predeterminados. Una lista completamente vacía para `SecurityControlCustomParameters` revierte los parámetros personalizados de todos los controles a sus valores predeterminados.

Por ejemplo, el siguiente AWS CLI comando revierte el parámetro de `daysToExpiration` control `ACM.1` a su valor predeterminado en la política de configuración especificada. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$ aws securityhub create-configuration-policy \
--region us-east-1 \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
--name "TestConfigurationPolicy" \
--description "Updated configuration policy" \
--updated-reason "Revert ACM.1 parameter to default value"
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,
 "EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-
foundational-security-best-practices/v/1.0.0","arn:aws:securityhub:::ruleset/
cis-aws-foundations-benchmark/v/1.2.0"],"SecurityControlsConfiguration":
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2"],
 "SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters":
 {"daysToExpiration": {"ValueType": "DEFAULT"}}}]}}}'
```

Reversión a los parámetros de control predeterminados en una sola cuenta y región

Si no utiliza la configuración centralizada o tiene una cuenta autoadministrada, puede revertir al uso de los valores predeterminados de los parámetros para su cuenta en una región a la vez.

Elija el método que prefiera y siga los pasos para revertir a los valores predeterminados de los parámetros para su cuenta en una sola región. Para volver a los valores predeterminados de los parámetros en otras regiones, repita estos pasos en cada región adicional.

> **Note**
>
> Si desactiva el CSPM de Security Hub, se restablecen los parámetros de control personalizados. Si vuelve a habilitar el CSPM de Security Hub en el futuro, todos los controles utilizarán los valores predeterminados de los parámetros para comenzar.

Security Hub CSPM console

Para revertir los valores predeterminados de los parámetros de control en una cuenta o región (consola)

1. Abra la consola CSPM de AWS Security Hub en. https://console.aws.amazon.com/securityhub/
2. En el panel de navegación, elija Controles. Elija el control que quiere revertir a los valores predeterminados de los parámetros.
3. En la pestaña `Parameters`, elija Personalizado junto a un parámetro de control. A continuación, seleccione Eliminar personalización. Este parámetro ahora usa el valor predeterminado del CSPM de Security Hub y se actualiza automáticamente cuando dicho valor cambie en el futuro.
4. Repita el paso anterior para cada valor de parámetro que quiere revertir.

Security Hub CSPM API

Para revertir los valores predeterminados de los parámetros de control en una cuenta o región (API)

1. Invoque la API UpdateSecurityControl.

2. En `SecurityControlId`, indique el ARN o el identificador del control cuyos parámetros quiere revertir.
3. En el objeto `Parameters`, para cada parámetro que quiere revertir, indique `DEFAULT` en el campo `ValueType`. Si `ValueType` está establecido en `DEFAULT`, no es necesario proporcionar un valor para el campo `Value`. Si se incluye un valor en la solicitud, el CSPM de Security Hub lo ignora.
4. De manera opcional, en `LastUpdateReason`, indique un motivo para revertir a los valores predeterminados de los parámetros.

Por ejemplo, el siguiente AWS CLI comando revierte el parámetro de `daysToExpiration` control `ACM.1` a su valor predeterminado. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$ aws securityhub update-security-control \
--region us-east-1 \
--security-control-id ACM.1 \
--parameters '{"daysToExpiration": {"ValueType": "DEFAULT"}}' \
--last-update-reason "New internal requirement"
```

Comprobación del estado de los cambios de los parámetros de control

Al intentar personalizar un parámetro de control o volver al valor predeterminado, puede validar si los cambios deseados se realizaron correctamente. Esto ayuda a garantizar que un control funcione como se espera y proporcione el valor de seguridad previsto. Si una actualización del parámetro no se completa correctamente, el CSPM de Security Hub retiene el valor actual del parámetro.

Para verificar que la actualización del parámetro se completó correctamente, puede revisar los detalles del control en la consola del CSPM de Security Hub. En el panel de navegación de la consola, elija Controles. A continuación, elija un control para mostrar sus detalles. La pestaña Parámetros muestra el estado del cambio del parámetro.

Desde el punto de vista programático, si la solicitud de actualización de un parámetro es válida, el valor del campo `UpdateStatus` es `UPDATING` en una respuesta a la operación BatchGetSecurityControls. Esto significa que la actualización era válida, pero es posible que todos los resultados aún no incluyan los valores de los parámetros actualizados. Cuando el valor de `UpdateState` cambia a `READY`, el CSPM de Security Hub usa los valores actualizados del

parámetro de control cuando ejecuta las comprobaciones de seguridad del control. Los resultados incluyen los valores de los parámetros actualizados.

La operación `UpdateSecurityControl` devuelve una respuesta `InvalidInputException` para los valores de los parámetros no válidos. La respuesta proporciona detalles adicionales sobre el motivo del error. Por ejemplo, es posible que haya especificado un valor que está fuera del rango válido de un parámetro. O bien, es posible que haya especificado un valor que no utiliza el tipo de datos correcto. Vuelva a enviar la solicitud con una entrada válida.

Si se produce un error interno al intentar actualizar el valor de un parámetro, Security Hub CSPM lo reintentará automáticamente si está habilitado. AWS Config Para obtener más información, consulte Consideraciones antes de habilitar y configurar AWS Config.

Revisión y administración de resultados de controles en el CSPM de Security Hub

La página de detalles del control muestra una lista de los resultados activos de un control. La lista no incluye resultados archivados.

La página de detalles del control admite la agregación entre regiones. Si ha establecido una región de agregación, el estado del control y la lista de controles de seguridad de la página de detalles del control incluyen las comprobaciones de todas las Regiones de AWS vinculadas.

La lista proporciona herramientas para filtrar y ordenar los resultados, de modo que pueda centrarse primero en los más urgentes. Un resultado puede incluir enlaces a información detallada sobre los recursos en la consola de servicio correspondiente. En el caso de los controles que se basan en AWS Config reglas, puede ver los detalles de la regla.

También puede usar la API CSPM de AWS Security Hub para recuperar una lista de hallazgos y detalles de los hallazgos.

Para obtener más información, consulte Revisión de los detalles y el historial de resultados.

Para reflejar el estado actual de la investigación de un resultado de control, debe configurar el estado del flujo de trabajo. Para obtener más información, consulte the section called “Configuración del estado de flujo de trabajo de los resultados”.

También puedes enviar los resultados de CSPM seleccionados de Security Hub a una acción personalizada en Amazon. EventBridge Para obtener más información, consulte the section called “Envío de hallazgos a una acción personalizada”.

Temas

- Filtrado y clasificación de resultados de control
- Ejemplos de resultados de controles

Filtrado y clasificación de resultados de control

Al seleccionar un control en la página de controles de la consola CSPM de AWS Security Hub o en la página de detalles de un estándar, se accede a la página de detalles del control.

La página de detalles del control muestra el título y la descripción del control, el estado general del control y un desglose de los controles de seguridad de las últimas 24 horas.

Utilice las opciones Filtrar por situadas junto a la lista de controles de seguridad para centrarse rápidamente en los resultados relacionados con un estado de flujo de trabajo o un estado de conformidad específicos.

Además de las opciones Filtrar por, puede utilizar la casilla Agregar filtro para filtrar la lista de verificación por otros campos, como el Cuenta de AWS identificador o el identificador del recurso.

Los resultados cuyo estado de conformidad es APROBADO se enumeran en primer lugar de forma predeterminada. Puede cambiar el orden predeterminado si selecciona una opción diferente en los encabezados de las columnas.

En la página de detalles del control, puede seleccionar Descargar para descargar la página actual de resultados de control en un archivo .csv.

Si filtra la lista de resultados, la descarga solo incluirá los controles que coincidan con el filtro. Si selecciona resultados específicos de la lista, la descarga solo incluirá los resultados seleccionados.

Para obtener más información sobre cómo filtrar resultados, consulte Filtrado de resultados en el CSPM de Security Hub.

Ejemplos de resultados de controles

Los siguientes ejemplos proporcionan ejemplos de los resultados del control CSPM de AWS Security Hub en el formato de búsqueda AWS de seguridad (ASFF). El contenido de los resultados de controles varía según si habilita los resultados consolidados de controles.

Si habilita los resultados consolidados de controles, el CSPM de Security Hub genera un único resultado para un control, incluso cuando el control se aplica a varios estándares habilitados. Si

no habilita esta característica, el CSPM de Security Hub genera un resultado separado para cada estándar habilitado al que se aplica el control. Por ejemplo, si habilita dos estándares y un control se aplica a ambos, recibe dos resultados separados para el control, uno por cada estándar. Si habilita los resultados consolidados de controles, recibe un único resultado para el control. Para obtener más información, consulte Resultados de control consolidados.

Las muestras de esta página ofrecen ejemplos para ambos casos. Las muestras incluyen resultados de controles para estándares individuales del CSPM de Security Hub cuando los resultados consolidados de controles se encuentran desactivados, y un único resultado de control para varios estándares del CSPM de Security Hub cuando los resultados consolidados de controles se encuentran habilitados.

Ejemplos de resultados de controles

- Ejemplo de hallazgo para elAWSEstándar fundamental de mejores prácticas de seguridad
- Ejemplo de hallazgo para el CISAWSFoundations Benchmark v5.0.0
- Ejemplo de hallazgo para el CISAWSFoundations Benchmark v3.0.0
- Ejemplo de hallazgo para el CISAWSFoundations Benchmark v1.4.0
- Ejemplo de hallazgo para el CISAWSFoundations Benchmark v1.2.0
- Ejemplo de resultado para el estándar NIST SP 800-53 Revisión 5
- Ejemplo de resultado para el estándar NIST SP 800-171 Revisión 2
- Ejemplo de resultado para el estándar Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago (PCI DSS) v3.2.1.
- Ejemplo de hallazgo para elAWSEstándar de etiquetado de recursos
- Ejemplo de hallazgo para elAWS Control TowerEstándar de gestión de servicios
- Ejemplo de resultado consolidado para varios estándares

> **Note**
>
> Los resultados de controles hacen referencia a distintos campos y valores en las regiones de China y en las regiones de AWS GovCloud (US). Para obtener más información, consulte Impacto de la consolidación en los campos y valores ASFF.

Ejemplo de hallazgo para elAWSEstándar fundamental de mejores prácticas de seguridad

La siguiente muestra ofrece un ejemplo de un resultado para un control que se aplica al estándar de Prácticas recomendadas de seguridad básica de AWS (FSBP). En esta muestra, los resultados consolidados de controles se encuentran desactivados.


```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-2:123456789012:subscription/aws-foundational-
security-best-practices/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-2::product/aws/securityhub",
  "ProductName": "Security Hub CSPM",
  "CompanyName": "AWS",
  "Region": "us-east-2",
  "GeneratorId": "aws-foundational-security-best-practices/v/1.0.0/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/AWS-
Foundational-Security-Best-Practices"
  ],
  "FirstObservedAt": "2020-08-06T02:18:23.076Z",
  "LastObservedAt": "2021-09-28T16:10:06.956Z",
  "CreatedAt": "2020-08-06T02:18:23.076Z",
  "UpdatedAt": "2021-09-28T16:10:00.093Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "CloudTrail.2 CloudTrail should have encryption at-rest enabled",
  "Description": "ThisAWScontrol checks whetherAWS CloudTrailis configured to use the
 server side encryption (SSE)AWS Key Management Service(AWS KMS) customer master key
 (CMK) encryption. The check will pass if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to correct this issue, consult theAWSSecurity Hub
 CSPM controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
```

```
    "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-
practices/v/1.0.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-2:123456789012:subscription/aws-foundational-security-best-practices/v/1.0.0",
    "ControlId": "CloudTrail.2",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/aws-
foundational-security-best-practices/v/1.0.0/CloudTrail.2",
    "aws/securityhub/ProductName": "Security Hub CSPM",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWSMacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-2::product/aws/
securityhub/arn:aws:securityhub:us-east-2:123456789012:subscription/aws-foundational-
security-best-practices/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWSMacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-2"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "standards/aws-foundation-best-practices/v/1.0.0"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
```

```
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/AWS-
Foundational-Security-Best-Practices"
    ]
  }
}
```

Ejemplo de hallazgo para el CISAWSFoundations Benchmark v5.0.0

El siguiente ejemplo proporciona un ejemplo de un hallazgo de un control que se aplica a CIS AWS Foundations Benchmark v5.0.0. En esta muestra, los resultados consolidados de controles se encuentran desactivados.

```
{
  "AwsAccountId": "123456789012",
  "CompanyName": "AWS",
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "EC2.7",
    "RelatedRequirements": [
      "CIS AWS Foundations Benchmark v5.0.0/5.1.1"
    ],
    "AssociatedStandards": [
      {
        "StandardsId": "standards/cis-aws-foundations-benchmark/v/5.0.0"
      }
    ]
  },
  "CreatedAt": "2025-10-10T17:04:00.952Z",
  "Description": "Elastic Compute Cloud (EC2) supports encryption at rest when using
 the Elastic Block Store (EBS) service. While disabled by default, forcing encryption
 at EBS volume creation is supported.",
  "FindingProviderFields": {
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
 Foundations Benchmark"
    ],
    "Severity": {
      "Normalized": 40,
      "Label": "MEDIUM",
```

```
      "Product": 40,
      "Original": "MEDIUM"
    }
  },
  "FirstObservedAt": "2025-10-10T17:03:57.895Z",
  "GeneratorId": "cis-aws-foundations-benchmark/v/5.0.0/5.1.1",
  "Id": "arn:aws:securityhub:us-west-1:123456789012:subscription/cis-aws-foundations-
benchmark/v/5.0.0/5.1.1/finding/443a9d3f-8a59-4fa0-8e2c-EXAMPLE111",
  "LastObservedAt": "2025-10-14T05:22:28.667Z",
  "ProcessedAt": "2025-10-14T05:22:50.099Z",
  "ProductArn": "arn:aws:securityhub:us-west-1::product/aws/securityhub",
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/cis-aws-foundations-benchmark/
v/5.0.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
west-1:123456789012:subscription/cis-aws-foundations-benchmark/v/5.0.0",
    "ControlId": "5.1.1",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/EC2.7/
remediation",
    "RelatedAWSResources:0/name": "securityhub-ec2-ebs-encryption-by-default-2a99554f",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-west-1:123456789012:control/cis-aws-
foundations-benchmark/v/5.0.0/5.1.1",
    "aws/securityhub/ProductName": "Security Hub CSPM",
    "aws/securityhub/CompanyName": "AWS",
    "aws/securityhub/annotation": "EBS Encryption by default is not enabled.",
    "Resources:0/Id": "arn:aws:iam::123456789012:root",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-west-1::product/aws/
securityhub/arn:aws:securityhub:us-west-1:123456789012:subscription/cis-aws-
foundations-benchmark/v/5.0.0/5.1.1/finding/443a9d3f-8a59-4fa0-8e2c-EXAMPLE111",
    "PreviousComplianceStatus": "FAILED"
  },
  "ProductName": "Security Hub CSPM",
  "RecordState": "ACTIVE",
  "Region": "us-west-1",
  "Remediation": {
    "Recommendation": {
      "Text": "For information on how to correct this issue, consult the AWS Security
 Hub controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/EC2.7/remediation"
    }
  },
  "Resources": [
    {
```

```
      "Id": "AWS::::Account:123456789012",
      "Partition": "aws",
      "Region": "us-west-1",
      "Type": "AwsAccount"
    }
  ],
  "SchemaVersion": "2018-10-08",
  "Severity": {
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM",
    "Product": 40
  },
  "Title": "5.1.1 EBS default encryption should be enabled",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/
CISAWSFoundations Benchmark"
  ],
  "UpdatedAt": "2025-10-14T05:22:38.671Z",
  "Workflow": {
    "Status": "NEW"
  },
  "WorkflowState": "NEW"
}
```

Ejemplo de hallazgo para el CISAWSFoundations Benchmark v3.0.0

El siguiente ejemplo proporciona un ejemplo de un hallazgo de un control que se aplica a CIS AWS Foundations Benchmark v3.0.0. En esta muestra, los resultados consolidados de controles se encuentran desactivados.

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-foundations-
benchmark/v/3.0.0/2.2.1/finding/38a89798-6819-4fae-861f-9cca8034602c",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub CSPM",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "cis-aws-foundations-benchmark/v/3.0.0/2.2.1",
  "AwsAccountId": "123456789012",
  "Types": [
```

```
    "Software and Configuration Checks/Industry and Regulatory Standards/
CISAWSFoundations Benchmark"
  ],
  "FirstObservedAt": "2024-04-18T07:46:18.193Z",
  "LastObservedAt": "2024-04-23T07:47:01.137Z",
  "CreatedAt": "2024-04-18T07:46:18.193Z",
  "UpdatedAt": "2024-04-23T07:46:46.165Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "2.2.1 EBS default encryption should be enabled",
  "Description": "Elastic Compute Cloud (EC2) supports encryption at rest when using
 the Elastic Block Store (EBS) service. While disabled by default, forcing encryption
 at EBS volume creation is supported.",
  "Remediation": {
    "Recommendation": {
      "Text": "For information on how to correct this issue, consult theAWSSecurity Hub
 CSPM controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/EC2.7/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/cis-aws-foundations-benchmark/
v/3.0.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/cis-aws-foundations-benchmark/v/3.0.0",
    "ControlId": "2.2.1",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/EC2.7/
remediation",
    "RelatedAWSResources:0/name": "securityhub-ec2-ebs-encryption-by-default-2843ed9e",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-1:123456789012:control/cis-aws-
foundations-benchmark/v/3.0.0/2.2.1",
    "aws/securityhub/ProductName": "Security Hub CSPM",
    "aws/securityhub/CompanyName": "AWS",
    "aws/securityhub/annotation": "EBS Encryption by default is not enabled.",
    "Resources:0/Id": "arn:aws:iam::123456789012:root",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-
foundations-benchmark/v/3.0.0/2.2.1/finding/38a89798-6819-4fae-861f-9cca8034602c"
  },
```

```
  "Resources": [
    {
      "Type": "AwsAccount",
      "Id": "AWS::::Account:123456789012",
      "Partition": "aws",
      "Region": "us-east-1"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "RelatedRequirements": [
      "CIS AWS Foundations Benchmark v3.0.0/2.2.1"
    ],
    "SecurityControlId": "EC2.7",
    "AssociatedStandards": [
      {
        "StandardsId": "standards/cis-aws-foundations-benchmark/v/3.0.0"
      }
    ]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/
CISAWSFoundations Benchmark"
    ]
  },
  "ProcessedAt": "2024-04-23T07:47:07.088Z"
}
```

Ejemplo de hallazgo para el CISAWSFoundations Benchmark v1.4.0

El siguiente ejemplo proporciona un ejemplo de un hallazgo de un control que se aplica a CIS AWS Foundations Benchmark v1.4.0. En esta muestra, los resultados consolidados de controles se encuentran desactivados.

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-foundations-
benchmark/v/1.4.0/3.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub CSPM",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "cis-aws-foundations-benchmark/v/1.4.0/3.7",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/
CISAWSFoundations Benchmark"
  ],
  "FirstObservedAt": "2022-10-21T22:14:48.913Z",
  "LastObservedAt": "2022-12-22T22:24:56.980Z",
  "CreatedAt": "2022-10-21T22:14:48.913Z",
  "UpdatedAt": "2022-12-22T22:24:52.409Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "3.7 Ensure CloudTrail logs are encrypted at rest using KMS CMKs",
  "Description": "AWS CloudTrailis a web service that recordsAWSAPI calls for an
 account and makes those logs available to users and resources in accordance with IAM
 policies.AWS Key Management Service(KMS) is a managed service that helps create and
 control the encryption keys used to encrypt account data, and uses Hardware Security
 Modules (HSMs) to protect the security of encryption keys. CloudTrail logs can be
 configured to leverage server side encryption (SSE) andAWS KMScustomer created master
 keys (CMK) to further protect CloudTrail logs. It is recommended that CloudTrail be
 configured to use SSE-KMS.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to correct this issue, consult theAWSSecurity Hub
 CSPM controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/cis-aws-foundations-benchmark/
v/1.4.0",
```

```
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/cis-aws-foundations-benchmark/v/1.4.0",
    "ControlId": "3.7",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-
enabled-855f82d1",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-1:123456789012:control/cis-aws-
foundations-benchmark/v/1.4.0/3.7",
    "aws/securityhub/ProductName": "Security Hub CSPM",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-west-2:123456789012:trail/AWSMacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-
foundations-benchmark/v/1.4.0/3.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-west-2:123456789012:trail/AWSMacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-1"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "RelatedRequirements": [
      "CISAWSFoundations Benchmark v1.4.0/3.7"
    ],
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "standards/cis-aws-foundations-benchmark/v/1.4.0"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
```

```
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/
CISAWSFoundations Benchmark"
    ]
  }
}
```

Ejemplo de hallazgo para el CISAWSFoundations Benchmark v1.2.0

En el siguiente ejemplo, se proporciona un ejemplo del hallazgo de un control que se aplica a CIS AWS Foundations Benchmark v1.2.0. En esta muestra, los resultados consolidados de controles se encuentran desactivados.

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-2:123456789012:subscription/cis-aws-foundations-
benchmark/v/1.2.0/2.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-2::product/aws/securityhub",
  "ProductName": "Security Hub CSPM",
  "CompanyName": "AWS",
  "Region": "us-east-2",
  "GeneratorId": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/
rule/2.7",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/
CISAWSFoundations Benchmark"
  ],
  "FirstObservedAt": "2020-08-29T04:10:06.337Z",
  "LastObservedAt": "2021-09-28T16:10:05.350Z",
  "CreatedAt": "2020-08-29T04:10:06.337Z",
  "UpdatedAt": "2021-09-28T16:10:00.087Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "2.7 Ensure CloudTrail logs are encrypted at rest using KMS CMKs",
```

```
  "Description": "AWS Key Management Service(KMS) is a managed service that helps
 create and control the encryption keys used to encrypt account data, and uses Hardware
 Security Modules (HSMs) to protect the security of encryption keys. CloudTrail
 logs can be configured to leverage server side encryption (SSE) and KMS customer
 created master keys (CMK) to further protect CloudTrail logs. It is recommended that
 CloudTrail be configured to use SSE-KMS.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to correct this issue, consult theAWSSecurity Hub
 CSPM controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsGuideArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0",
    "StandardsGuideSubscriptionArn": "arn:aws:securityhub:us-
east-2:123456789012:subscription/cis-aws-foundations-benchmark/v/1.2.0",
    "RuleId": "2.7",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/cis-aws-
foundations-benchmark/v/1.2.0/2.7",
    "aws/securityhub/ProductName": "Security Hub CSPM",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWSMacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-2::product/aws/
securityhub/arn:aws:securityhub:us-east-2:123456789012:subscription/cis-aws-
foundations-benchmark/v/1.2.0/2.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWSMacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-2"
    }
  ],
  "Compliance": {
```

```
    "Status": "FAILED",
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "ruleset/cis-aws-foundations-benchmark/v/1.2.0"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/
CISAWSFoundations Benchmark"
    ]
  }
}
```

Ejemplo de resultado para el estándar NIST SP 800-53 Revisión 5

La siguiente muestra ofrece un ejemplo de un resultado para un control que se aplica al estándar NIST SP 800-53 Revisión 5. En esta muestra, los resultados consolidados de controles se encuentran desactivados.

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/nist-800-53/v/5.0.0/
CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub CSPM",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "nist-800-53/v/5.0.0/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2023-02-17T14:22:46.726Z",
```

```
  "LastObservedAt": "2023-02-17T14:22:50.846Z",
  "CreatedAt": "2023-02-17T14:22:46.726Z",
  "UpdatedAt": "2023-02-17T14:22:46.726Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "CloudTrail.2 CloudTrail should have encryption at-rest enabled",
  "Description": "ThisAWScontrol checks whetherAWS CloudTrailis configured to use the
 server side encryption (SSE)AWS Key Management Service(AWS KMS) customer master key
 (CMK) encryption. The check will pass if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to fix this issue, consult theAWSSecurity Hub CSPM
 NIST 800-53 R5 documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/nist-800-53/v/5.0.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/nist-800-53/v/5.0.0",
    "ControlId": "CloudTrail.2",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.9/
remediation",
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/aws-
foundational-security-best-practices/v/1.0.0/CloudTrail.2",
    "aws/securityhub/ProductName": "Security Hub CSPM",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-west-2:123456789012:trail/AWSMacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/nist-800-53/
v/5.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
```

```
      "Id": "arn:aws:cloudtrail:us-east-1:123456789012:trail/AWSMacieTrail-DO-NOT-
EDIT",

      "Partition": "aws",

      "Region": "us-east-1"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "RelatedRequirements": [
        "NIST.800-53.r5 AU-9",
        "NIST.800-53.r5 CA-9(1)",
        "NIST.800-53.r5 CM-3(6)",
        "NIST.800-53.r5 SC-13",
        "NIST.800-53.r5 SC-28",
        "NIST.800-53.r5 SC-28(1)",
        "NIST.800-53.r5 SC-7(10)",
        "NIST.800-53.r5 SI-7(6)"
    ],
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [
      {
        "StandardsId": "standards/nist-800-53/v/5.0.0"
      }
    ]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards"
    ]
  },
  "ProcessedAt": "2023-02-17T14:22:53.572Z"
}
```

Ejemplo de resultado para el estándar NIST SP 800-171 Revisión 2

La siguiente muestra ofrece un ejemplo de un resultado para un control que se aplica al estándar NIST SP 800-171 Revisión 2. En esta muestra, los resultados consolidados de controles se encuentran desactivados.


```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/nist-800-171/v/2.0.0/
CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "nist-800-171/v/2.0.0/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "AwsAccountName": "TestAcct",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2025-05-29T05:23:58.690Z",
  "LastObservedAt": "2025-05-30T05:50:11.898Z",
  "CreatedAt": "2025-05-29T05:24:24.772Z",
  "UpdatedAt": "2025-05-30T05:50:34.292Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "CloudTrail.2 CloudTrail should have encryption at-rest enabled",
  "Description": "This AWS control checks whetherAWS CloudTrailis configured to use the
 server side encryption (SSE)AWS Key Management Service(AWS KMS) customer master key
 (CMK) encryption. The check will pass if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
      "Text": "For information on how to correct this issue, consult theAWSSecurity Hub
 CSPM controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/nist-800-171/v/2.0.0",
```

```
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/nist-800-171/v/2.0.0",
    "ControlId": "CloudTrail.2",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-
enabled-0ab1c2d4",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-1:123456789012:control/
nist-800-171/v/2.0.0/CloudTrail.2",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:ca-central-1:123456789012:trail/aws-
BaselineCloudTrail",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/nist-800-171/
v/2.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Id": "arn:aws:cloudtrail:ca-central-1:123456789012:trail/aws-
BaselineCloudTrail",
      "Partition": "aws",
      "Region": "us-east-1",
      "Type": "AwsCloudTrailTrail"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "CloudTrail.2",
    "RelatedRequirements": [
      "NIST.800-171.r2/3.3.8"
    ],
    "AssociatedStandards": [
      {
        "StandardsId": "standards/nist-800-171/v/2.0.0"
      }
    ]
  },
  "Workflow": {
    "Status": "NEW"
  },
  "WorkflowState": "NEW",
  "RecordState": "ACTIVE",
```

```
  "FindingProviderFields": {
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards"
    ],
    "Severity": {
      "Product": 40,
      "Label": "MEDIUM",
      "Normalized": 40,
      "Original": "MEDIUM"
    }
  },
  "ProcessedAt": "2025-05-30T05:50:40.297Z"
}
```

Ejemplo de resultado para el estándar Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago (PCI DSS) v3.2.1.

La siguiente muestra ofrece un ejemplo de un resultado para un control que se aplica al Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago (PCI DSS) v3.2.1. En esta muestra, los resultados consolidados de controles se encuentran desactivados.

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-2:123456789012:subscription/pci-dss/v/3.2.1/
PCI.CloudTrail.1/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-2::product/aws/securityhub",
  "ProductName": "Security Hub CSPM",
  "CompanyName": "AWS",
  "Region": "us-east-2",
  "GeneratorId": "pci-dss/v/3.2.1/PCI.CloudTrail.1",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/PCI-DSS"
  ],
  "FirstObservedAt": "2020-08-06T02:18:23.089Z",
  "LastObservedAt": "2021-09-28T16:10:06.942Z",
  "CreatedAt": "2020-08-06T02:18:23.089Z",
  "UpdatedAt": "2021-09-28T16:10:00.090Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
```

```
  },
  "Title": "PCI.CloudTrail.1 CloudTrail logs should be encrypted at rest usingAWS
 KMSCMKs",
  "Description": "ThisAWScontrol checks whetherAWS CloudTrailis configured to use the
 server side encryption (SSE)AWS Key Management Service(AWS KMS) customer master key
 (CMK) encryption by checking if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to correct this issue, consult theAWSSecurity Hub
 CSPM controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/pci-dss/v/3.2.1",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-2:123456789012:subscription/pci-dss/v/3.2.1",
    "ControlId": "PCI.CloudTrail.1",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/pci-dss/
v/3.2.1/PCI.CloudTrail.1",
    "aws/securityhub/ProductName": "Security Hub CSPM",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWSMacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-2::product/aws/
securityhub/arn:aws:securityhub:us-east-2:123456789012:subscription/pci-dss/v/3.2.1/
PCI.CloudTrail.1/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWSMacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-2"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
```

```
    "RelatedRequirements": [
      "PCI DSS 3.4"
    ],
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "standards/pci-dss/v/3.2.1"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/PCI-DSS"
    ]
  }
}
```

Ejemplo de hallazgo para elAWSEstándar de etiquetado de recursos

La siguiente muestra ofrece un ejemplo de un resultado para un control que se aplica al estándar Etiquetado de recursos de AWS. En esta muestra, los resultados consolidados de controles se encuentran desactivados.

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:eu-central-1:123456789012:security-control/EC2.44/finding/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:eu-central-1::product/aws/securityhub",
  "ProductName": "Security Hub CSPM",
  "CompanyName": "AWS",
  "Region": "eu-central-1",
  "GeneratorId": "security-control/EC2.44",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
```

```
  "FirstObservedAt": "2024-02-19T21:00:32.206Z",
  "LastObservedAt": "2024-04-29T13:01:57.861Z",
  "CreatedAt": "2024-02-19T21:00:32.206Z",
  "UpdatedAt": "2024-04-29T13:01:41.242Z",
  "Severity": {
    "Label": "LOW",
    "Normalized": 1,
    "Original": "LOW"
  },
  "Title": "EC2 subnets should be tagged",
  "Description": "This control checks whether an Amazon EC2 subnet has tags with the
 specific keys defined in the parameter requiredTagKeys. The control fails if the
 subnet doesn't have any tag keys or if it doesn't have all the keys specified in
 the parameter requiredTagKeys. If the parameter requiredTagKeys isn't provided, the
 control only checks for the existence of a tag key and fails if the subnet isn't
 tagged with any key. System tags, which are automatically applied and begin with aws:,
 are ignored.",
  "Remediation": {
    "Recommendation": {
      "Text": "For information on how to correct this issue, consult theAWSSecurity Hub
 CSPM controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/EC2.44/remediation"
    }
  },
  "ProductFields": {
    "RelatedAWSResources:0/name": "securityhub-tagged-ec2-subnet-6ceafede",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "aws/securityhub/ProductName": "Security Hub CSPM",
    "aws/securityhub/CompanyName": "AWS",
    "aws/securityhub/annotation": "No tags are present.",
    "Resources:0/Id": "arn:aws:ec2:eu-central-1:123456789012:subnet/
subnet-1234567890abcdef0",
    "aws/securityhub/FindingId": "arn:aws:securityhub:eu-central-1::product/aws/
securityhub/arn:aws:securityhub:eu-central-1:123456789012:security-control/EC2.44/
finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsEc2Subnet",
      "Id": "arn:aws:ec2:eu-central-1:123456789012:subnet/subnet-1234567890abcdef0",
      "Partition": "aws",
      "Region": "eu-central-1",
      "Details": {
        "AwsEc2Subnet": {
```

```
          "AssignIpv6AddressOnCreation": false,
          "AvailabilityZone": "eu-central-1b",
          "AvailabilityZoneId": "euc1-az3",
          "AvailableIpAddressCount": 4091,
          "CidrBlock": "10.24.34.0/23",
          "DefaultForAz": true,
          "MapPublicIpOnLaunch": true,
          "OwnerId": "123456789012",
          "State": "available",
          "SubnetArn": "arn:aws:ec2:eu-central-1:123456789012:subnet/
subnet-1234567890abcdef0",
          "SubnetId": "subnet-1234567890abcdef0",
          "VpcId": "vpc-021345abcdef6789"
        }
      }
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "EC2.44",
    "AssociatedStandards": [
      {
        "StandardsId": "standards/aws-resource-tagging-standard/v/1.0.0"
      }
    ],
    "SecurityControlParameters": [
      {
        "Name": "requiredTagKeys",
        "Value": [
          "peepoo"
        ]
      }
    ],
            },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "LOW",
      "Original": "LOW"
    },
```

```
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards"
    ]
  },
  "ProcessedAt": "2024-04-29T13:02:03.259Z"
}
```

Ejemplo de hallazgo para elAWS Control TowerEstándar de gestión de servicios

La siguiente muestra ofrece un ejemplo de un resultado para un control que se aplica al estándar administrado por el servicio de AWS Control Tower. En esta muestra, los resultados consolidados de controles se encuentran desactivados.

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/service-managed-aws-
control-tower/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub CSPM",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "service-managed-aws-control-tower/v/1.0.0/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2022-11-17T01:25:30.296Z",
  "LastObservedAt": "2022-11-17T01:25:45.805Z",
  "CreatedAt": "2022-11-17T01:25:30.296Z",
  "UpdatedAt": "2022-11-17T01:25:30.296Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "CT.CloudTrail.2 CloudTrail should have encryption at-rest enabled",
  "Description": "ThisAWScontrol checks whetherAWS CloudTrailis configured to use the
 server side encryption (SSE)AWS Key Management Service(AWS KMS) customer master key
 (CMK) encryption. The check will pass if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
```

```
      "Text": "For information on how to correct this issue, consult theAWSSecurity Hub
 CSPM controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/service-managed-aws-control-tower/
v/1.0.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/service-managed-aws-control-tower/v/1.0.0",
    "ControlId": "CT.CloudTrail.2",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-1:123456789012:control/service-
managed-aws-control-tower/v/1.0.0/CloudTrail.2",
    "aws/securityhub/ProductName": "Security Hub CSPM",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWSMacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/service-managed-
aws-control-tower/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsAccount",
      "Id": "AWS::::Account:123456789012",
      "Partition": "aws",
      "Region": "us-east-1"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "standards/service-managed-aws-control-tower/v/1.0.0"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
```

```
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards"
    ]
  }
}
```

Ejemplo de resultado consolidado para varios estándares

La siguiente muestra ofrece un ejemplo de un resultado para un control que se aplica a varios estándares habilitados. En esta muestra, los resultados consolidados de controles se encuentran habilitados.

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:security-control/CloudTrail.2/
finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "security-control/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2024-08-09T14:57:04.521Z",
  "LastObservedAt": "2025-05-30T03:30:17.407Z",
  "CreatedAt": "2024-08-09T14:57:04.521Z",
  "UpdatedAt": "2025-05-30T03:30:32.781Z",
  "Severity": {
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "CloudTrail should have encryption at-rest enabled",
```

```
  "Description": "This AWS control checks whetherAWS CloudTrailis configured to use the
 server side encryption (SSE)AWS Key Management Service(AWS KMS) customer master key
 (CMK) encryption. The check will pass if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
      "Text": "For information on how to correct this issue, consult theAWSSecurity Hub
 CSPM controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-
enabled-01a2b345",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-1:123456789012:trail/TestTrail-DO-
NOT-DELETE",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:security-control/CloudTrail.2/
finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-east-1:123456789012:trail/TestTrail-DO-NOT-DELETE",
      "Partition": "aws",
      "Region": "us-east-1",
      "Details": {
        "AwsCloudTrailTrail": {
          "HasCustomEventSelectors": false,
          "IncludeGlobalServiceEvents": true,
          "LogFileValidationEnabled": true,
          "HomeRegion": "us-east-1",
          "IsMultiRegionTrail": true,
          "S3BucketName": "cloudtrail-awslogs-do-not-delete",
          "IsOrganizationTrail": false,
          "Name": "TestTrail-DO-NOT-DELETE"
        }
      }
    }
  ],
  "Compliance": {
    "Status": "FAILED",
```

```
    "SecurityControlId": "CloudTrail.2",
    "RelatedRequirements": [
      "CIS AWS Foundations Benchmark v1.2.0/2.7",
      "CIS AWS Foundations Benchmark v1.4.0/3.7",
      "CIS AWS Foundations Benchmark v3.0.0/3.5",
      "NIST.800-171.r2/3.3.8",
      "PCI DSS v3.2.1/3.4",
      "PCI DSS v4.0.1/10.3.2"
    ],
    "AssociatedStandards": [
      { "StandardsId": "ruleset/cis-aws-foundations-benchmark/v/1.2.0"},
      { "StandardsId": "standards/aws-foundational-security-best-practices/v/1.0.0"},
      { "StandardsId": "standards/cis-aws-foundations-benchmark/v/1.4.0"},
      { "StandardsId": "standards/cis-aws-foundations-benchmark/v/3.0.0"},
      { "StandardsId": "standards/nist-800-171/v/2.0.0"},
      { "StandardsId": "standards/pci-dss/v/3.2.1"},
      { "StandardsId": "standards/pci-dss/v/4.0.1"}
    ]
  },
  "Workflow": {
    "Status": "NEW"
  },
  "WorkflowState": "NEW",
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards"
    ],
    "Severity": {
      "Normalized": 40,
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    }
  },
  "ProcessedAt": "2025-05-30T03:31:00.831Z"
}
```


Comprensión de las integraciones en el CSPM de Security Hub

AWS Security Hub CSPM puede recopilar las conclusiones de seguridad de varias soluciones de seguridad de terceros compatibles Servicios de AWS . AWS Partner Network Estas integraciones pueden ayudarlo a obtener una visión integral de la seguridad y el cumplimiento en todo su entorno.

AWS Security Hub CSPM incorpora los hallazgos de las soluciones integradas y los convierte al formato de búsqueda de AWS seguridad (ASFF).

> **Important**
>
> En el caso de las integraciones de productos compatibles AWS y de terceros, Security Hub CSPM recibe y consolida los hallazgos que se generan solo después de habilitar Security Hub CSPM para su. Cuentas de AWS El servicio no recibe ni consolida de forma retroactiva los resultados de seguridad generados antes de habilitar el CSPM de Security Hub.

La página de integraciones de la consola CSPM de Security Hub proporciona acceso a las integraciones de productos de terceros y disponibles. AWS La API del CSPM de Security Hub también incluye operaciones para administrar integraciones.

Es posible que una integración no esté disponible en todos los casos. Regiones de AWS Si una integración no es compatible en la región en la que inició sesión en la consola del CSPM de Security Hub, dicha integración no aparece en la página Integraciones de la consola. Para obtener una lista de las integraciones disponibles en las regiones de China AWS GovCloud (US) Regions, consulteDisponibilidad de las integraciones por región.

Además de las integraciones de terceros integradas, puede integrar productos de seguridad personalizados con Security Hub CSPM. Servicio de AWS Luego puede enviar los resultados desde estos productos al CSPM de Security Hub a través de la API del CSPM de Security Hub. También puede usar la API para actualizar resultados existentes que el CSPM de Security Hub haya recibido desde un producto de seguridad personalizado.

Temas

- Revisión de una lista de las integraciones del CSPM de Security Hub
- Habilitación del flujo de resultados desde una integración del CSPM de Security Hub
- Desactivación del flujo de resultados provenientes de una integración con el CSPM de Security Hub
- Visualización de los resultados a partir de una integración con el CSPM de Security Hub
- Servicio de AWS integraciones con Security Hub CSPM
- Third-party integraciones de productos con Security Hub CSPM
- Integración del CSPM de Security Hub con productos personalizados

Revisión de una lista de las integraciones del CSPM de Security Hub

Elija el método que prefiera y siga los pasos para revisar la lista de integraciones del CSPM de AWS Security Hub o para ver detalles sobre una integración específica.

Security Hub CSPM console

Para revisar las opciones y los detalles de las integraciones (consola)

1. Abra la consola AWS CSPM de Security Hub en. https://console.aws.amazon.com/securityhub/
2. En el panel de navegación del CSPM de Security Hub, seleccione Integraciones.

En la página Integraciones, primero se muestran las integraciones con otros Servicios de AWS , seguidas por las integraciones con productos de terceros.

Para cada integración, la página Integraciones proporciona la siguiente información:

- El nombre de la empresa
- El nombre del producto
- Una descripción de la integración
- Las categorías a las que se aplica la integración
- Cómo habilitar la integración
- El estado actual de la integración

Puede filtrar la lista utilizando texto de los siguientes campos:

- Nombre de la empresa
- Product name (Nombre del producto)
- Descripción de integración
- Categorías

Security Hub CSPM API

Para revisar las opciones y los detalles de las integraciones (API)

Para obtener una lista de integraciones, utilice la operación DescribeProducts. Si está utilizando el AWS CLI, ejecute el describe-products comando.

Para obtener detalles sobre una integración específica, utilice el parámetro `ProductArn` para especificar el nombre de recurso de Amazon (ARN) de la integración.

Por ejemplo, el siguiente AWS CLI comando recupera detalles sobre la integración de Security Hub CSPM con 3CoreSec.

```
$ aws securityhub describe-products --product-arn "arn:aws:securityhub:us-east-1::product/3coresec/3coresec"
```

Habilitación del flujo de resultados desde una integración del CSPM de Security Hub

En la página de integraciones de la consola CSPM de AWS Security Hub, puede ver los pasos necesarios para habilitar cada integración.

Para la mayoría de las integraciones con otros Servicios de AWS, el único paso necesario para habilitar la integración es habilitar el otro servicio. La información de integración incluye un enlace a la página principal del otro servicio. Cuando habilita el otro servicio, se crea y aplica automáticamente un permiso a nivel de recurso que permite al CSPM de Security Hub recibir resultados desde ese servicio.

En el caso de las integraciones de productos de terceros, es posible que tengas que comprar la integración en el y AWS Marketplace, a continuación, configurarla. La información de integración proporciona enlaces para completar estas tareas.

Si hay más de una versión de un producto disponible AWS Marketplace, selecciona la versión a la que quieres suscribirte y, a continuación, elige Continuar con la suscripción. Por ejemplo, algunos productos ofrecen una versión estándar y una AWS GovCloud (US) versión.

Cuando se habilita una integración de productos, se asocia automáticamente una política de recursos a la suscripción del producto. Esta política de recursos define los permisos que el CSPM de Security Hub necesita para recibir resultados de ese producto.

Una vez que haya completado los pasos preliminares para habilitar una integración, puede deshabilitar y volver a habilitar el flujo de resultados desde esa integración. En la página

Integraciones, para las integraciones que envíen resultados, el campo Estado indica si está actualmente aceptando resultados.

Security Hub CSPM console

Para deshabilitar y habilitar el flujo de resultados desde una integración (consola)

1. Abra la consola CSPM de AWS Security Hub en. https://console.aws.amazon.com/securityhub/
2. En el panel de navegación del CSPM de Security Hub, seleccione Integraciones.
3. En el caso de las integraciones que envían resultados, la información de Estado indica si el CSPM de Security Hub actualmente acepta resultados a partir de esa integración.
4. Seleccione Aceptar los resultados.

Security Hub CSPM API

Utilice la operación EnableImportFindingsForProduct. Si está utilizando el AWS CLI, ejecute el enable-import-findings-for-product comando. Para permitir que Security Hub reciba resultados desde una integración, necesita el ARN del producto. Para obtener los ARN de las integraciones disponibles, utilice la operación DescribeProducts. Si está utilizando el AWS CLI, ejecute el describe-products.

Por ejemplo, el siguiente AWS CLI comando permite que Security Hub CSPM reciba los resultados de la integración de CrowdStrike Falcon. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$ aws securityhub enable-import-findings-for product --product-arn
 "arn:aws:securityhub:us-east-1:123456789333:product/crowdstrike/crowdstrike-falcon"
```

Desactivación del flujo de resultados provenientes de una integración con el CSPM de Security Hub

Elija el método que prefiera y siga los pasos para deshabilitar el flujo de hallazgos desde una integración de AWS Security Hub con CSPM.

Security Hub CSPM console

Para deshabilitar el flujo de resultados desde una integración (consola)

1. Abra la consola AWS CSPM de Security Hub en. https://console.aws.amazon.com/securityhub/
2. En el panel de navegación del CSPM de Security Hub, seleccione Integraciones.
3. En el caso de las integraciones que envían resultados, la información de Estado indica si el CSPM de Security Hub actualmente acepta resultados a partir de esa integración.
4. Seleccione Dejar de aceptar resultados.

Security Hub CSPM API

Utilice la operación DisableImportFindingsForProduct. Si está utilizando el AWS CLI, ejecute el disable-import-findings-for-product comando. Para desactivar el flujo de resultados de una integración, necesita el ARN de suscripción para la integración habilitada. Para obtener el ARN de suscripción, utilice la operación ListEnabledProductsForImport. Si está utilizando el AWS CLI, ejecute el list-enabled-products-for-import.

Por ejemplo, el siguiente AWS CLI comando desactiva el flujo de hallazgos al CSPM de Security Hub desde la CrowdStrike integración de Falcon. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$ aws securityhub disable-import-findings-for-product --product-subscription-arn
 "arn:aws:securityhub:us-west-1:123456789012:product-subscription/crowdstrike/
crowdstrike-falcon"
```

Visualización de los resultados a partir de una integración con el CSPM de Security Hub

Cuando empiece a aceptar las conclusiones de una integración de CSPM de AWS Security Hub, la página de integraciones de la consola de CSPM de Security Hub mostrará el estado de la integración como Conclusiones aceptadas. Para ver una lista de los resultados provenientes de la integración, seleccione Ver resultados.

La lista de resultados muestra los resultados activos de la integración seleccionada que tienen un estado de flujo de trabajo `NEW` o `NOTIFIED`.

Si habilita la agregación entre regiones, en la región de agregación, la lista incluye los resultados de la región de agregación y de las regiones vinculadas en las que la integración esté habilitada. Security Hub no habilita de forma automática las integraciones basadas en la configuración de agregación entre regiones.

En otras regiones, la lista de resultados de una integración solo contiene los resultados de la región actual.

Para obtener información sobre cómo configurar la agregación entre regiones, consulte the section called “Agregar datos en las regiones”.

En la lista de resultados puede realizar las siguientes acciones.

- Cambiar los filtros y la agrupación de la lista
- Ver los detalles de cada resultado
- Actualizar el estado de flujo de trabajo de los resultados
- Enviar los resultados a acciones personalizadas

Servicio de AWS integraciones con Security Hub CSPM

AWS Security Hub CSPM admite integraciones con varios otros. Servicios de AWS Estas integraciones pueden ayudar a obtener una visión global de la seguridad y conformidad en todo su entorno de AWS .

A menos que se indique lo contrario a continuación, Servicio de AWS las integraciones que envían las conclusiones al CSPM de Security Hub se activan automáticamente después de habilitar Security Hub CSPM y el otro servicio. Es posible que se necesite realizar pasos adicionales para habilitar algunas integraciones que reciben resultados del CSPM de Security Hub. Revise la información sobre cada integración para obtener más información.

Algunas integraciones no están disponibles en todas. Regiones de AWS En la consola del CSPM de Security Hub, una integración no aparece en la página Integraciones si no es compatible en la región actual. Para ver una lista de las integraciones que están disponibles en las regiones de China AWS GovCloud (US) Regions, consulta. Disponibilidad de las integraciones por región

Descripción general de AWS integraciones de servicios con Security Hub CSPM

La siguiente tabla proporciona una descripción general de AWS los servicios que envían los hallazgos al CSPM de Security Hub o los reciben del CSPM de Security Hub.

Servicio integrado AWS	Dirección
AWS Config	Envía resultados
AWS Firewall Manager	Envía resultados
Amazon GuardDuty	Envía resultados
AWS Health	Envía resultados
AWS Identity and Access Management Access Analyzer	Envía resultados
Amazon Inspector	Envía resultados
AWS IoT Device Defender	Envía resultados
Amazon Macie	Envía resultados
Amazon Route 53 Resolver Firewall DNS	Envía resultados
AWS Systems Manager Patch Manager	Envía resultados
AWS Audit Manager	Recibe resultados
Amazon Q Developer en aplicaciones de chat	Recibe resultados
Amazon Detective	Recibe resultados
Amazon Security Lake	Recibe resultados
AWS Systems Manager E xplorer y OpsCenter	Recibe y actualiza resultados

Servicio integrado AWS	Dirección	
AWS Trusted Advisor	Recibe resultados	

Servicios de AWS que envían los hallazgos a Security Hub (CSPM)

Los siguientes elementos se Servicios de AWS integran con el CSPM de Security Hub y pueden enviar los hallazgos a este. El CSPM de Security Hub convierte los resultados al Formato de resultados de seguridad de AWS.

AWS Config (Envía las conclusiones)

AWS Config es un servicio que le permite evaluar, auditar y evaluar las configuraciones de sus AWS recursos. AWS Config supervisa y registra de forma continua las configuraciones de sus AWS recursos y le permite automatizar la evaluación de las configuraciones registradas comparándolas con las configuraciones deseadas.

Al utilizar la integración con AWS Config, puede ver los resultados de las evaluaciones de reglas AWS Config administradas y personalizadas como hallazgos en Security Hub CSPM. Estos resultados se pueden ver junto con otros resultados del CSPM de Security Hub, lo que proporciona una visión general completa de la posición de seguridad.

AWS Config usa Amazon EventBridge para enviar evaluaciones de AWS Config reglas a Security Hub CSPM. El CSPM de Security Hub transforma las evaluaciones de reglas en resultados que adoptan el Formato de resultados de seguridad de AWS. Posteriormente, el CSPM de Security Hub complementa los resultados, según sea posible, con información adicional sobre los recursos afectados, como el nombre de recurso de Amazon (ARN), las etiquetas del recurso y la fecha de creación.

Para obtener más información sobre esta integración, consulte las secciones siguientes.

Cómo AWS Config envía las conclusiones a Security Hub (CSPM).

Todos los resultados en el CSPM de Security Hub usan el formato JSON estándar de ASFF. El ASFF incluye detalles sobre el origen del hallazgo, el recurso afectado y el estado actual del hallazgo. AWS Config envía evaluaciones de reglas gestionadas y personalizadas a Security Hub CSPM a través de. EventBridge El CSPM de Security Hub transforma las evaluaciones de reglas en resultados que siguen el formato ASFF y enriquece los resultados en la medida de lo posible.

Tipos de hallazgos que AWS Config envía a Security Hub CSPM

Una vez activada la integración, AWS Config envía las evaluaciones de todas las reglas AWS Config administradas y personalizadas al CSPM de Security Hub. Solo se envían las evaluaciones que se realizaron después de habilitar el CSPM de Security Hub. Por ejemplo, supongamos que la evaluación de una regla de AWS Config revela cinco recursos fallidos. Si habilita el CSPM de Security Hub después de esa evaluación y la regla identifica un sexto recurso con fallas, AWS Config envía únicamente la evaluación de ese sexto recurso al CSPM de Security Hub.

Se excluyen las evaluaciones a partir de AWS Config reglas vinculadas a servicios, como las que se utilizan para comprobar los controles de CSPM de Security Hub. La excepción son las conclusiones generadas por las reglas vinculadas a servicios que crean y administran en. AWS Control Tower AWS Config Incluir las conclusiones de estas reglas ayuda a garantizar que los datos de las conclusiones incluyan los resultados de las comprobaciones proactivas realizadas por. AWS Control Tower

Enviando AWS Config hallazgos a Security Hub CSPM

Cuando se activa la integración, el CSPM de Security Hub asigna automáticamente los permisos necesarios para recibir resultados de AWS Config. El CSPM de Security Hub utiliza permisos de nivel de servicio a servicio que le proporcionan una forma segura de activar esta integración e importar los resultados desde Amazon. AWS Config EventBridge

Latencia para el envío de resultados

Cuando AWS Config crea un nuevo resultado, normalmente puede verlo en Security Hub CSPM en un plazo de cinco minutos.

Reintentos cuando el CSPM de Security Hub no está disponible

AWS Config envía los hallazgos al CSPM de Security Hub haciendo el mejor esfuerzo posible. EventBridge Cuando un evento no se envía correctamente al CSPM de Security Hub, EventBridge vuelve a intentarlo hasta 24 horas o 185 veces, lo que ocurra primero.

Actualizando el existente AWS Config hallazgos en Security Hub CSPM

Tras enviar AWS Config un hallazgo al CSPM de Security Hub, este puede enviar actualizaciones del mismo resultado al CSPM de Security Hub para reflejar las observaciones adicionales sobre la actividad de búsqueda. Las actualizaciones solo se envían para eventos de

`ComplianceChangeNotification`. Si no se produce ningún cambio relacionado con el cumplimiento, no se envían actualizaciones al CSPM de Security Hub. El CSPM de Security Hub elimina los resultados a los 90 días desde su actualización más reciente o, si no ocurre ninguna actualización, a los 90 días desde su creación.

El CSPM de Security Hub no archiva los hallazgos desde los que se envían, AWS Config incluso si se elimina el recurso asociado.

Regiones en las que AWS Config existen hallazgos

AWS Config los hallazgos se producen a nivel regional. AWS Config envía los hallazgos al CSPM de Security Hub en la misma región o regiones en las que se producen los hallazgos.

Visualización AWS Config hallazgos en Security Hub (CSPM).

Para ver sus AWS Config hallazgos, seleccione Hallazgos en el panel de navegación de Security Hub CSPM. Para filtrar los hallazgos y mostrar solo los AWS Config hallazgos, seleccione el nombre del producto en el menú desplegable de la barra de búsqueda. Introduzca Config y seleccione Aplicar.

Interpretación AWS Config buscar nombres en Security Hub CSPM

El CSPM de Security Hub transforma las evaluaciones de AWS Config reglas en hallazgos que siguen a. AWS Formato de búsqueda de seguridad (ASFF) AWS Config las evaluaciones de reglas utilizan un patrón de eventos diferente en comparación con el ASFF. La siguiente tabla asigna los campos de las evaluaciones de reglas de AWS Config a sus equivalentes en el ASFF tal como aparecen en el CSPM de Security Hub.

Configuración de tipo de resultado de la evaluación de reglas	Tipo de resultado ASFF	Valor codificado
detail.aws AccountId	AwsAccountId	
detall.nuevo Evaluatio nResult.resultRecordedTime	CreatedAt	
detalle. nuevo Evaluatio nResult.resultRecordedTime	UpdatedAt	

Configuración de tipo de resultado de la evaluación de reglas	Tipo de resultado ASFF	Valor codificado
	ProductArn	<partition><region >«arn ::securityhub:: /config» product/aws
	ProductName	“Config”
	CompanyName	"AWS"
	Region	“eu-central-1”
configuración RuleArn	GeneratorId, ProductFields	
detalle. ConfigRuleARN/find ing/hash	Id	
detail.config RuleName	Título, ProductFields	
detail.config RuleName	Description (Descripción)	“Este resultado se crea para un cambio de conformidad del recurso para la regla de configuración: `${detail. ConfigRuleName}` “
Elemento de configuración “ARN” o ARN calculado por el CSPM de Security Hub	Resources[i].id	
detail.resourceType	Resources[i].Type	"AwsS3Bucket"
	Resources[i].Partition	"aws"
	Resources[i].Region	“eu-central-1”
Elemento de configuración “configuración”	Resources[i].Details	

Configuración de tipo de resultado de la evaluación de reglas	Tipo de resultado ASFF	Valor codificado
	SchemaVersion	“10/08/2018”
	Severity.Label	Consultar “Interpretación de la etiqueta de gravedad” a continuación
	Tipos	[“Comprobaciones de configuración y software”]
detail.new EvaluationResult.complianceType	Compliance.Status	“NO_APROBADO”, “NO_DISPONIBLE”, “APROBADO” o “ADVERTENCIA”
	Workflow.Status	«RESUELTO» si se AWS Config genera un resultado con el Compliance.Status signo «APROBADO» o si el resultado Compliance.Status cambia de «FALLIDO» a «APROBADO». De lo contrario, Workflow.Status será «NUEVO». Puede cambiar este valor con la operación de la BatchUpdateFindings API.

Interpretación de la etiqueta de gravedad

Todos los resultados de las evaluaciones de AWS Config reglas tienen una etiqueta de gravedad predeterminada de MEDIUM en la ASFF. Puede actualizar la etiqueta de gravedad de un resultado con la operación de la API `BatchUpdateFindings`.

Hallazgo típico de AWS Config

El CSPM de Security Hub transforma las evaluaciones de las AWS Config reglas en hallazgos que siguen la ASFF. El siguiente es un ejemplo de un hallazgo típico de la ASFF AWS Config .

> **Note**
>
> Si la descripción tiene más de 1.024 caracteres, se truncará a 1.024 caracteres y dirá «(truncada)» al final.


```
{
 "SchemaVersion": "2018-10-08",
 "Id": "arn:aws:config:eu-central-1:123456789012:config-rule/config-rule-mburzq/
finding/45g070df80cb50b68fa6a43594kc6fda1e517932",
 "ProductArn": "arn:aws:securityhub:eu-central-1::product/aws/config",
 "ProductName": "Config",
 "CompanyName": "AWS",
 "Region": "eu-central-1",
 "GeneratorId": "arn:aws:config:eu-central-1:123456789012:config-rule/config-rule-
mburzq",
 "AwsAccountId": "123456789012",
 "Types": [
  "Software and Configuration Checks"
 ],
 "CreatedAt": "2022-04-15T05:00:37.181Z",
 "UpdatedAt": "2022-04-19T21:20:15.056Z",
 "Severity": {
  "Label": "MEDIUM",
  "Normalized": 40
 },
 "Title": "s3-bucket-level-public-access-prohibited-config-integration-demo",
 "Description": "This finding is created for a resource compliance change for config
 rule: s3-bucket-level-public-access-prohibited-config-integration-demo",
 "ProductFields": {
  "aws/securityhub/ProductName": "Config",
  "aws/securityhub/CompanyName": "AWS",
  "aws/securityhub/FindingId": "arn:aws:securityhub:eu-central-1::product/aws/
config/arn:aws:config:eu-central-1:123456789012:config-rule/config-rule-mburzq/
finding/46f070df80cd50b68fa6a43594dc5fda1e517902",
  "aws/config/ConfigRuleArn": "arn:aws:config:eu-central-1:123456789012:config-rule/
config-rule-mburzq",
```

```
  "aws/config/ConfigRuleName": "s3-bucket-level-public-access-prohibited-config-
integration-demo",
  "aws/config/ConfigComplianceType": "NON_COMPLIANT"
 },
 "Resources": [{
  "Type": "AwsS3Bucket",
  "Id": "arn:aws:s3:::amzn-s3-demo-bucket",
  "Partition": "aws",
  "Region": "eu-central-1",
  "Details": {
   "AwsS3Bucket": {
    "OwnerId": "4edbba300f1caa608fba2aad2c8fcfe30c32ca32777f64451eec4fb2a0f10d8c",
    "CreatedAt": "2022-04-15T04:32:53.000Z"
   }
  }
 }],
 "Compliance": {
  "Status": "FAILED"
 },
 "WorkflowState": "NEW",
 "Workflow": {
  "Status": "NEW"
 },
 "RecordState": "ACTIVE",
 "FindingProviderFields": {
  "Severity": {
   "Label": "MEDIUM"
  },
  "Types": [
   "Software and Configuration Checks"
  ]
 }
}
```


Habilitación y configuración de la integración

Después de habilitar el CSPM de Security Hub, esta integración se activa automáticamente. AWS Config empieza a enviar resultados al CSPM de Security Hub de inmediato.

Cómo detener la publicación de resultados en el CSPM de Security Hub

Para dejar de enviar resultados al CSPM de Security Hub, puede usar la consola del CSPM de Security Hub o la API del CSPM de Security Hub.

Para obtener instrucciones sobre cómo detener el flujo de resultados, consulte Habilitación del flujo de resultados desde una integración del CSPM de Security Hub.

AWS Firewall Manager (Envía los resultados)

Firewall Manager envía resultados al CSPM de Security Hub cuando una política de firewall de aplicaciones web (WAF) para recursos o una regla de lista de control de acceso web (web ACL) no cumple con los requisitos de cumplimiento. Firewall Manager también envía las conclusiones cuando AWS Shield Advanced no protege los recursos o cuando se identifica un ataque.

Después de habilitar el CSPM de Security Hub, esta integración se activa automáticamente. Firewall Manager empieza a enviar resultados al CSPM de Security Hub de inmediato.

Para obtener más información sobre la integración, consulte la página Integraciones en la consola del CSPM de Security Hub.

Para obtener más información sobre Firewall Manager, consulte la Guía para desarrolladores de AWS WAF .

Amazon GuardDuty (envía los hallazgos)

GuardDuty envía todos los tipos de búsqueda que genera a Security Hub CSPM. Algunos tipos de resultados tienen requisitos previos, requisitos de habilitación o limitaciones por región. Para obtener más información, consulte la GuardDuty búsqueda de tipos en la Guía del GuardDuty usuario de Amazon.

Las nuevas conclusiones de GuardDuty se envían a Security Hub CSPM en un plazo de cinco minutos. Las actualizaciones de los hallazgos se envían en función de la configuración de hallazgos actualizados para Amazon EventBridge en GuardDuty la configuración.

Al generar resultados de GuardDuty muestra mediante la página de GuardDuty configuración, Security Hub CSPM recibe los resultados de muestra y omite el prefijo `[Sample]` en el tipo de resultado. Por ejemplo, el ejemplo de búsqueda introducido GuardDuty `[SAMPLE] Recon:IAMUser/ResourcePermissions` se muestra como `Recon:IAMUser/ResourcePermissions` en Security Hub CSPM.

Después de habilitar el CSPM de Security Hub, esta integración se activa automáticamente. GuardDuty empieza inmediatamente a enviar resultados al CSPM de Security Hub.

Para obtener más información sobre la GuardDuty integración, consulte Integración con AWS Security Hub CSPM en la Guía del usuario de Amazon. GuardDuty

AWS Health (Envía los hallazgos)

AWS Health proporciona una visibilidad continua del rendimiento de sus recursos y la disponibilidad de su Servicios de AWS tierra Cuentas de AWS. Puede usar los eventos AWS Health para saber cómo pueden afectar los cambios de servicios y recursos a las aplicaciones que ejecuta en AWS.

La integración con AWS Health no utiliza`BatchImportFindings`. En su lugar, AWS Health utiliza la mensajería de eventos de servicio a servicio para enviar las conclusiones al CSPM de Security Hub.

Para obtener más información sobre la integración, consulte las siguientes secciones.

Cómo AWS Health envía las conclusiones a Security Hub (CSPM).

En Security Hub CSPM, se realiza seguimiento de los problemas de seguridad como resultados. Algunos hallazgos provienen de problemas detectados por otros AWS servicios o por socios externos. El CSPM de Security Hub también cuenta con un conjunto de reglas que utiliza para detectar problemas de seguridad y generar resultados.

El CSPM de Security Hub proporciona herramientas para administrar resultados procedentes de todos estos orígenes. Puede ver y filtrar listas de resultados y ver los detalles de una búsqueda. Consulte Revisión de detalles e historial de resultados en el CSPM de Security Hub. También puede realizar un seguimiento del estado de una investigación sobre un resultado. Consulte Configuración del estado del flujo de trabajo de los resultados en el CSPM de Security Hub.

Todos los resultados en el CSPM de Security Hub utilizan un formato JSON estándar denominado AWS Formato de búsqueda de seguridad (ASFF). ASFF incluye detalles sobre el origen del problema, los recursos afectados y el estado actual del resultado.

AWS Health es uno de los AWS servicios que envía los hallazgos al CSPM de Security Hub.

Tipos de hallazgos que AWS Health envía a Security Hub CSPM

Una vez habilitada la integración, AWS Health envía los hallazgos que cumplen con una o más de las especificaciones enumeradas al CSPM de Security Hub. El CSPM de Security Hub ingiere los resultados en el AWS Formato de búsqueda de seguridad (ASFF).

- Resultados que contienen cualquiera de los siguientes valores para el Servicio de AWS:
  - `RISK`
  - `ABUSE`
  - `ACM`
  - `CLOUDHSM`

- CLOUDTRAIL
- CONFIG
- CONTROLTOWER
- DETECTIVE
- EVENTS
- GUARDDUTY
- IAM
- INSPECTOR
- KMS
- MACIE
- SES
- SECURITYHUB
- SHIELD
- SSO
- COGNITO
- IOTDEVICEDEFENDER
- NETWORKFIREWALL
- ROUTE53
- WAF
- FIREWALLMANAGER
- SECRETSMANAGER
- BACKUP
- AUDITMANAGER
- ARTIFACT
- CLOUDENDURE
- CODEGURU
- ORGANIZATIONS
- DIRECTORYSERVICE
- RESOURCEMANAGER

- CLOUDWATCH

  - `DRS`
  - `INSPECTOR2`
  - `RESILIENCEHUB`
- Hallazgos con las palabras `securityabuse`, o `certificate` en el campo AWS Health `typeCode`
- Hallazgos sobre dónde se encuentra el AWS Health servicio `risk` o `abuse`

Enviando AWS Health hallazgos a Security Hub CSPM

Si decide aceptar las conclusiones de AWS Health, Security Hub CSPM asignará automáticamente los permisos necesarios para recibir las conclusiones de. AWS Health Security Hub CSPM utiliza permisos de nivel de servicio a servicio que le proporcionan una forma fácil y segura de habilitar esta integración e importar los hallazgos desde AWS Health Amazon en su nombre. EventBridge Al seleccionar Aceptar resultados, otorga al CSPM de Security Hub el permiso para consumir resultados provenientes de AWS Health.

Latencia para el envío de resultados

Cuando se AWS Health crea un nuevo resultado, normalmente se envía al CSPM de Security Hub en un plazo de cinco minutos.

Reintentos cuando el CSPM de Security Hub no está disponible

AWS Health envía los resultados al CSPM de Security Hub haciendo todo lo posible. EventBridge Cuando un evento no se envía correctamente a Security Hub CSPM, EventBridge vuelve a intentar enviar el evento durante 24 horas.

Actualización de resultados existentes en el CSPM de Security Hub

Después de AWS Health enviar un hallazgo al CSPM de Security Hub, este puede enviar actualizaciones sobre el mismo resultado para reflejar las observaciones adicionales sobre la actividad de búsqueda al CSPM de Security Hub.

Regiones en las que existen resultados

En el caso de los eventos mundiales, AWS Health envía los resultados al CSPM de Security Hub en us-east-1 (AWS partición), cn-northwest-1 (partición de China) y gov-us-west-1 (partición). GovCloud AWS Health envía Region-specific los eventos al CSPM de Security Hub en la misma región o regiones en las que se producen los eventos.

Visualización AWS Health hallazgos en Security Hub (CSPM).

Para ver sus AWS Health hallazgos en Security Hub CSPM, seleccione Hallazgos en el panel de navegación. Para filtrar los hallazgos y mostrar solo AWS Health los hallazgos, selecciona Salud en el campo Nombre del producto.

Interpretación AWS Health buscar nombres en Security Hub CSPM

AWS Health envía los resultados al CSPM de Security Hub mediante el. AWS Formato de búsqueda de seguridad (ASFF) AWS Health finding utiliza un patrón de eventos diferente al del formato ASFF CSPM de Security Hub. En la siguiente tabla se detallan todos los campos de AWS Health búsqueda con sus equivalentes en ASFF tal y como aparecen en el CSPM de Security Hub.

Tipo de resultado de Estado	Tipo de resultado ASFF	Valor codificado
inscrita	AwsAccountId	
detail.startTime	CreatedAt	
detalle.evento Descripti on.latestDescription	Description (Descripción)	
detall.evento TypeCode	GeneratorId	
detail.eventArn (incluido account) + hash de detail.st artTime	Id	
<region>«arn:aws:security hub:: /health» product/aws	ProductArn	
account o resourceId	Resources[i].id	
	Resources[i].Type	“Otros”
	SchemaVersion	“10/08/2018”
	Severity.Label	Consultar “Interpretación de la etiqueta de gravedad” a continuación

Tipo de resultado de Estado	Tipo de resultado ASFF	Valor codificado
AWS Health «-» detalle.evento TypeCode	Title	
-	Tipos	[“Comprobaciones de configuración y software”]
event.time	UpdatedAt	
URL del evento de la consola Estado	SourceUrl	

Interpretación de la etiqueta de gravedad

La etiqueta de gravedad del resultado de ASFF se determina mediante la siguiente lógica:

- Gravedad CRÍTICA si:
  - El campo `service` del resultado AWS Health tiene el valor `Risk`
  - El campo `typeCode` del resultado AWS Health tiene el valor `AWS_S3_OPEN_ACCESS_BUCKET_NOTIFICATION`
  - El campo `typeCode` del resultado AWS Health tiene el valor `AWS_SHIELD_INTERNET_TRAFFIC_LIMITATIONS_PLACED_IN_RESPONSE_TO_DDOS_ATTACK`
  - El campo `typeCode` del resultado AWS Health tiene el valor `AWS_SHIELD_IS_RESPONDING_TO_A_DDOS_ATTACK_AGAINST_YOUR_AWS_RESOURCES`

  Gravedad ALTA si:

  - El campo `service` del resultado AWS Health tiene el valor `Abuse`
  - El campo `typeCode` del resultado AWS Health contiene el valor `SECURITY_NOTIFICATION`
  - El campo `typeCode` del resultado AWS Health contiene el valor `ABUSE_DETECTION`

  Gravedad MEDIA si:

  - El campo `service` del resultado es cualquiera de los siguientes: `ACM`, `ARTIFACT`, `AUDITMANAGER`, `BACKUP`, `CLOUDENDURE`, `CLOUDHSM`, `CLOUDTRAIL`, `CLOUDWATCH`, `CODEGURGU`, `COGNITO`, `CONFIG`, `CONTROLTOWER`, `DETECTIVE`, `DIRECTORYSERVICE`, `DRS`, `EVENTS`, `FIREWALLMANAGER`, `GUARDDUTY`, `IAM`, `INSPECTOR`, `INSPECTOR2`,

IOTDEVICEDEFENDER, KMS, MACIE, NETWORKFIREWALL, ORGANIZATIONS, RESILIENCEHUB, RESOURCEMANAGER, ROUTE53, SECURITYHUB, SECRETSMANAGER, SES, SHIELD, SSO o WAF

- El campo typeCode del resultado AWS Health contiene el valor CERTIFICATE
- El campo typeCode del resultado AWS Health contiene el valor END_OF_SUPPORT

Hallazgo típico de AWS Health

AWS Health envía los resultados al CSPM de Security Hub mediante el. AWS Formato de búsqueda de seguridad (ASFF) El siguiente es un ejemplo de un hallazgo típico de. AWS Health

> **Note**
>
> Si la descripción contiene más de 1024 caracteres, se truncará en 1024 caracteres y al final dirá (truncada).


```
{
            "SchemaVersion": "2018-10-08",
            "Id": "arn:aws:health:us-east-1:123456789012:event/SES/
AWS_SES_CMF_PENDING_TO_SUCCESS/
AWS_SES_CMF_PENDING_TO_SUCCESS_303388638044_33fe2115-8dad-40ce-
b533-78e29f49de96/101F7FBAEFC663977DA09CFF56A29236602834D2D361E6A8CA5140BFB3A69B30",
            "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/health",
            "GeneratorId": "AWS_SES_CMF_PENDING_TO_SUCCESS",
            "AwsAccountId": "123456789012",
            "Types": [
                "Software and Configuration Checks"
            ],
            "CreatedAt": "2022-01-07T16:34:04.000Z",
            "UpdatedAt": "2022-01-07T19:17:43.000Z",
            "Severity": {
                "Label": "MEDIUM",
                "Normalized": 40
            },
            "Title": "AWS Health - AWS_SES_CMF_PENDING_TO_SUCCESS",
            "Description": "Congratulations! Amazon SES has successfully detected the
 MX record required to use 4557227d-9257-4e49-8d5b-18a99ced4be9.cmf.pinpoint.sysmon-
iad.adzel.com as a custom MAIL FROM domain for verified identity cmf.pinpoint.sysmon-
iad.adzel.com in AWS Region US East (N. Virginia).\\n\\nYou can now use this MAIL
 FROM domain with cmf.pinpoint.sysmon-iad.adzel.com and any other verified identity
```

```
 that is configured to use it. For information about how to configure a verified
 identity to use a custom MAIL FROM domain, see http://docs.aws.amazon.com/ses/latest/
DeveloperGuide/mail-from-set.html .\\n\\nPlease note that this email only applies to
 AWS Region US East (N. Virginia).",
            "SourceUrl": "https://phd.aws.amazon.com/phd/home#/event-log?
eventID=arn:aws:health:us-east-1::event/SES/AWS_SES_CMF_PENDING_TO_SUCCESS/
AWS_SES_CMF_PENDING_TO_SUCCESS_303388638044_33fe2115-8dad-40ce-b533-78e29f49de96",
            "ProductFields": {
                "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/
aws/health/arn:aws:health:us-east-1::event/SES/AWS_SES_CMF_PENDING_TO_SUCCESS/
AWS_SES_CMF_PENDING_TO_SUCCESS_303388638044_33fe2115-8dad-40ce-b533-78e29f49de96",
                "aws/securityhub/ProductName": "Health",
                "aws/securityhub/CompanyName": "AWS"
            },
            "Resources": [
                {
                    "Type": "Other",
                    "Id": "4557227d-9257-4e49-8d5b-18a99ced4be9.cmf.pinpoint.sysmon-
iad.adzel.com"
                }
            ],
            "WorkflowState": "NEW",
            "Workflow": {
                "Status": "NEW"
            },
            "RecordState": "ACTIVE",
            "FindingProviderFields": {
                "Severity": {
                    "Label": "MEDIUM"
                },
                "Types": [
                    "Software and Configuration Checks"
                ]
            }
        }
    ]
}
```

Habilitación y configuración de la integración

Después de habilitar el CSPM de Security Hub, esta integración se activa automáticamente. AWS Health empieza inmediatamente a enviar resultados al CSPM de Security Hub.

Cómo detener la publicación de resultados en el CSPM de Security Hub

Para dejar de enviar resultados al CSPM de Security Hub, puede usar la consola del CSPM de Security Hub o la API del CSPM de Security Hub.

Para obtener instrucciones sobre cómo detener el flujo de resultados, consulte Habilitación del flujo de resultados desde una integración del CSPM de Security Hub.

AWS Identity and Access Management Access Analyzer (Envía los hallazgos)

Con el Analizador de acceso de IAM, todos los resultados se envían al CSPM de Security Hub.

IAM Access Analyzer utiliza un razonamiento lógico para analizar las políticas basadas en recursos que se aplican a los recursos de la cuenta compatibles. IAM Access Analyzer genera un resultado cuando detecta una declaración de la política que permite que una entidad principal externa pueda acceder a un recurso de la cuenta.

En IAM Access Analyzer, solo la cuenta de administrador puede ver los resultados de los analizadores que se aplican a una organización. En el caso de los analizadores de la organización, el campo `AwsAccountId` ASFF refleja el ID de la cuenta de administrador. Bajo `ProductFields`, el campo `ResourceOwnerAccount` indica la cuenta en la que se descubrió el resultado. Si habilita analizadores de forma individual para cada cuenta, el CSPM de Security Hub genera varios resultados: uno que identifica el ID de la cuenta de administrador y otro que identifica el ID de la cuenta de recursos.

Para obtener más información, consulte Integración con AWS Security Hub CSPM en la guía del usuario de IAM.

Amazon Inspector (Envía resultados)

Amazon Inspector es un servicio de gestión de vulnerabilidades que analiza continuamente sus cargas de trabajo en AWS en busca de vulnerabilidades. Amazon Inspector descubre y escanea automáticamente las instancias e imágenes de contenedor de Amazon EC2 que residen en Amazon Elastic Container Registry. El escaneo busca vulnerabilidades de software y exposición no deseada en la red.

Después de habilitar el CSPM de Security Hub, esta integración se activa automáticamente. Amazon Inspector comienza de inmediato a enviar al CSPM de Security Hub todos los resultados que genera.

Para obtener más información sobre la integración, consulte Integración con el CSPM de AWS Security Hub en la Guía del usuario de Amazon Inspector.

El CSPM de Security Hub también puede recibir resultados de Amazon Inspector Classic. Amazon Inspector Classic envía al CSPM de Security Hub los resultados generados durante las ejecuciones de evaluaciones para todos los paquetes de reglas admitidos.

Para obtener más información sobre la integración, consulte Integración con AWS Security Hub CSPM en la guía del usuario de Amazon Inspector Classic.

Los resultados de Amazon Inspector y Amazon Inspector Classic utilizan el mismo ARN de producto. Los resultados de Amazon Inspector presentan la siguiente entrada en `ProductFields`:

```
"aws/inspector/ProductVersion": "2",
```

> **Note**
>
> Los resultados de seguridad generados por Amazon Inspector Code Security no están disponibles para esta integración. Sin embargo, puede acceder a estos resultados concretos en la consola de Amazon Inspector y a través de la API de Amazon Inspector.

AWS IoT Device Defender (Envía los hallazgos)

AWS IoT Device Defender es un servicio de seguridad que audita la configuración de sus dispositivos de IoT, monitorea los dispositivos conectados para detectar comportamientos anormales y ayuda a mitigar los riesgos de seguridad.

Tras habilitar AWS IoT Device Defender tanto el CSPM como Security Hub, visite la página de integraciones de la consola CSPM de Security Hub y elija Aceptar los hallazgos para auditar, Detectar o ambos. AWS IoT Device Defender Audit and Detect comienza a enviar todos los resultados al CSPM de Security Hub.

AWS IoT Device Defender Audit envía los resúmenes de las comprobaciones al CSPM de Security Hub, que contienen información general sobre un tipo de comprobación de auditoría y una tarea de auditoría específicos. AWS IoT Device Defender Detect envía al CSPM de Security Hub los resultados de las infracciones en relación con el aprendizaje automático (ML), los comportamientos estadísticos y estáticos. Audit también envía actualizaciones de resultados al CSPM de Security Hub.

Para obtener más información sobre esta integración, consulte Integración con el CSPM de AWS Security Hub en la Guía del desarrollador de AWS IoT .

Amazon Macie (Envía resultados)

Amazon Macie es un servicio de seguridad de datos que detecta datos confidenciales mediante el machine learning y la coincidencia de patrones, proporciona visibilidad de los riesgos de seguridad de los datos y permite establecer una protección automatizada contra esos riesgos. Un resultado de Macie puede indicar que existe una posible infracción de políticas o información confidencial en el entorno de datos de Amazon S3.

Después de habilitar el CSPM de Security Hub, Macie comienza automáticamente a enviar resultados de políticas al CSPM de Security Hub. Es posible configurar la integración para que también envíe resultados de información confidencial al CSPM de Security Hub.

En el CSPM de Security Hub, el tipo de resultado para un resultado de políticas o de información confidencial se cambia a un valor compatible con el formato ASFF. Por ejemplo, el tipo de resultado `Policy:IAMUser/S3BucketPublic` en Macie se muestra como `Effects/Data Exposure/Policy:IAMUser-S3BucketPublic` en el CSPM de Security Hub.

Macie también envía resultados de ejemplo generados al CSPM de Security Hub. En el caso de los resultados de muestra, el nombre del recurso afectado es `macie-sample-finding-bucket` y el valor del campo `Sample` es `true`.

Para obtener más información, consulte Evaluación de resultados de Macie con Security Hub en la Guía del usuario de Amazon Macie.

Amazon Route 53 Resolver Firewall DNS (envía las conclusiones)

Con el firewall de Amazon Route 53 Resolver DNS, puede filtrar y regular el tráfico de DNS saliente para su nube privada virtual (VPC). Esto se logra mediante la creación de colecciones reutilizables de reglas de filtrado en grupos de reglas de DNS Firewall, la asociación de esos grupos de reglas con la VPC y la supervisión de la actividad en los registros y métricas de DNS Firewall. Puede ajustar cómo se comporta DNS Firewall en función de la actividad observada. DNS Firewall es una característica de Route 53 Resolver.

Route 53 Resolver DNS Firewall puede enviar varios tipos de resultados al CSPM de Security Hub:

- Hallazgos relacionados con consultas bloqueadas o alertadas para los dominios asociados a las listas de dominios AWS administradas, que son listas de dominios que AWS administra.
- Resultados relacionados con consultas bloqueadas o con alertas en dominios asociados con una lista de dominios personalizada que defina.

- Resultados relacionados con consultas bloqueadas o con alertas por DNS Firewall Advanced, una característica de Route 53 Resolver que puede detectar consultas asociadas con amenazas avanzadas de DNS, como algoritmos de generación de dominios (DGA) y túneles DNS.

Después de habilitar Security Hub CSPM y Route 53 Resolver DNS Firewall, DNS Firewall comienza a enviar automáticamente las conclusiones de las listas de dominios AWS administradas y del firewall DNS avanzado al CSPM de Security Hub. Para enviar también al CSPM de Security Hub resultados de una lista de dominios personalizada, habilite manualmente la integración en el CSPM de Security Hub.

En el CSPM de Security Hub, todos los resultados de Route 53 Resolver DNS Firewall tienen el siguiente tipo: `TTPs/Impact/Impact:Runtime-MaliciousDomainRequest.Reputation`.

Para obtener más información, consulte Envío de resultados desde Route 53 Resolver DNS Firewall al CSPM de Security Hub en la Guía para desarrolladores de Amazon Route 53.

AWS Systems Manager Administrador de parches (envía los hallazgos)

AWS Systems Manager El administrador de parches envía las conclusiones al CSPM de Security Hub cuando las instancias de la flota de un cliente no cumplen con su estándar de cumplimiento de parches.

Patch Manager automatiza el proceso de aplicación de parches a instancias administradas con actualizaciones relacionadas con la seguridad y otros tipos de actualizaciones.

Después de habilitar el CSPM de Security Hub, esta integración se activa automáticamente. El Administrador de parches de Systems Manager comienza inmediatamente a enviar resultados al CSPM de Security Hub.

Para obtener más información acerca de cómo utilizar Patch Manager, consulte AWS Systems Manager Patch Manager en la Guía del usuario de AWS Systems Manager .

AWS servicios que reciben las conclusiones del CSPM de Security Hub

Los siguientes AWS servicios están integrados con Security Hub CSPM y reciben las conclusiones de Security Hub CSPM. Cuando se indique lo contrario, el servicio integrado también puede actualizar resultados. En este caso, las actualizaciones de resultados que realice en el servicio integrado también se reflejarán en el CSPM de Security Hub.

AWS Audit Manager (Recibe los hallazgos)

AWS Audit Manager recibe las conclusiones del CSPM de Security Hub. Estos resultados ayudan a los usuarios de Audit Manager a prepararse para las auditorías.

Para obtener más información sobre Audit Manager, consulte la guía del usuario de AWS Audit Manager. AWS Las comprobaciones del CSPM de Security Hub compatibles con AWS Audit Manager enumeran los controles para los cuales el CSPM de Security Hub envía resultados a Audit Manager.

Amazon Q Developer en aplicaciones de chat (recibe resultados)

Amazon Q Developer en aplicaciones de chat es un agente interactivo que ayuda a supervisar e interactuar con los recursos de AWS en los canales de Slack y salas de chat de Amazon Chime.

Amazon Q Developer en aplicaciones de chat recibe resultados del CSPM de Security Hub.

Para obtener más información sobre la integración de Amazon Q Developer en aplicaciones de chat con el CSPM de Security Hub, consulte la Descripción general de la integración con el CSPM de Security Hub en la Guía del administrador de Amazon Q Developer en aplicaciones de chat.

Amazon Detective (Recibe resultados)

Detective recopila automáticamente los datos de registro de sus AWS recursos y utiliza el aprendizaje automático, el análisis estadístico y la teoría de grafos para ayudarle a visualizar y llevar a cabo investigaciones de seguridad de forma más rápida y eficiente.

La integración de Security Hub CSPM con Detective le permite pasar de los GuardDuty hallazgos de Amazon en Security Hub CSPM a Detective. A continuación, puede utilizar las herramientas y visualizaciones de Detective para investigarlos. Esta integración no requiere ninguna configuración adicional en el CSPM de Security Hub ni en Detective.

En el caso de los hallazgos recibidos de otras personas Servicios de AWS, el panel de detalles de la consola CSPM de Security Hub incluye la subsección Investigate in Detective. Esa subsección contiene un enlace a Detective, donde puede investigar más a fondo el problema de seguridad que indicó el resultado. También puede crear un gráfico de comportamiento en Detective basado en resultados del CSPM de Security Hub para realizar investigaciones más eficaces. Para obtener más información, consulte Resultados de seguridad de AWS en la Guía de administración de Amazon Detective.

Si la agregación entre regiones está habilitada, al pasar de la región de agregación, Detective se abre en la región en la que se originó el resultado.

Si un enlace no funciona, para obtener información sobre la solución de problemas, consulte Solución de problemas del pivot.

Amazon Security Lake (Recibe resultados)

Security Lake es un servicio de lago de datos de seguridad totalmente gestionado. Puede usar Amazon Security Lake para centralizar automáticamente los datos de seguridad de fuentes en la nube, en las instalaciones y personalizadas en un lago de datos almacenado en su cuenta. Los suscriptores pueden consumir datos de Security Lake para casos de uso de investigación y análisis.

Para activar esta integración, debe habilitar ambos servicios y agregar el CSPM de Security Hub como fuente en la consola de Security Lake, la API de Security Lake o. AWS CLI Una vez que complete estos pasos, el CSPM de Security Hub empieza a enviar todos los resultados a Security Lake.

Security Lake normaliza automáticamente los resultados del CSPM de Security Hub y los convierte a un esquema de código abierto estandarizado denominado Marco de Esquema de Ciberseguridad Abierto (OCSF). En Security Lake, puede agregar uno o más suscriptores para consumir los resultados del CSPM de Security Hub.

Para obtener más información sobre esta integración, incluidas las instrucciones sobre cómo agregar el CSPM de Security Hub como fuente y crear suscriptores, consulte la sección Integración con el CSPM de AWS Security Hub en la guía del usuario de Amazon Security Lake.

AWS Systems Manager Explorer y OpsCenter (recibe y actualiza los hallazgos)

AWS Systems Manager Explore y OpsCenter reciba los hallazgos de Security Hub CSPM y actualícelos en Security Hub CSPM.

Explorer le proporciona un panel personalizable con información y análisis clave sobre el estado y el rendimiento operativos de su entorno de AWS .

OpsCenter le proporciona una ubicación central para ver, investigar y resolver los elementos de trabajo operativos.

Para obtener más información sobre Explorer y OpsCenter, consulte Administración de operaciones en la Guía del AWS Systems Manager usuario.

AWS Trusted Advisor (Recibe los hallazgos)

Trusted Advisor se basa en las mejores prácticas aprendidas al atender a cientos de miles de AWS clientes. Trusted Advisor inspecciona su AWS entorno y, a continuación, hace recomendaciones

cuando existen oportunidades para ahorrar dinero, mejorar la disponibilidad y el rendimiento del sistema o ayudar a cerrar las brechas de seguridad.

Al habilitar tanto Trusted Advisor el CSPM como Security Hub, la integración se actualiza automáticamente.

El CSPM de Security Hub envía los resultados de sus comprobaciones de las mejores prácticas de seguridad AWS fundamentales a. Trusted Advisor

Para obtener más información sobre la integración de Security Hub con CSPM Trusted Advisor, consulte Visualización de los controles de CSPM de AWS Security Hub en la Guía del usuario de soporte. AWS Trusted Advisor AWS

Third-party integraciones de productos con Security Hub CSPM

AWS Security Hub CSPM se integra con varios productos de socios externos. Una integración puede realizar una o más de las acciones siguientes:

- Enviar resultados que genera al CSPM de Security Hub
- Recibir resultados del CSPM de Security Hub
- Actualizar resultados en el CSPM de Security Hub

Las integraciones que envían resultados al CSPM de Security Hub tienen un nombre de recurso de Amazon (ARN).

Es posible que una integración no esté disponible en todos los casos. Regiones de AWS Si una integración no es compatible en la región en la que inició sesión en la consola del CSPM de Security Hub, dicha integración no aparece en la página Integraciones de la consola. Para obtener una lista de las integraciones disponibles en las regiones de China AWS GovCloud (US) Regions, consulteDisponibilidad de las integraciones por región.

Si tiene una solución de seguridad y está interesado en convertirse en socio del CSPM de Security Hub, envíe un correo electrónico a `<securityhub-partners@amazon.com>`. Para obtener más información, consulte la Guía de integración para socios.

Descripción general de las integraciones de terceros con el CSPM de Security Hub

La siguiente tabla ofrece una descripción general de las integraciones de terceros que pueden enviar resultados al CSPM de Security Hub o recibir resultados del CSPM de Security Hub.

Integración	Dirección	ARN (si corresponde)
3CORESec – 3CORESec NTA	Envía resultados	arn:aws:securityhub: <REGION>::product/3coresec/3coresec
Alert Logic – SIEMless Threat Management	Envía resultados	arn:aws:securityhub: <REGION>:733251395267:product/alertlogic/althreatmanagement
Aqua Security – Aqua Cloud Native Security Platform	Envía resultados	arn:aws:securityhub: <REGION>::product/aquasecurity/aquasecurity
Aqua Security – Kube-bench	Envía resultados	arn:aws:securityhub: <REGION>::product/aqua-security/kube-bench
Armor – Armor Anywhere	Envía resultados	arn:aws:securityhub: <REGION>:679703615338:product/armordefense/armoranywhere
AttackIQ – AttackIQ	Envía resultados	arn:aws:securityhub: <REGION>::product/attackiq/attackiq-platform
Barracuda Networks – Cloud Security Guardian	Envía resultados	arn:aws:securityhub: <REGION>:151784055945:product/barra

Integración	Dirección	ARN (si corresponde)
		cuda/cloudsecurity guardian
BigID – BigID Enterprise	Envía resultados	arn:aws:securityhub: <REGION>::product/bigid/bigid-enterprise
Blue Hexagon – Blue Hexagon forAWS	Envía resultados	arn:aws:securityhub: <REGION>::product/blue-hexagon/blue-hexagon-for-aws
Check Point – CloudGuard IaaS	Envía resultados	arn:aws:securityhub: <REGION>:758245563457:product/checkpoint/cloudguard-iaas
Check Point – CloudGuard Posture Management	Envía resultados	arn:aws:securityhub: <REGION>:634729597623:product/checkpoint/dome9-arc
Claroty – xDome	Envía resultados	arn:aws:securityhub: <REGION>::product/claroty/xdome
Cloud Storage Security – Antivirus for Amazon S3	Envía resultados	arn:aws:securityhub: <REGION>::product/cloud-storage-security/antivirus-for-amazon-s3

Integración	Dirección	ARN (si corresponde)
Contrast Security	Envía resultados	`arn:aws:securityhub: <REGION>::product/contrast-security/security-assess`
CrowdStrike – CrowdStrike Falcon	Envía resultados	`arn:aws:securityhub: <REGION>:517716713836:product/crowdstrike/crowdstrike-falcon`
CyberArk – Privileged Threat Analytics	Envía resultados	`arn:aws:securityhub: <REGION>:749430749651:product/cyberark/cyberark-pta`
Data Theorem – Data Theorem	Envía resultados	`arn:aws:securityhub: <REGION>::product/data-theorem/api-cloud-web-secure`
Drata	Envía resultados	`arn:aws:securityhub: <REGION>::product/drata/drata-integration`
Forcepoint – Forcepoint CASB	Envía resultados	`arn:aws:securityhub: <REGION>:365761988620:product/forcepoint/forcepoint-casb`

Integración	Dirección	ARN (si corresponde)
Forcepoint – Forcepoint Cloud Security Gateway	Envía resultados	`arn:aws:securityhub: <REGION>::product/forcepoint/forcepoint-cloud-security-gateway`
Forcepoint – Forcepoint DLP	Envía resultados	`arn:aws:securityhub: <REGION>:365761988620:product/forcepoint/forcepoint-dlp`
Forcepoint – Forcepoint NGFW	Envía resultados	`arn:aws:securityhub: <REGION>:365761988620:product/forcepoint/forcepoint-ngfw`
Fugue – Fugue	Envía resultados	`arn:aws:securityhub: <REGION>::product/fugue/fugue`
Guardicore – Centra 4.0	Envía resultados	`arn:aws:securityhub: <REGION>::product/guardicore/guardicore`
HackerOne – Vulnerability Intelligence	Envía resultados	`arn:aws:securityhub: <REGION>::product/hackerone/vulnerability-intelligence`
JFrog – Xray	Envía resultados	`arn:aws:securityhub: <REGION>::product/jfrog/jfrog-xray`

Integración	Dirección	ARN (si corresponde)
Juniper Networks – vSRX Next Generation Firewall	Envía resultados	`arn:aws:securityhub: <REGION>::product/juniper-networks/vsrx-next-generation-firewall`
k9 Security – Access Analyzer	Envía resultados	`arn:aws:securityhub: <REGION>::product/k9-security/access-analyzer`
Lacework – Lacework	Envía resultados	`arn:aws:securityhub: <REGION>::product/lacework/lacework`
McAfee – MVISION Cloud Native Application Protection Platform (CNAPP)	Envía resultados	`arn:aws:securityhub: <REGION>::product/mcafee-skyhigh/mcafee-mvision-cloud-aws`
NETSCOUT – NETSCOUT Cyber Investigator	Envía resultados	`arn:aws:securityhub:us-east-1::product/netscout/netscout-cyber-investigator`
Orca Cloud Security Platform	Envía resultados	`arn:aws:securityhub: <REGION>::product/orca-security/orca-security`

Integración	Dirección	ARN (si corresponde)
Palo Alto Networks – Prisma Cloud Compute	Envía resultados	`arn:aws:securityhub: <REGION>:496947949261:product/twistlock/twistlock-enterprise`
Palo Alto Networks – Prisma Cloud Enterprise	Envía resultados	`arn:aws:securityhub: <REGION>:188619942792:product/paloaltonetworks/redlock`
Plerion – Cloud Security Platform	Envía resultados	`arn:aws:securityhub: <REGION>::product/plerion/cloud-security-platform`
Prowler – Prowler	Envía resultados	`arn:aws:securityhub: <REGION>::product/prowler/prowler`
Qualys – Vulnerability Management	Envía resultados	`arn:aws:securityhub: <REGION>:805950163170:product/qualys/qualys-vm`
Rapid7 – InsightVM	Envía resultados	`arn:aws:securityhub: <REGION>:336818582268:product/rapid7/insightvm`
SentinelOne – SentinelOne	Envía resultados	`arn:aws:securityhub: <REGION>::product/sentinelone/endpoint-protection`

Integración	Dirección	ARN (si corresponde)
Snyk	Envía resultados	`arn:aws:securityhub: <region>::product/snyk/snyk`
Sonrai Security – Sonrai Dig	Envía resultados	`arn:aws:securityhub: <REGION>::product/sonrai-security/sonrai-dig`
Sophos – Server Protection	Envía resultados	`arn:aws:securityhub: <REGION>:062897671886:product/sophos/sophos-server-protection`
StackRox – StackRox Kubernetes Security	Envía resultados	`arn:aws:securityhub: <REGION>::product/stackrox/kubernetes-security`
Sumo Logic – Machine Data Analytics	Envía resultados	`arn:aws:securityhub: <REGION>:956882708938:product/sumologicinc/sumologic-mda`
Symantec – Cloud Workload Protection	Envía resultados	`arn:aws:securityhub: <REGION>:754237914691:product/symantec-corp/symantec-cwp`
Tenable – Tenable.io	Envía resultados	`arn:aws:securityhub: <REGION>:422820575223:product/tenable/tenable-io`

Integración	Dirección	ARN (si corresponde)
Trend Micro – Cloud One	Envía resultados	`arn:aws:securityhub: <REGION>::product/trend-micro/cloud-one`
Vectra – Cognito Detect	Envía resultados	`arn:aws:securityhub: <REGION>:978576646331:product/vectra-ai/cognito-detect`
Wiz	Envía resultados	`arn:aws:securityhub: <REGION>::product/wiz-security/wiz-security`
Atlassian - Jira Service Management	Recibe y actualiza resultados	No aplicable
Atlassian - Jira Service Management Cloud	Recibe y actualiza resultados	No aplicable
Atlassian – Opsgenie	Recibe resultados	No aplicable
Dynatrace	Recibe resultados	No aplicable
Elastic	Recibe resultados	No aplicable
Fortinet – FortiCNP	Recibe resultados	No aplicable
IBM – QRadar	Recibe resultados	No aplicable
Logz.io Cloud SIEM	Recibe resultados	No aplicable
MetricStream	Recibe resultados	No aplicable
MicroFocus – MicroFocus Arcsight	Recibe resultados	No aplicable

Integración	Dirección	ARN (si corresponde)
New Relic Vulnerability Management	Recibe resultados	No aplicable
PagerDuty – PagerDuty	Recibe resultados	No aplicable
Palo Alto Networks – Cortex XSOAR	Recibe resultados	No aplicable
Palo Alto Networks – VM-Series	Recibe resultados	No aplicable
Rackspace Technology – Cloud Native Security	Recibe resultados	No aplicable
Rapid7 – InsightConnect	Recibe resultados	No aplicable
RSA – RSA Archer	Recibe resultados	No aplicable
ServiceNow – ITSM	Recibe y actualiza resultados	No aplicable
Slack – Slack	Recibe resultados	No aplicable
Splunk – Splunk Enterprise	Recibe resultados	No aplicable
Splunk – Splunk Phantom	Recibe resultados	No aplicable
ThreatModeler	Recibe resultados	No aplicable
Trellix – Trellix Helix	Recibe resultados	No aplicable
Caveonix – Caveonix Cloud	Envía y recibe resultados	`arn:aws:securityhub: <REGION>::product/caveonix/caveonix-cloud`

Integración	Dirección	ARN (si corresponde)
Cloud Custodian – Cloud Custodian	Envía y recibe resultados	`arn:aws:securityhub: <REGION>::product/cloud-custodian/cloud-custodian`
DisruptOps, Inc. – DisruptOPS	Envía y recibe resultados	`arn:aws:securityhub: <REGION>::product/disruptops-inc/disruptops`
Kion	Envía y recibe resultados	`arn:aws:securityhub: <REGION>::product/cloudtamerio/cloudtamerio`
Turbot – Turbot	Envía y recibe resultados	`arn:aws:securityhub: <REGION>:453761072151:product/turbot/turbot`

Third-party integraciones que envían los resultados a Security Hub (CSPM).

Las siguientes integraciones de productos de socios externos pueden enviar resultados al CSPM de Security Hub. El CSPM de Security Hub transforma los resultados al formato de resultados de seguridad de AWS.

3 CoreSec – 3 núcleos Sec NTA

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>::product/3coresec/3coresec`

3CORESec proporciona servicios de detección gestionados tanto para sistemas en las instalaciones como de AWS . Su integración con el CSPM de Security Hub ofrece visibilidad sobre amenazas como malware, escalamiento de privilegios, movimiento lateral y segmentación incorrecta de la red.

Enlace al producto

Documentación de socios

Alert Logic – Gestión de amenazas sin interrupciones

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>:733251395267:product/alertlogic/althreatmanagement`

Obtenga el nivel de cobertura adecuado: visibilidad de las vulnerabilidades y los activos, detección de amenazas y gestión de incidentes AWS WAF, y opciones asignadas a los analistas de SOC.

Enlace al producto

Documentación de socios

Aqua Security – Plataforma de seguridad nativa de Aqua Cloud

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>::product/aquasecurity/aquasecurity`

Aqua Cloud Native Security Platform (CSP)proporciona una seguridad total durante todo el ciclo de vida de las aplicaciones basadas en contenedores y sin servidor, desde los entornos de producción en fase de ejecución hasta los entornos de CI/CD producción en ejecución.

Enlace al producto

Documentación de socios

Aqua Security – Kube-bench

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>::product/aqua-security/kube-bench`

Kube-bench es una herramienta de código abierto que ejecuta el Punto de referencia de Kubernetes del Center for Internet Security (Centro para la seguridad de Internet, CIS) con respecto a su entorno.

Enlace al producto

Documentación de socios

Armor – Armor Anywhere

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>:679703615338:product/armordefense/armoranywhere`

Armor Anywhereofrece seguridad y cumplimiento gestionados para. AWS

Enlace al producto

Documentación de socios

AttackIQ – AttackIQ

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>::product/attackiq/attackiq-platform`

AttackIQ Platform emula un comportamiento adverso real conforme al marco MITRE ATT&CK para ayudarle a validar y mejorar su posición general de seguridad.

Enlace al producto

Documentación de socios

Barracuda Networks – Cloud Security Guardian

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>:151784055945:product/barracuda/cloudsecurityguardian`

Barracuda Cloud Security Sentry ayuda a las organizaciones a mantener la seguridad al desarrollar aplicaciones y migrar cargas de trabajo hacia o desde la nube pública.

AWS Enlace a Marketplace

Enlace al producto

BigID – BigID Enterprise

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>::product/bigid/bigid-enterprise`

La BigID Enterprise Privacy Management Platform ayuda a las empresas a gestionar y proteger sus datos confidenciales (PII) en todos sus sistemas.

Enlace al producto

Documentación de socios

Hexágono azul – Hexágono azul for AWS

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>::product/blue-hexagon/blue-hexagon-for-aws`

Blue Hexagon es una plataforma de detección de amenazas en tiempo real. Utiliza principios de aprendizaje profundo para detectar amenazas conocidas y desconocidas, como malware y anomalías en la red.

AWS Enlace a Marketplace

Documentación de socios

Check Point – CloudGuard IaaS

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>:758245563457:product/checkpoint/cloudguard-iaas`

Check Point CloudGuardAmplía fácilmente la seguridad integral de prevención de amenazas y, al AWS mismo tiempo, protege los activos en la nube.

Enlace al producto

Documentación de socios

Check Point – CloudGuard Gestión de la postura

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>:634729597623:product/checkpoint/dome9-arc`

Una plataforma SaaS que ofrece seguridad de la red en la nube verificable, protección de IAM avanzada y gobernanza y conformidad integrales.

Enlace al producto

Documentación de socios

Claridad – Cúpula

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>::product/claroty/xdome`

Claroty xDome ayuda a las organizaciones a proteger sus sistemas ciberfísicos a través de la Internet de las cosas ampliada (Extended Internet of Things, XIoT) en entornos industriales (OT), sanitarios (IoMT) y empresariales (IoT).

Enlace al producto

Documentación de socios

Cloud Storage Security – Antivirus para Amazon S3

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>::product/cloud-storage-security/antivirus-for-amazon-s3`

Cloud Storage Security proporciona análisis antivirus y antimalware nativos en la nube para objetos de Amazon S3.

Antivirus for Amazon S3 ofrece escaneos programados y en tiempo real de objetos y archivos en Amazon S3 para detectar malware y amenazas. Proporciona visibilidad y solución a los problemas y a los archivos infectados.

Enlace al producto

Documentación de socios

Contrast Security: Contrast Assess

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>::product/contrast-security/security-assess`

Contrast Security Contrast Assess es una herramienta IAST que ofrece detección de vulnerabilidades en tiempo real en aplicaciones web, API y microservicios. Contrast Assess se integra con el CSPM de Security Hub para ayudar a proporcionar visibilidad y respuesta centralizadas para todas las cargas de trabajo.

Enlace al producto

Documentación de socios

CrowdStrike – CrowdStrike Halcón

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>:517716713836:product/crowdstrike/crowdstrike-falcon`

El sensor CrowdStrike Falcon único y ligero unifica los antivirus de próxima generación, la detección y la respuesta de terminales y la búsqueda 24/7 gestionada en la nube.

AWS Enlace a Marketplace

Documentación de socios

CyberArk – Privileged Threat Analytics

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>:749430749651:product/cyberark/cyberark-pta`

Privileged Threat Analytics recopila, detecta, alerta y responde a actividades y comportamiento de alto riesgo de las cuentas privilegiadas que podrían tener ataques en curso.

Enlace al producto

Documentación de socios

Teorema de los datos – Teorema de datos

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>::product/data-theorem/api-cloud-web-secure`

Data TheoremAnaliza continuamente las aplicaciones web, las API y los recursos de la nube en busca de fallas de seguridad y brechas de privacidad de los datos para evitar violaciones de AppSec datos.

Enlace al producto

Documentación de socios

Datos

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>::product/drata/drata-integration`

Drata es una plataforma de automatización de la conformidad que le ayuda a lograr y mantener a cumplir con diversos marcos de referencia, como SOC2, ISO y RGPD. La integración entre Drata y el CSPM de Security Hub ayuda a centralizar los resultados de seguridad en un solo lugar.

AWS Enlace a Marketplace

Documentación de socios

Forcepoint – Forcepoint CASB

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-casb`

Forcepoint CASB le permite detectar el uso de aplicaciones en la nube, analizar riesgos y aplicar controles adecuados para SaaS y aplicaciones personalizadas.

Enlace al producto

Documentación de socios

Forcepoint – Pasarela de seguridad en la nube de Forcepoint

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>::product/forcepoint/forcepoint-cloud-security-gateway`

Forcepoint Cloud Security Gateway es un servicio de seguridad en la nube convergente que proporciona visibilidad, control y protección contra amenazas a los usuarios y los datos, estén donde estén.

Enlace al producto

Documentación de socios

Forcepoint – Forcepoint DLP

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-dlp`

Forcepoint DLP aborda el riesgo centrado en el ser humano con visibilidad y control dondequiera que los empleados trabajen y donde residan los datos.

Enlace al producto

Documentación de socios

Forcepoint – Forcepoint NGFW

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-ngfw`

Forcepoint NGFWle permite conectar su AWS entorno a la red empresarial con la escalabilidad, la protección y la información necesarias para administrar su red y responder a las amenazas.

Enlace al producto

Documentación de socios

Fuga – Fuga

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>::product/fugue/fugue`

Fugue es una plataforma nativa en la nube escalable y sin agentes que automatiza la validación continua de la infraestructura como código y los entornos de tiempo de ejecución en la nube mediante las mismas políticas.

Enlace al producto

Documentación de socios

Guardicore – Centra 4.0

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>::product/guardicore/guardicore`

Guardicore Centra proporciona visualización de flujo, microsegmentación y detección de interrupción para cargas de trabajo en los modernos centros de datos y nubes.

Enlace al producto

Documentación de socios

HackerOne – Inteligencia de vulnerabilidades

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>::product/hackerone/vulnerability-intelligence`

La plataforma HackerOne se asocia con la comunidad mundial de hackers para descubrir los problemas de seguridad más relevantes. Vulnerability Intelligencepermite a su organización ir más allá del escaneo automatizado. Comparte vulnerabilidades que los piratas informáticos éticos de HackerOne han validado y proporciona medidas para reproducirlas.

AWS enlace al mercado

Documentación de socios

JFrog – Radiografía

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>::product/jfrog/jfrog-xray`

JFrog Xray es una herramienta universal de análisis de la composición de software (Software Composition Analysis, SCA) para la seguridad de aplicaciones que escanea continuamente los archivos binarios para comprobar si cumplen con las licencias y si presentan vulnerabilidades de seguridad para que pueda ejecutar una cadena de suministro de software segura.

AWS Enlace a Marketplace

Documentación de socios

Juniper Networks – Firewall de próxima generación vSRX

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>::product/juniper-networks/vsrx-next-generation-firewall`

Juniper Networks'El firewall virtual de próxima generación de vSRX ofrece un firewall virtual completo basado en la nube con seguridad avanzada, redes sólidas SD-WAN y seguras y automatización integrada.

AWS Enlace a Marketplace

Documentación de socios

Enlace al producto

Seguridad k9 – Analizador de acceso

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>::product/k9-security/access-analyzer`

k9 Security le notifica cuando se producen cambios de acceso importantes en su cuenta de AWS Identity and Access Management . Con élk9 Security, puede comprender el acceso que tienen los usuarios y las funciones de IAM a los datos críticos Servicios de AWS y a sus datos.

k9 Security está diseñado para ofrecer servicios continuos, lo que le permite poner IAM en funcionamiento con auditorías de acceso prácticas y la automatización sencilla de políticas para AWS CDK y Terraform.

Enlace al producto

Documentación de socios

Encajes – Encajes

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>::product/lacework/lacework`

Lacework es la plataforma de seguridad basada en datos para la nube. La plataforma de seguridad en la nube Lacework automatiza la seguridad en la nube a escala para que pueda innovar con rapidez y seguridad.

Enlace al producto

Documentación de socios

McAfee – Plataforma de protección de aplicaciones nativas en la nube (CNAPP) de MVISION

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>::product/mcafee-skyhigh/mcafee-mvision-cloud-aws`

McAfee MVISION Cloud Native Application Protection Platform (CNAPP)ofrece la gestión de la seguridad en la nube (CSPM) y la plataforma de protección de la carga de trabajo en la nube (CWPP) para su entorno. AWS

Enlace al producto

Documentación de socios

NETSCOUT – Investigador cibernético de NETSCOUT

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>::product/netscout/netscout-cyber-investigator`

NETSCOUT Cyber Investigator es una plataforma empresarial de análisis forense, investigación de riesgos y amenazas a la red que ayuda a reducir el impacto de las ciberamenazas en las empresas.

Enlace al producto

Documentación de socios

Plataforma de seguridad en la nube Orca

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>::product/orca-security/orca-security`

Orca Cloud Security PlatformIdentifica, prioriza y soluciona los riesgos y los problemas de cumplimiento en todo su entorno de nube. Orca'sLa AI-driven plataforma, que da prioridad a los agentes, ofrece una cobertura integral para detectar vulnerabilidades, errores de configuración, movimientos laterales, riesgos de API, datos confidenciales, eventos y comportamientos anómalos e identidades demasiado permisivas.

Orca se integra con el CSPM de Security Hub para aportar telemetría profunda de seguridad en la nube al CSPM de Security Hub. Orca, mediante su tecnología SideScanning, prioriza riesgos en la infraestructura en la nube, las cargas de trabajo, las aplicaciones, los datos, las API, las identidades y más.

Enlace al producto

Documentación de socios

Palo Alto Networks – Prisma Cloud Compute

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>:496947949261:product/twistlock/twistlock-enterprise`

Prisma Cloud Compute es una plataforma de ciberseguridad nativa de la nube que protege las máquinas virtuales, los contenedores y las plataformas sin servidor.

Enlace al producto

Documentación de socios

Palo Alto Networks – Prisma Cloud Enterprise

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>:188619942792:product/paloaltonetworks/redlock`

Protege su AWS implementación con análisis de seguridad en la nube, detección avanzada de amenazas y supervisión del cumplimiento.

Enlace al producto

Documentación de socios

Plerion – Plataforma de seguridad en la nube

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>::product/plerion/cloud-security-platform`

Plerion es una plataforma de seguridad en la nube con un enfoque único orientado a las amenazas y al riesgo que ofrece medidas preventivas, de inspección y correctivas en todas sus cargas de trabajo. La integración entre Plerion y el CSPM de Security Hub permite centralizar los resultados de seguridad y tomar medidas al respecto desde un único lugar.

AWS Enlace a Marketplace

Documentación de socios

Merodeador – Merodeador

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>::product/prowler/prowler`

Prowleres una herramienta de seguridad de código abierto que permite realizar AWS comprobaciones relacionadas con las mejores prácticas de seguridad, el fortalecimiento y la supervisión continua.

Enlace al producto

Documentación de socios

Qualys – Administración de vulnerabilidades

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>:805950163170:product/qualys/qualys-vm`

Qualys Vulnerability Management (VM) escanea e identifica continuamente las vulnerabilidades, protegiendo sus activos.

Enlace al producto

Documentación de socios

Rapid7 – InsightVM

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>:336818582268:product/rapid7/insightvm`

Rapid7 InsightVM proporciona administración de vulnerabilidades para entornos modernos, lo que permite encontrar, priorizar y remediar vulnerabilidades de manera eficiente.

Enlace al producto

Documentación de socios

SentinelOne – SentinelOne

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>::product/sentinelone/endpoint-protection`

SentinelOnees una plataforma autónoma de detección y respuesta ampliadas (XDR) que abarca la AI-powered prevención, la detección, la respuesta y la búsqueda en puntos finales, contenedores, cargas de trabajo en la nube y dispositivos de IoT.

AWS Enlace a Marketplace

Enlace al producto

Snyk

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>::product/snyk/snyk`

Snyk proporciona una plataforma de seguridad que analiza componentes de aplicaciones para detectar riesgos de seguridad en las cargas de trabajo que se estén ejecutando en AWS. Estos riesgos se envían al CSPM de Security Hub como resultados, lo que ayuda a los desarrolladores y a los equipos de seguridad a visualizarlos y priorizarlos junto con el resto de sus resultados de seguridad de AWS .

AWS Enlace a Marketplace

Documentación de socios

Sonrai Security – Sonrai Dig

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>::product/sonrai-security/sonrai-dig`

Sonrai Dig supervisa y corrige las configuraciones incorrectas de la nube y las infracciones de las políticas para que pueda mejorar su posición de seguridad y conformidad.

Enlace al producto

Documentación de socios

Sophos – Server Protection

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>:062897671886:product/sophos/sophos-server-protection`

Sophos Server Protection defiende las aplicaciones y los datos críticos en el núcleo de su organización, con técnicas completas de defensa en profundidad.

Enlace al producto

StackRox – StackRox Seguridad de Kubernetes

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>::product/stackrox/kubernetes-security`

StackRox ayuda a las empresas a proteger sus implementaciones de contenedores y Kubernetes a escala al aplicar sus políticas de conformidad y seguridad a lo largo de todo el ciclo de vida de los contenedores: creación, implementación y ejecución.

Enlace al producto

Documentación de socios

Sumo Logic – Machine Data Analytics

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>:956882708938:product/sumologicinc/sumologic-mda`

Sumo Logic es una segura plataforma de análisis de datos de las máquinas que permite a los equipos de operaciones de crear, ejecutar y proteger sus aplicaciones de AWS .

Enlace al producto

Documentación de socios

Symantec – Cloud Workload Protection

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>:754237914691:product/symantec-corp/symantec-cwp`

Cloud Workload Protection ofrece protección completa para las instancias Amazon EC2 con antimalware, prevención de intrusiones y monitorización de la integridad de los archivos.

Enlace al producto

Documentación de socios

Tenable – Tenable.io

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>:422820575223:product/tenable/tenable-io`

Puede identificar, investigar y priorizar las vulnerabilidades con precisión. Administrado en la nube.

Enlace al producto

Documentación de socios

Trend Micro – Cloud One

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>::product/trend-micro/cloud-one`

Trend Micro Cloud One proporciona la información de seguridad correcta a los equipos en el momento y lugar correctos. Esta integración envía las conclusiones de seguridad a Security Hub CSPM en tiempo real, lo que mejora la visibilidad de sus AWS recursos y detalles de los Trend Micro Cloud One eventos en Security Hub CSPM.

AWS Enlace a Marketplace

Documentación de socios

Vectra – Cognito Detect

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>:978576646331:product/vectra-ai/cognito-detect`

Vectra está transformando la ciberseguridad mediante la aplicación de IA avanzada para detectar y responder a los ciberatacantes ocultos antes de que puedan robar o causar daños.

AWS Enlace a Marketplace

Documentación de socios

Wiz – Wiz Security

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>::product/wiz-security/wiz-security`

Wizanaliza continuamente las configuraciones, las vulnerabilidades, las redes, la configuración de IAM, los secretos y más de sus Cuentas de AWS usuarios y cargas de trabajo para descubrir

problemas críticos que representan un riesgo real. Integre Wiz con el CSPM de Security Hub para visualizar y responder a los problemas que Wiz detecta desde la consola del CSPM de Security Hub.

AWS Enlace a Marketplace

Documentación de socios

Third-party Integraciones que reciben los hallazgos de Security Hub CSPM

Las siguientes integraciones de productos de socios externos pueden recibir resultados del CSPM de Security Hub. Cuando se indique, el producto también podría actualizar resultados. En ese caso, las actualizaciones que realice en los resultados dentro del producto del socio también se reflejan en el CSPM de Security Hub.

Atlassian - Administración de servicios de Jira

Tipo de integración: Recibir y actualizar

El formulario Jira envía AWS Service Management Connector los resultados del CSPM de Security Hub a. Jira Jiralos problemas se crean en función de los hallazgos. Cuando se actualizan los problemas de Jira, los resultados correspondientes se actualizan en el CSPM de Security Hub.

La integración solo es compatible con Jira Server y Jira Data Center.

Para obtener una descripción general de la integración y su funcionamiento, vea el video CSPM de AWS Security Hub: integración bidireccional con Atlassian Jira Service Management.

Enlace al producto

Documentación de socios

Atlassian - Jira Service Management Cloud

Tipo de integración: Recibir y actualizar

Jira Service Management Cloud es el componente de nube de Jira Service Management.

El formulario Jira envía AWS Service Management Connector los resultados del CSPM de Security Hub a. Jira Los resultados desencadenan la creación de problemas en Jira Service Management Cloud. Cuando actualiza esos problemas en Jira Service Management Cloud, los resultados correspondientes también se actualizan en el CSPM de Security Hub.

Enlace al producto

Documentación de socios

Atlassian – Opsgenie

Tipo de integración: Recibir

Opsgenie es una moderna solución de administración de incidentes para servicios siempre en funcionamiento, que permite a los equipos de desarrollo y operaciones planear interrupciones del servicio y mantener el control durante incidentes.

La integración con el CSPM de Security Hub garantiza que los incidentes críticos de seguridad se deriven a los equipos correspondientes para su resolución inmediata.

Enlace al producto

Documentación de socios

Dynatrace

Tipo de integración: Recibir

La integración de Dynatrace con el CSPM de Security Hub ayuda a unificar, visualizar y automatizar los resultados de seguridad de distintas herramientas y entornos. Añadir el contexto del Dynatrace tiempo de ejecución a las conclusiones de seguridad permite establecer prioridades de forma más inteligente, ayuda a reducir el ruido generado por las alertas y permite que sus DevSecOps equipos se centren en solucionar de manera eficiente los problemas críticos que afectan a sus aplicaciones y entornos de producción.

Enlace al producto

Documentación de socios

Elastic

Tipo de integración: Recibir

Elastic crea soluciones impulsadas por búsqueda para seguridad, observabilidad y búsquedas. Con la integración con el CSPM de Security Hub, Elastic ingiere mediante programación los resultados y productos de información que provienen del CSPM de Security Hub, los normaliza para establecer correlaciones y realizar análisis, y presenta paneles y detecciones unificadas en Elastic Security, lo que permite una clasificación y una investigación más rápidas sin necesidad de implementar agentes.

Enlace al producto

Documentación de socios

Fortinet – Para TICNP

Tipo de integración: Recibir

FortiCNP es un producto de protección nativo en la nube que agrupa los resultados de seguridad en información procesable y prioriza la información de seguridad en función de la puntuación de riesgo para reducir la fatiga de alertas y acelerar la corrección.

Enlace a AWS Marketplace

Documentación de socios

IBM – QRadar

Tipo de integración: Recibir

IBM QRadar de SIEM proporciona a los equipos de seguridad una forma rápida y precisa de detectar, priorizar, investigar y responder a las amenazas.

Enlace al producto

Documentación de socios

Logz.io SIEM en la nube

Tipo de integración: Recibir

Logz.io es un proveedor de Cloud SIEM que proporciona una correlación avanzada de los datos de registro y eventos para ayudar a los equipos de seguridad a detectar, analizar y responder a las amenazas de seguridad en tiempo real.

Enlace al producto

Documentación de socios

MetricStream – CyberGRC

Tipo de integración: Recibir

MetricStream CyberGRC le ayuda a gestionar, medir y mitigar los riesgos de ciberseguridad. Al recibir resultados del CSPM de Security Hub, CyberGRC ofrece mayor visibilidad sobre estos riesgos, lo que permite priorizar inversiones en ciberseguridad y cumplir con las políticas de TI.

AWS Enlace a Marketplace

Enlace al producto

MicroFocus – MicroFocus Arcsight

Tipo de integración: Recibir

ArcSight acelera la detección y la respuesta efectivas a las amenazas en tiempo real, integrando la correlación de eventos y los análisis supervisados y no supervisados con la automatización y la orquestación de las respuestas.

Enlace al producto

Documentación de socios

Administración de vulnerabilidades de New Relic

Tipo de integración: Recibir

New Relic Vulnerability Management recibe resultados de seguridad del CSPM de Security Hub, lo que permite contar con una vista centralizada de la seguridad junto con la telemetría de rendimiento, todo en el contexto completo de la pila.

AWS Enlace a Marketplace

Documentación de socios

PagerDuty – PagerDuty

Tipo de integración: Recibir

La plataforma de administración de operaciones digitales PagerDuty permite a los equipos mitigar proactivamente los problemas que afectan a los clientes, dirigiendo automáticamente cualquier señal a las acciones e información adecuadas.

AWS los usuarios pueden usar el PagerDuty conjunto de AWS integraciones para escalar sus entornos AWS e híbridos con confianza.

Al combinarse con las alertas de seguridad que el CSPM de Security Hub agrupa y organiza, PagerDuty permite automatizar la respuesta ante amenazas y configurar rápidamente acciones personalizadas para evitar problemas potenciales.

Los usuarios de PagerDuty que llevan a cabo un proyecto de migración a la nube pueden moverlo rápidamente, a la vez que se disminuye el impacto de los problemas que se producen durante todo el ciclo de vida de la migración.

Enlace al producto

Documentación de socios

Palo Alto Networks – Cortex SOAR

Tipo de integración: Recibir

Cortex XSOAR es una plataforma de orquestación, automatización y respuesta de seguridad (SOAR) que se integra con toda la pila de productos de seguridad para acelerar la respuesta ante incidentes y las operaciones de seguridad.

Enlace al producto

Documentación de socios

Palo Alto Networks – VM-Series

Tipo de integración: Recibir

La integración de Palo Alto VM-Series con el CSPM de Security Hub recopila inteligencia de amenazas y la envía al firewall de nueva generación VM-Series como una actualización automática de la política de seguridad que bloquea actividad maliciosa de direcciones IP.

Enlace al producto

Documentación de socios

Tecnología Rackspace – Seguridad nativa en la nube

Tipo de integración: Recibir

Rackspace Technology ofrece servicios de seguridad administrados además de productos de seguridad nativos de AWS para el monitoreo las 24 horas del día, los 7 días de la semana, los 365 días del año por parte de Rackspace SOC, análisis avanzado y mitigación de amenazas.

Enlace al producto

Rapid7 – InsightConnect

Tipo de integración: Recibir

Rapid7 InsightConnect es una solución de automatización y orquestación de seguridad que permite a su equipo optimizar las operaciones SOC con poco o ningún código.

Enlace al producto

Documentación de socios

RSA – RSA Archer

Tipo de integración: Recibir

RSA Archer IT and Security Risk Management le permite determinar qué activos son fundamentales para su empresa, establecer y comunicar políticas y estándares de seguridad, detectar y responder a ataques, identificar y corregir deficiencias de seguridad y establecer prácticas recomendadas claras sobre gestión de riesgos de TI.

Enlace al producto

Documentación de socios

ServiceNow – ITSM

Tipo de integración: Recibir y actualizar

La integración de ServiceNow con el CSPM de Security Hub permite consultar los resultados de seguridad del servicio directamente desde ServiceNow ITSM. Puede configurar ServiceNow para crear automáticamente un incidente o problema cuando reciba un resultado del CSPM de Security Hub.

Cualquier actualización de estos incidentes y problemas genera actualizaciones en los resultados del CSPM de Security Hub.

Para obtener una descripción general de la integración y su funcionamiento, vea el video CSPM de AWS Security Hub: integración bidireccional con ServiceNow ITSM.

Enlace al producto

Documentación de socios

Slack – Slack

Tipo de integración: Recibir

Slack es una capa de la pila de tecnología empresarial que reúne personas, datos y aplicaciones. Conforma un lugar integral donde las personas pueden trabajar juntas de forma eficaz, encontrar información importante y acceder a cientos de miles de aplicaciones y servicios críticos para dar lo mejor en su trabajo.

Enlace al producto

Documentación de socios

Splunk – Splunk Enterprise

Tipo de integración: Recibir

Splunkutiliza Amazon CloudWatch Events como consumidor de las conclusiones del CSPM de Security Hub. Envíe sus datos a Splunk para un análisis de seguridad avanzado y SIEM.

Enlace al producto

Documentación de socios

Splunk – Splunk Phantom

Tipo de integración: Recibir

Con la Splunk Phantom aplicación CSPM de AWS Security Hub, las conclusiones se envían a un sitio Phantom para enriquecer el contexto de forma automatizada con información adicional sobre amenazas o para realizar acciones de respuesta automatizadas.

Enlace al producto

Documentación de socios

ThreatModeler

Tipo de integración: Recibir

ThreatModeler es una solución de modelado de amenazas automatizada que protege y amplía el ciclo de vida del desarrollo del software empresarial y la nube.

Enlace al producto

Documentación de socios

Trellix – Hélice de Trellix

Tipo de integración: Recibir

Trellix Helix es una plataforma de operaciones de seguridad alojada en la nube que permite a las organizaciones tomar el control de cualquier incidente, desde la alerta hasta la solución.

Enlace al producto

Documentación de socios

Third-party integraciones que envían y reciben hallazgos de Security Hub CSPM

Las siguientes integraciones de productos de socios externos pueden enviar resultados al CSPM de Security Hub y recibir resultados de este servicio.

Caveonix – Caveonix Cloud

Tipo de integración: Enviar y recibir

ARN del producto: `arn:aws:securityhub:<REGION>::product/caveonix/caveonix-cloud`

La Caveonix AI-powered plataforma automatiza la visibilidad, la evaluación y la mitigación en las nubes híbridas y abarca los servicios, las máquinas virtuales y los contenedores nativos de la nube. AI integrarse con AWS Security Hub CSPM, Caveonix combina AWS datos y análisis avanzados para obtener información sobre las alertas de seguridad y el cumplimiento.

AWS Enlace a Marketplace

Documentación de socios

Cloud Custodian – Cloud Custodian

Tipo de integración: Enviar y recibir

ARN del producto: `arn:aws:securityhub:<REGION>::product/cloud-custodian/cloud-custodian`

Cloud Custodian permite a los usuarios estar bien administrados en la nube. El sencillo DSL de YAML permite que unas reglas fácilmente definidas habiliten una infraestructura de nube bien administrada, segura y optimizada en costos.

Enlace al producto

Documentación de socios

DisruptOps, Inc. – DisruptOPS

Tipo de integración: Enviar y recibir

ARN del producto: `arn:aws:securityhub:<REGION>::product/disruptops-inc/disruptops`

La plataforma de operaciones de seguridad DisruptOps ayuda a las organizaciones a mantener las prácticas recomendadas de seguridad en la nube utilizando barreras de protección automatizadas.

Enlace al producto

Documentación de socios

Kion

Tipo de integración: Enviar y recibir

ARN del producto: `arn:aws:securityhub:<REGION>::product/cloudtamerio/cloudtamerio`

Kion (anteriormente cloudtamer.io) es una solución completa de gobernanza de la nube para AWS. Kion ofrece a las partes interesadas visibilidad de las operaciones en la nube y ayuda a los usuarios de la nube a gestionar cuentas, controlar el presupuesto y los costos y garantizar la conformidad continua.

Enlace al producto

Documentación de socios

Turbot – Turbot

Tipo de integración: Enviar y recibir

ARN del producto: `arn:aws:securityhub:<REGION>::product/turbot/turbot`

Turbot garantiza que la infraestructura de la nube sea segura, conforme, escalable y rentable.

Enlace al producto

Documentación de socios

Integración del CSPM de Security Hub con productos personalizados

Además de los hallazgos generados por los AWS servicios integrados y los productos de terceros, AWS Security Hub CSPM puede consumir los hallazgos generados por otros productos de seguridad personalizados.

Puede enviar estos resultados al CSPM de Security Hub mediante la operación BatchImportFindings de la API del CSPM de Security Hub. Puede usar la misma operación para actualizar resultados provenientes de productos personalizados que ya envió al CSPM de Security Hub.

Al configurar la integración personalizada, utilice las directrices y listas de verificación incluidas en la Guía de integración para socios del CSPM de Security Hub.

Requisitos y recomendaciones para las integraciones de productos personalizados

Antes de poder invocar correctamente la operación de la API `BatchImportFindings`, debe habilitar el CSPM de Security Hub.

También debe proporcionar detalles sobre los resultados del producto personalizado con el the section called “Formato de resultados: ASFF”. Revise los siguientes requisitos y recomendaciones para las integraciones de productos personalizados:

Configuración del ARN del producto

Cuando habilita el CSPM de Security Hub, se genera un nombre de recurso de Amazon (ARN) predeterminado para el CSPM de Security Hub en la cuenta actual.

Este ARN del producto tiene el siguiente formato: `arn:aws:securityhub:<region>:<account-id>:product/<account-id>/default`. Por ejemplo, `arn:aws:securityhub:us-west-2:123456789012:product/123456789012/default`.

Utilice este ARN del producto como el valor para el atributo `ProductArn` al invocar la operación de la API `BatchImportFindings`.

Configuración de los nombres de la empresa y los productos

Puede usar `BatchImportFindings` para establecer un nombre de empresa preferido y un nombre de producto preferido para la integración personalizada que envía resultados al CSPM de Security Hub.

Los nombres que especifique reemplazan el nombre de empresa y el nombre de producto preconfigurados, denominados nombre personal y nombre predeterminado, respectivamente; y aparecen en la consola del CSPM de Security Hub y en el JSON de cada resultado. Consulte BatchImportFindings para encontrar proveedores.

Configuración de los ID de resultados

Debe proporcionar, administrar e incrementar sus propios ID de resultados, utilizando el atributo `Id`.

Cada nuevo resultado debería tener un ID de resultado único. Si el producto personalizado envía varios resultados con el mismo ID de resultado, el CSPM de Security Hub procesa únicamente el primer resultado.

Establecer el ID de cuenta

Debe especificar su propio ID de cuenta, utilizando el atributo `AwsAccountId`.

Establecer las fechas creadas en y actualizadas en las fechas

Debe proporcionar sus propias marcas de tiempo para los atributos `CreatedAt` y `UpdatedAt`.

Actualización de los resultados de los productos personalizados

Además de enviar los nuevos resultados de los productos personalizados, también puede utilizar la operación de la API `BatchImportFindings` para actualizar los resultados existentes de los productos personalizados.

Para actualizar los resultados existentes, utilice el ID del resultado existente (a través del atributo `Id`). Vuelva a enviar el resultado completo con la información adecuada actualizada en la solicitud, incluida una marca de tiempo `UpdatedAt` modificada.

Integraciones personalizadas de ejemplo

Puede utilizar los siguientes ejemplos de integraciones de productos personalizados como guía para crear su propia solución personalizada:

Envío de resultados provenientes de análisis de Chef InSpec al CSPM de Security Hub

Puede crear una CloudFormation plantilla que ejecute un análisis de Chef InSpec cumplimiento y, a continuación, envíe las conclusiones al CSPM de Security Hub.

Para obtener más detalles, consulte Supervisión continua de cumplimiento con Chef InSpec y AWS en el CSPM de Security Hub.

Envío al CSPM de Security Hub de vulnerabilidades en contenedores detectadas por Trivy

Puede crear una CloudFormation plantilla que se utilice AquaSecurity Trivy para escanear los contenedores en busca de vulnerabilidades y, a continuación, enviar esos hallazgos de vulnerabilidad al CSPM de Security Hub.

Para obtener más información, consulte Cómo crear una CI/CD canalización para analizar las vulnerabilidades de los contenedores con AWS Security Hub Trivy CSPM.

Integración de Security Hub CSPM con Microsoft Azure

Para supervisar sus recursos de Microsoft Azure, puede integrar Microsoft Azure con AWS Security Hub CSPM. A continuación, Security Hub CSPM habilita automáticamente las comprobaciones de administración de postura para su entorno de Azure y genera conclusiones sobre su entorno. Más específicamente, el servicio le proporciona lo siguiente:

> **Note**
>
> Puede administrar los estándares y controles de Azure mediante la consola CSPM de Security Hub, las API y. AWS CloudFormation La función de configuración central CSPM de Security Hub no es compatible con los estándares de Azure.

- Hallazgos de ASFF: Security Hub CSPM genera hallazgos en el formato AWS Security Finding Format (ASFF) para las comprobaciones de postura que realiza para sus recursos de Azure.
- CIS Microsoft Azure Foundations Benchmark v4.0: comprobaciones de conformidad automatizadas con respecto al estándar CIS Azure v4.0. Este estándar incluye controles de identidad, redes, almacenamiento, registro y bases de datos.
- Prácticas recomendadas básicas de Azure: detección automática de errores de configuración de los recursos de Azure según las mejores prácticas de seguridad AWS seleccionadas que abarcan la seguridad de la red, la administración de identidades, la protección de datos y el registro.

- Gestión de la postura: evaluación continua de las configuraciones de los recursos de Azure comparándolas con las mejores prácticas de seguridad y los estándares de cumplimiento, con 122 controles en ambos estándares.
- Per-provider puntuaciones de seguridad: separe las puntuaciones de seguridad de Azure para AWS que pueda realizar un seguimiento de cada entorno de forma independiente.

Para crear la integración, debe conectar el entorno de Azure al Security Hub CSPM mediante el siguiente proceso:

> **Note**
>
> Los estándares de Azure se diferencian de AWS los estándares en los siguientes aspectos:
>
> - Los estándares de Azure no requieren AWS Config requisitos previos manuales. A diferencia de AWS lo que ocurre cuando CSPM-only los clientes necesitan una grabadora gestionada por el cliente, los estándares de Azure utilizan automáticamente una grabadora interna vinculada a un servicio.
> - Los estándares de Azure siempre utilizan reglas de configuración internas vinculadas a un servicio. AWS los estándares solo usan reglas de configuración vinculadas a servicios cuando Security Hub también está habilitado.

1. El entorno de Azure se configura con el registro de una aplicación, credenciales de identidad federadas, asignaciones de funciones de Azure e infraestructura de Event Hub.
2. Con la consola CSPM de Security Hub, se crea un conector para la integración. Debe especificar el ID de inquilino de Azure, el ID de cliente de la aplicación y el ámbito de supervisión.
3. AWS Config recopila datos de configuración de recursos de su entorno de Azure.

   AWS Config se usa internamente para recopilar datos de configuración de recursos. A diferencia de AWS la administración de posturas, en la que hay que habilitar AWS Config y pagar de forma explícita la grabación, la administración de posturas de Azure AWS Config se gestiona automáticamente. No necesita activarla AWS Config por separado, configurar una grabadora ni pagar por separado el AWS Config uso. Estos costes están incluidos en los precios de CSPM de Security Hub.
4. Security Hub CSPM comienza a recibir datos de configuración de recursos y eventos del registro de actividad de su entorno de Azure.

5. Security Hub CSPM genera conclusiones sobre la administración de posturas sobre su entorno de Azure.

Cómo AWS Config se utiliza

AWS Config se usa internamente para recopilar datos de configuración de recursos y detectar cambios en el entorno de Azure. El conector lo gestiona automáticamente. No es necesario activarlo AWS Config por separado, configurar una grabadora ni pagar por su AWS Config uso. Estos costos están incluidos en los precios de CSPM de Security Hub para los recursos de Azure.

Service-linked conectores y conectores administrados por el cliente

Security Hub CSPM admite dos tipos de conectores:

Service-linked conector (SLC)

Se crea automáticamente al configurar la integración de Azure en Security Hub. El alcance de un conector vinculado a un servicio siempre coincide con el alcance definido en el conector de Security Hub. No puede modificar el alcance de un conector vinculado a un servicio directamente; en su lugar, modifique el alcance en Security Hub. Security Hub gestiona el ciclo de vida de los conectores vinculados a servicios en su nombre.

Customer-managed conector (CMC)

Se crea directamente en la consola CSPM de Security Hub, en la página de integraciones. Utilice un conector gestionado por el cliente cuando desee utilizar el Security Hub (CSPM) de forma independiente del Security Hub, o cuando necesite un ámbito diferente al del conector del Security Hub. Cuando existen ambos tipos, el alcance del conector vinculado al servicio siempre debe ser igual o mayor que el alcance del conector administrado por el cliente.

> **Note**
>
> A diferencia de Security Hub, Security Hub CSPM no ofrece una selección por capacidad para los conectores de Azure. Al crear un conector en Security Hub CSPM, todas las funciones de administración de la postura se activan juntas.

Para obtener información sobre la estimación y el cálculo de los costes de la integración de Security Hub CSPM con Azure, consulte los precios de AWS Security Hub CSPM.

Temas

- Requisitos previos para integrar Security Hub CSPM con Microsoft Azure
- Configuración de Microsoft Azure para que se integre con Security Hub CSPM
- Configuración de Security Hub CSPM para que se integre con Microsoft Azure
- Eliminar un conector de Microsoft Azure en Security Hub (CSPM)

Requisitos previos para integrar Security Hub CSPM con Microsoft Azure

Antes de integrar Microsoft Azure con AWS Security Hub CSPM, complete las siguientes tareas en su entorno AWS y en el de Azure. Esto ayuda a garantizar que tanto usted como Security Hub CSPM dispongan de los recursos y permisos que necesitan para supervisar los recursos de Azure.

Temas

- Requisitos previos para AWS
- Requisitos previos para Microsoft Azure

Requisitos previos para AWS

Compruebe que tiene lo siguiente en su Cuenta de AWS:

AWS Security Hub (CSPM) activado

El CSPM de Security Hub debe estar habilitado en el conector Cuenta de AWS y en el Región de AWS lugar en el que desee crearlo.

Permisos de IAM de la consola

El principal de IAM que crea el conector debe tener los siguientes permisos:

- `config:GetConnector`
- `config:ListConnectors`
- `config:PutConnector`

La federación de identidades salientes de IAM está habilitada

Debe habilitar la federación de identidades salientes de IAM en su. Cuenta de AWS Esta función permite a AWS los servicios autenticarse ante proveedores de identidad externos (como Microsoft Entra ID) mediante credenciales federadas en lugar de secretos de larga duración.

Tras habilitar la federación de identidades salientes, anote la URL del emisor del token. Esta URL tiene el siguiente formato:

```
https://uuid.tokens.sts.global.api.aws
```

Necesitará esta URL al configurar las credenciales de identidad federadas en Azure.

Requisitos previos para Microsoft Azure

Compruebe que dispone de lo siguiente en su entorno de Azure:

Inquilino de Azure

Debe tener un inquilino de Azure en la nube comercial de Azure. No se admiten Azure Government ni Azure China.

Disponibilidad del registro de Microsoft Entra ID

El registro de recursos requiere registros de auditoría e inicio de sesión de Microsoft Graph de su inquilino de Microsoft Entra ID. Algunos registros de Microsoft Entra ID requieren una licencia de Microsoft Entra ID P1 o P2.

Si el arrendatario carece de los registros necesarios, el registro de recursos podría informar de errores parciales. El registro de la aplicación y las asignaciones de funciones de Azure no proporcionan los datos de registro faltantes.

Función de administrador global

La persona que configura el entorno de Azure debe tener el rol de administrador global en Microsoft Entra ID. Esta función es necesaria para registrar las solicitudes, conceder el consentimiento del administrador para los permisos de la API de Microsoft Graph, asignar funciones de RBAC en el ámbito del grupo de administración raíz de inquilinos y configurar los ajustes de diagnóstico de los registros de auditoría de Entra ID.

> **Note**
>
> En muchas organizaciones, el administrador global de Azure y el administrador de AWS seguridad son personas distintas. La configuración de Azure se puede completar de forma independiente mediante el script de configuración generado.

Registro de la aplicación Azure

Debe registrar una aplicación en Microsoft Entra ID. Esta aplicación sirve como identidad que se AWS utiliza para autenticarse en su entorno de Azure mediante credenciales federadas. No se requieren secretos de cliente.

Azure Event Hub

Debe crear un espacio de nombres y una instancia de Event Hub de Azure para recibir los eventos Activity Log y Entra ID Audit Log. El script de configuración automatiza esta creación.

Permisos de la API de Microsoft Graph

La aplicación registrada requiere los siguientes permisos de la API de Microsoft Graph (tipo de aplicación, requiere el consentimiento del administrador):

- `Directory.Read.All`— Lea los datos del directorio, incluidos los usuarios, los grupos y los directores de servicio.
- `AuditLog.Read.All`— Lea los eventos del registro de auditoría de Entra ID.
- `Policy.Read.All`— Lea las políticas de la organización y las configuraciones de acceso condicional.

Función de lector RBAC de Azure

Al director del servicio se le debe asignar la función de lector en el ámbito del grupo de administración raíz arrendatario. Esto otorga acceso de solo lectura a todos los recursos de Azure en todas las suscripciones del inquilino.

Tras completar estas tareas, estará listo para configurar su entorno de Azure.

Configuración de Microsoft Azure para que se integre con Security Hub CSPM

Tras completar las tareas previas, puede configurar su entorno de Microsoft Azure para que admita la integración con AWS Security Hub CSPM. Para ayudarlo a hacerlo, la consola CSPM de Security Hub genera un script de configuración personalizado para su configuración.

Para generar el script, haga lo siguiente:

1. Abra la consola CSPM de Security Hub.

2. En el panel de navegación, elija Integraciones.
3. Seleccione Crear conector de Azure.
4. Complete la configuración del conector (ID de inquilino, ámbito y nombre) y, a continuación, copie el script de configuración generado.

Para ejecutar el script, utilice la CLI de Azure y autentíquese con una cuenta de administrador global (`az login`).

Al ejecutar el script, este realiza una serie de tareas. En las siguientes secciones se describe cada tarea que realiza el script. Si su organización restringe la ejecución del script, puede realizar estas tareas manualmente, utilizando este tema como guía. Después de configurar el entorno de Azure, puede configurar Security Hub CSPM para que se integre con Azure.

> **Note**
>
> El registro de una sola aplicación de Azure se comparte entre los servicios de AWS seguridad. Si también usas Security Hub o Amazon Inspector para Azure, ellos utilizarán el mismo registro de aplicaciones. No es necesario crear registros independientes para cada AWS servicio.

Tareas

- Paso 1: Registrar una aplicación de Azure
- Paso 2: Crear un principal de servicio
- Paso 3: Configurar las credenciales de identidad federadas
- Paso 4: Asignar la función de lector
- Paso 5: Configurar los permisos de la API de Microsoft Graph
- Paso 6: configurar Azure Event Hub
- Paso 7: configurar el registro de actividad y exportar el registro de auditoría de Entra ID

Paso 1: Registrar una aplicación de Azure

Registra una nueva aplicación en Microsoft Entra ID. Esta aplicación sirve como la identidad que se AWS utiliza para autenticarse en su entorno de Azure mediante credenciales federadas. No se requieren secretos de cliente.

```
$ az ad app create --display-name "AWSSecurityHubIntegration"
```

Anote el ID de la aplicación (cliente) de la salida (el `appId` atributo). Proporcionará este valor al crear el conector en la consola CSPM de Security Hub.

Paso 2: Crear un principal de servicio

Cree un principal de servicio para la aplicación registrada. Las asignaciones de roles de Azure se utilizan para conceder permisos al principal de servicio. El principal de servicio realiza acciones en su entorno de Azure.

```
$ az ad sp create --id application-client-id
```

¿Dónde *`application-client-id`* está el ID de la aplicación (cliente) del paso anterior?

Paso 3: Configurar las credenciales de identidad federadas

Configure las credenciales de identidad federadas en la aplicación para AWS permitir la autenticación sin secretos de cliente. Esto establece una confianza OIDC entre Azure y Azure. AWS No se almacenan credenciales ni secretos de larga duración.

```
$ az ad app federated-credential create \
  --id application-client-id \
  --parameters '{
    "name": "AWSConfigFederation",
    "issuer": "token-issuer-url",
    "subject": "arn:aws:iam::account-id:role/aws-service-role/
thirdparty.config.amazonaws.com/AWSServiceRoleForConfigThirdParty",
    "audiences": ["api://AzureADTokenExchange"],
    "description": "Federation for AWS Config third-party cloud resource discovery"
  }'
```

Valores clave:

- Emisor: la URL de su emisor de tokens de IAM Outbound Identity Federation. Sigue el formato. `https://uuid.tokens.sts.global.api.aws`
- Asunto: el ARN del rol `AWSServiceRoleForConfigThirdParty` vinculado al servicio en su. Cuenta de AWS AWS crea esta función vinculada a un servicio automáticamente durante la configuración del conector.

- Público: `api://AzureADTokenExchange` (valor estándar para la federación de identidades de cargas de trabajo).

Paso 4: Asignar la función de lector

Asigne la función de lector al principal de servicio en el ámbito raíz (/). Esto otorga acceso de solo lectura a todos los recursos de Azure en todas las suscripciones del inquilino.

> **Asigne Reader en el ámbito raíz**
>
> Asegúrese de asignar la función de lector al ámbito raíz (/), no al ámbito del grupo de administración raíz del inquilino. El CSPM de Security Hub lee los recursos de asignación de roles de Azure en todos los ámbitos, incluidas las asignaciones asignadas al ámbito raíz del inquilino. Una asignación de lector en el grupo de administración raíz no incluye las asignaciones cuyo ámbito sea/, por lo que, sin ella, esas lecturas fallan y se produce un error de autorización y el conector puede entrar en un estado degradado.

```
$ az role assignment create \
  --assignee application-client-id \
  --role "Reader" \
  --scope "/"
```

> **Root-scope la asignación requiere un acceso elevado**
>
> La asignación de un rol en el ámbito raíz (/) requiere un acceso elevado. Si se produce un error en la asignación de funciones, compruebe que la administración de acceso a los recursos de Azure esté configurada en Sí en Microsoft Entra ID > Propiedades. A continuación, cierra sesión y vuelve a iniciarla para actualizar el token.

> **Elimine la elevación temporal de la raíz**
>
> Al habilitar la administración del acceso para los recursos de Azure, se otorga al administrador que ha iniciado sesión la función de administrador de acceso de usuarios en el ámbito raíz (/), que puede gestionar el acceso en todos los grupos de suscripción y administración del inquilino. Una vez completada la incorporación, vuelva a configurar

la administración del acceso a los recursos de Azure como No en Microsoft Entra ID > Propiedades, guarde y cierre sesión para que esta elevación no permanezca activa.

Paso 5: Configurar los permisos de la API de Microsoft Graph

Conceda los siguientes permisos de la API Graph de Microsoft (tipo de aplicación) a la aplicación y, a continuación, conceda el consentimiento del administrador:

- `Application.Read.All`
- `AuditLog.Read.All`
- `DelegatedPermissionGrant.Read.All`
- `Device.Read.All`
- `Group.Read.All`
- `GroupMember.Read.All`
- `GroupSettings.Read.All`
- `Organization.Read.All`
- `Policy.Read.All`
- `RoleManagement.Read.Directory`
- `User.Read.All`
- `UserAuthenticationMethod.Read.All`

```
$ az ad app permission admin-consent --id application-client-id
```

Paso 6: configurar Azure Event Hub

AWS Config usa un Azure Event Hub para recibir notificaciones casi en tiempo real sobre los cambios en la configuración de los recursos en su entorno de Azure. El script de configuración crea la infraestructura de Event Hub y la etiqueta para su detección.

```
$ az group create \
  --name "aws-securityhub-integration" \
  --location event-hub-region

$ az eventhubs namespace create \
```

```
  --resource-group "aws-securityhub-integration" \
  --name "aws-securityhub-account-id" \
  --location event-hub-region \
  --sku Standard

$ az eventhubs eventhub create \
  --resource-group "aws-securityhub-integration" \
  --namespace-name "aws-securityhub-account-id" \
  --name "activitylog" \
  --message-retention 1 \
  --partition-count 4

$ az eventhubs eventhub consumer-group create \
  --resource-group "aws-securityhub-integration" \
  --namespace-name "aws-securityhub-account-id" \
  --eventhub-name "activitylog" \
  --name "AWSConfig"
```

Tras crear el Event Hub, etiquete el espacio de nombres para su detección y asigne la función de receptor de datos:

```
$ az tag create \
  --resource-id namespace-resource-id \
  --tags "AWSConfig-account-id-region=activitylog"

$ az role assignment create \
  --assignee application-client-id \
  --role "Azure Event Hubs Data Receiver" \
  --scope namespace-resource-id
```

> **Note**
>
> En el formato de etiquetaAWSConfig-*account-id*-*region*, *account-id* es tu Cuenta de AWS identificador de 12 dígitos y *region* es Región de AWS donde estás creando el conector (por ejemplo,us-east-1). Estos valores identifican quién Cuenta de AWS y qué región son los propietarios de esta integración de Event Hub.

Configuración clave:

- SKU del espacio de nombres: estándar (obligatorio para los grupos de consumidores).

- Nombre de Event Hub —`activitylog`.
- Grupo de consumidores —`AWSConfig`.
- Etiqueta: `AWSConfig-`*`account-id`*`-`*`region`* con valor`activitylog`. Esta etiqueta permite AWS Config descubrir el Event Hub automáticamente.
- Asignación de funciones: Azure Event Hubs Data Receiver en el espacio de nombres.

Paso 7: configurar el registro de actividad y exportar el registro de auditoría de Entra ID

Configure Azure para exportar los registros de actividad y los registros de auditoría de Entra ID al Event Hub.

Exportación del registro de actividad:

Configure los ajustes de diagnóstico en cada suscripción para exportar los registros de actividad al Event Hub. El script de configuración lo configura automáticamente para todas las suscripciones supervisadas. Los registros de actividad capturan la actividad a nivel de suscripción, incluidas las asignaciones de funciones y los cambios de recursos.

Exportación del registro de auditoría de Entra ID:

Configure los ajustes de diagnóstico en el Entra ID de Microsoft para exportar los registros de auditoría al mismo Event Hub. Dirígete a Microsoft Entra ID > Supervisión > Configuración de diagnóstico > Añadir configuración de diagnóstico. AuditLogsActívalos y dirígelos a tu Event Hub.

Exportación continua de Microsoft Defender for Cloud (opcional):

Para enviar las alertas de seguridad de Defender for Cloud a Security Hub CSPM, configure la exportación continua a su Event Hub. En el portal de Azure, vaya a Microsoft Defender for Cloud > Configuración del entorno > seleccione Suscripción > Exportación continua. Selecciona Event Hub como destino de exportación y elige tu espacio de nombres de Event Hub. Activa las alertas de seguridad como tipo de datos de exportación.

Configuración de eventos de datos de Amazon Inspector (opcional):

Si planea usar Amazon Inspector para el escaneo de máquinas virtuales de Azure, es necesaria una configuración adicional de eventos de datos. Para obtener más información sobre la configuración de Inspector-specific los eventos de datos, consulte la documentación de Amazon Inspector para la integración con Azure.

Configuración de Security Hub CSPM para que se integre con Microsoft Azure

Tras completar las tareas previas y configurar el entorno de Microsoft Azure, puede configurar AWS Security Hub CSPM para que se integre con Azure. Para configurar Security Hub CSPM para que se integre con Azure, debe crear un conector. Tras crear el conector, se producen los siguientes eventos:

1. Security Hub CSPM valida las credenciales de Azure y la conectividad con su entorno de Azure. Este proceso puede tardar varios minutos.
2. AWS Config comienza a descubrir y registrar los datos de configuración de sus recursos de Azure.
3. Security Hub CSPM comienza a generar hallazgos de administración de posturas para sus recursos de Azure una vez que se completa la recopilación de datos de recursos.

> **Note**
>
> Si ya creó un conector en Security Hub, se creó automáticamente un conector vinculado a un servicio en Security Hub CSPM. No necesita crear un conector independiente administrado por el cliente, a menos que necesite un ámbito diferente.

Temas

- Cree un conector de Azure
- Estándares y controles de habilitación
- Ajuste el alcance de un conector de Azure
- Compruebe el estado de un conector de Azure
- Solucione los problemas de un conector de Azure
- Cómo gestiona Security Hub CSPM los identificadores de recursos
- Controles disponibles para Azure

Cree un conector de Azure

Para crear un conector de Microsoft Azure para su entorno, complete los siguientes pasos mediante la consola CSPM de AWS Security Hub o la API.

1. Abra la consola CSPM de Security Hub.
2. En el panel de navegación, elija Integraciones.
3. Elija Crear conector de Azure.
4. Para el ID de inquilino de Azure, introduzca su identificador de inquilino de Azure Active Directory.
5. En Aplicación (ID de cliente), introduzca el ID de aplicación para el registro de la aplicación de Azure que creó.
6. Configure los ajustes adicionales y el alcance del conector de la siguiente manera:
   - En Nombre, introduzca un nombre exclusivo para el conector. El nombre puede contener hasta 50 caracteres alfanuméricos y puede incluir guiones (-).

     > **Important**
     >
     > Los nombres y las descripciones se utilizan para identificar su contenido, y le recomendamos que no incluya información sensible, confidencial o de identificación personal (PII) en ellos.

   - En Descripción, si lo desea, introduzca una breve descripción del conector. La descripción puede contener hasta 200 caracteres.
   - En Suscripciones, elija Todas las suscripciones para supervisar todas las suscripciones actuales y futuras del inquilino, o Suscripciones específicas para supervisar solo las suscripciones que especifique. Si eliges monitorear solo suscripciones específicas, ingresa el ID de cada una.
   - En el caso de las regiones, elija las regiones de Azure en las que están desplegados sus recursos.

     > **Note**
     >
     > Los controles que evalúan los recursos de Microsoft Entra ID y Microsoft Graph requieren que el ámbito de la región global se incluya en la configuración de la integración. Si selecciona únicamente regiones de Azure específicas, estos controles no generarán resultados.

7. Revise la configuración y elija Crear conector.

Tras crear el conector, Security Hub CSPM valida las credenciales de Azure e inicia la detección de recursos. El conector debería mostrar el estado Activo en un plazo de 2 a 5 minutos.

Estándares y controles de habilitación

Tras crear el conector, debe habilitar los estándares de seguridad de Azure para empezar a generar resultados. Para obtener información general sobre la activación de los estándares y la administración de los controles, consulte Habilitar los estándares y Habilitar y deshabilitar los controles.

Estándares disponibles

- CIS Microsoft Azure Foundations Benchmark v4.0: un punto de referencia de seguridad ampliamente adoptado que define las mejores prácticas para proteger los entornos de Azure. Cada control evalúa un aspecto específico de la configuración de Azure (por ejemplo, el cifrado de las cuentas de almacenamiento, las reglas de los grupos de seguridad de la red y la configuración de identidad y acceso).
- Prácticas recomendadas fundamentales de Azure: evalúa los recursos de Azure para determinar los riesgos de exposición al correlacionar la accesibilidad de la red, el acceso público y los indicadores de datos confidenciales. Genera hallazgos de tipo exposición que destacan los recursos que corren un riesgo elevado.

Los estándares de Azure tienen su propio conjunto de controles, separados de los controles. AWS No hay controles entre nubes que evalúen tanto los recursos de Azure como AWS los de Azure de una sola vez.

Habilitación de un estándar

Puede habilitar los estándares de Azure a través de la consola CSPM de Security Hub o a través de. API/CLI Navegue hasta Estándares en la consola CSPM de Security Hub y active el estándar deseado. Como alternativa, utilice la CLI:

```
$ aws securityhub batch-enable-standards \
  --standards-subscription-requests '[{"StandardsArn": "Standard-ARN"}]' \
  --region your-aws-region
```

> **Note**
>
> Puede habilitar los estándares de Azure antes o después de crear el conector; no están acoplados. Sin embargo, los resultados solo se generarán una vez que el conector y el estándar estén activos y se hayan recopilado los datos de los recursos.

Gestionar los controles individuales

Una vez que se activa un estándar (normalmente en cuestión de segundos), puede ver y gestionar los controles individuales:

- Ver controles: utilice la consola CSPM de Security Hub (Estándares > seleccione estándar > Controles) o la `list-standards-control-associations` API.
- Desactivar un control: si un control específico no es aplicable a su entorno, puede desactivarlo.
- Configurar parámetros personalizados: algunos controles aceptan parámetros de entrada personalizados (por ejemplo, los umbrales de longitud de las contraseñas). Estos se pueden configurar a través de la `update-security-control` API.

Notas importantes

- Los estándares de Azure se aplican de manera uniforme en todo el ámbito de los conectores. No puede habilitar estándares o controles diferentes para diferentes suscripciones de Azure dentro del mismo conector.
- Los controles dependen de la disponibilidad de los datos de los recursos. Cada control evalúa un tipo de recurso de Azure específico. Si aún no AWS Config ha recopilado los datos de configuración de un tipo de recurso en particular, el control generará un resultado PASS predeterminado para esos recursos. Estos resultados predeterminados del PASS se actualizarán automáticamente para convertirlos en evaluaciones precisas a medida que lleguen los datos de los recursos. No trate las puntuaciones de cumplimiento iniciales como precisas hasta que se complete la recopilación de datos sobre los recursos.
- Los parámetros de entrada personalizados para los controles de seguridad se pueden configurar incluso antes de crear un conector; se mantienen de forma independiente.
- Los controles que evalúan la configuración a nivel de suscripción (por ejemplo, planes de Microsoft Defender, alertas de registro de actividades) producen un resultado por suscripción de Azure en lugar de por recurso individual.

- Los estándares multinube no se pueden incluir en las políticas de configuración central. Debe administrar la habilitación estándar de Azure de forma independiente en cada uno y. Cuenta de AWS Región de AWS

Ajuste el alcance de un conector de Azure

Después de crear un conector de Microsoft Azure, puede ajustar el alcance del conector cambiando las suscripciones de Azure o las regiones de Azure que supervisa. Si ajusta el alcance, la mayoría de los tipos de cambios surten efecto en aproximadamente 15 minutos.

Antes de ajustar el alcance, tenga en cuenta lo siguiente:

- El alcance de un conector administrado por el cliente no puede superar el alcance de ningún conector vinculado a un servicio existente en la misma cuenta y región.
- Cuando se amplía el alcance, Security Hub CSPM comienza a generar hallazgos para nuevos recursos después de AWS Config recopilar sus datos de configuración.
- Al reducir el alcance, los hallazgos existentes sobre los recursos retirados pasan a un estado archivado.

Compruebe el estado de un conector de Azure

Puede comprobar el estado de un conector de Microsoft Azure en cualquier momento. Vaya a Integraciones en la consola CSPM de Security Hub y confirme que el conector muestre el estado Activo.

Los resultados iniciales suelen aparecer entre 15 y 30 minutos después de que se complete la recopilación de los datos de los recursos.

> **Note**
>
> Con el tiempo, el estado de funcionamiento del conector es uniforme. Cuando se produce un problema con los permisos o la configuración, el estado del conector cambia rápidamente a Degradado con un mensaje en el que se puede actuar. Sin embargo, una vez solucionado el problema, el estado puede tardar hasta 24 horas en volver a Conectado.
>
> - Un estado degradado tras una corrección reciente no indica necesariamente que se trate de un problema continuo.

- Para ver en tiempo real los errores de registro, consulta las CloudWatch métricas del espacio de nombres.

Solucione los problemas de un conector de Azure

Si tiene problemas con el conector, utilice la siguiente información para diagnosticar y resolver problemas comunes.

El estado del conector es incorrecto

Este problema suele producirse si las credenciales federadas no están configuradas correctamente en Azure.

Para solucionar este problema, compruebe que la URL del emisor del token y el ARN del asunto de sus credenciales federadas de Azure coincidan con las suyas. Cuenta de AWS

No se ha encontrado nada después de 30 minutos

Este problema puede producirse si Event Hub no recibe los registros de actividad o si no hay ningún estándar activado.

Para solucionar este problema, compruebe que el espacio de nombres de Event Hub esté etiquetado correctamente (`AWSConfig-`*`account-id`*`-`*`region`*`=activitylog`), que el grupo de `AWSConfig` consumidores exista, que la función de receptor de datos esté asignada y que al menos un estándar de Azure esté habilitado.

No se pueden registrar algunos recursos de Azure

El error puede producirse por cualquiera de los siguientes motivos:

- El entorno de Azure no cumple los requisitos previos para el registro de recursos.
- El registro de la aplicación no cuenta con el consentimiento del administrador para los permisos de la API de Microsoft Graph.
- La asignación del rol de lector no cubre todos los ámbitos requeridos.
- El arrendatario de Microsoft Entra ID no tiene los datos de registro necesarios.

Para solucionar el error, haga lo siguiente:

1. Para confirmar que su entorno cumple todos los requisitos, consulte los requisitos previos de Microsoft Azure.

2. Confirma que el registro de la aplicación tiene los permisos de la API de Microsoft Graph necesarios con el consentimiento del administrador.
3. Compruebe que el director del servicio tenga la función de lector en el ámbito del grupo de administración raíz del inquilino.

El conector permanece en estado pendiente

Este problema puede producirse si el registro de la aplicación Azure está mal configurado.

Para solucionar este problema, compruebe que la URL del emisor de la credencial de identidad federada y el identificador del asunto coincidan con los suyos. Cuenta de AWS Compruebe también que se haya otorgado el consentimiento del administrador para todos los permisos de la API de Microsoft Graph necesarios.

Cómo gestiona Security Hub CSPM los identificadores de recursos

Al habilitar la integración de Azure para AWS Security Hub CSPM, los identificadores de recursos de otros proveedores de nube se almacenarán en AWS Security AWS Config Hub CSPM y otros AWS servicios (según sea necesario) como metadatos relacionados con la administración de los datos de configuración de recursos correspondientes recopilados de los otros proveedores de nube. Dichos identificadores de recursos no constituyen su contenido y le recomendamos que no incluya en ellos información sensible, confidencial o de identificación personal.

Los siguientes identificadores de su entorno de nube conectada se almacenan y utilizan AWS para proporcionar capacidades de seguridad multinube:

- Identificadores de recursos: ID de inquilino de Azure, ID de suscripción, ubicación (región), ID de recurso (ID o nombres de grupos de recursos, proveedor de recursos, tipo de recurso)

Las relaciones entre estos identificadores, incluida la forma en que los recursos se relacionan entre sí y la forma en que los hallazgos se relacionan con los recursos, también se almacenan como metadatos de servicio. AWS utiliza estos identificadores para la correlación de recursos, asociando los hallazgos a los recursos, el registro operativo del servicio y la deduplicación.

Controles disponibles para Azure

Tras habilitar los estándares de Azure, los siguientes 122 controles evalúan los recursos de Azure. Los controles se distribuyen en dos estándares:

- CIS Microsoft Azure Foundations Benchmark v4.0: 96 controles asignados a secciones CIS específicas
- Prácticas recomendadas fundamentales de Azure: 26 controles que abarcan otras prácticas recomendadas de seguridad

> **Note**
>
> Los controles que evalúan los recursos de Microsoft Entra ID y Microsoft Graph requieren que el ámbito de la región global se incluya en la configuración de la integración.

Controles de Azure disponibles

Título de control	Tipo de recurso	Standard
Las aplicaciones de Azure Container con la identidad administrada habilitada deben tener el privilegio mínimo	`microsoft.app/containerapps`	Prácticas recomendadas fundamentales de Azure
Las aplicaciones de contenedor de Azure no deben pasar las credenciales del SDK de Azure como variables de entorno	`microsoft.app/containerapps`	Prácticas recomendadas fundamentales de Azure
Las aplicaciones de contenedores de Azure no deberían tener habilitada la entrada externa	`microsoft.app/containerapps`	Prácticas recomendadas fundamentales de Azure
Los entornos de Azure Container App no deben tener acceso ilimitado a NSG	`microsoft.app/containerapps`	Prácticas recomendadas fundamentales de Azure
Los entornos administrados por la aplicación Azure Container no deben tener habilitada la IP pública	`microsoft.app/managedenvironments`	Prácticas recomendadas fundamentales de Azure
Las asignaciones de funciones de Azure no deberían conceder un amplio acceso	`microsoft.authorization/roleassignments`	Prácticas recomendadas fundamentales de Azure

Título de control	Tipo de recurso	Standard
de administrador en el ámbito de la suscripción		
Las asignaciones de roles de Azure no deben otorgar el rol de administrador de acceso de usuario	`microsoft.authorization/roleassignments`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Las definiciones de roles personalizados de Azure no deben tener permisos administrativos comodín	`microsoft.authorization/roledefinitions`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Las asignaciones de políticas de Microsoft Cloud Security Benchmark deben tener el modo de aplicación habilitado	`microsoft.authorization/policyassignments`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Los clústeres de Azure Kubernetes Service (AKS) no deberían tener servidores de API de acceso público sin restricciones de IP	`microsoft.containerservice/managedclusters`	Prácticas recomendadas fundamentales de Azure
Los clústeres de Azure Kubernetes Service (AKS) deberían cifrar los secretos de Kubernetes en reposo	`microsoft.containerservice/managedclusters`	Prácticas recomendadas fundamentales de Azure
Los clústeres de Azure Kubernetes Service (AKS) deben ejecutar una versión de Kubernetes compatible	`microsoft.containerservice/managedclusters`	Prácticas recomendadas fundamentales de Azure
Las cuentas de Azure Cosmos DB deben tener habilitada la copia de seguridad continua	`microsoft.documentdb/databaseaccounts`	Prácticas recomendadas fundamentales de Azure

Título de control	Tipo de recurso	Standard
Los servidores flexibles de Azure Database para MySQL deben tener deshabilitado el acceso a la red pública	`microsoft.dbformysql/flexibleservers`	Prácticas recomendadas fundamentales de Azure
Los espacios de trabajo de Azure Databricks deben implementarse en una red virtual administrada por el cliente	`microsoft.databricks/workspaces`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Los espacios de trabajo de Azure Databricks deben tener configurada la entrega de registros de diagnóstico	`microsoft.databricks/workspaces`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Los espacios de trabajo de Azure Databricks deben usar claves administradas por el cliente para el cifrado de discos administrado	`microsoft.databricks/workspaces`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Las políticas de autorización de Microsoft Entra ID deberían prohibir que los usuarios predeterminados registren aplicaciones	`microsoft.graph/policies/authorizationpolicy`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
El ID de Azure Entra debe tener habilitados los valores predeterminados de seguridad	`microsoft.graph/policies/identitysecuritydefaultsenforcementpolicy`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Los inquilinos de Microsoft Entra deben tener una política de acceso condicional que bloquee el acceso desde ubicaciones geográficas no permitidas	`microsoft.graph/organization`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI

Título de control	Tipo de recurso	Standard
Los inquilinos de Microsoft Entra deben tener una política de acceso condicional que bloquee el flujo de autenticación del código del dispositivo	`microsoft.graph/organization`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Las políticas de acceso condicional de Azure deberían requerir MFA para todos los usuarios	`microsoft.graph/organization`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Los inquilinos de Microsoft Entra deberían requerir la autenticación multifactor para los inicios de sesión riesgosos mediante una política de acceso condicional	`microsoft.graph/organization`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Los inquilinos de Azure deberían requerir la MFA mediante acceso condicion al para la API de administración de servicios de Azure	`microsoft.graph/organization`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Al menos una política de acceso condicional debe requerir MFA para los portales de administración de Microsoft	`microsoft.graph/organization`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Las políticas de autorización de Microsoft Entra deberían impedir que los usuarios no administradores creen inquilinos	`microsoft.graph/policies/authorizationpolicy`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Las políticas de métodos de autentica ción de Microsoft Entra ID deben establecer el período de reconfirmación en un valor distinto de cero	`microsoft.graph/policies/authenticationmethodspolicy`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI

Título de control	Tipo de recurso	Standard
Las políticas de autorización de Microsoft Entra deberían restringir el consentimiento del usuario para las aplicaciones	`microsoft.graph/policies/authorizationpolicy`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Las políticas de autorización de Azure deberían restringir el consentimiento del usuario a las aplicaciones de editores verificados	`microsoft.graph/policies/authorizationpolicy`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Las políticas de autorización de Microsoft Entra deberían restringir el acceso de los usuarios invitados a sus propios objetos de directorio	`microsoft.graph/policies/authorizationpolicy`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Las políticas de autorización de Azure deberían restringir las invitaciones de invitados únicamente a las funciones de administrador	`microsoft.graph/policies/authorizationpolicy`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Las políticas de autorización de Azure deberían restringir la creación de grupos de seguridad a los administradores	`microsoft.graph/policies/authorizationpolicy`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Los inquilinos de Microsoft Entra deben requerir una autenticación multifactor para registrar o unir dispositivos	`microsoft.graph/organization`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Los roles del directorio Microsoft Entra ID deben tener entre 2 y 4 administradores globales	`microsoft.graph/directoryrole`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI

Título de control	Tipo de recurso	Standard
La configuración de grupos de Azure Entra ID debería restringir la creación de grupos a los administradores	`microsoft.graph/organization`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Las suscripciones a Azure deben tener una configuración de diagnóstico configurada para los registros de actividad	`microsoft.insights/diagnosticsettings`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Las suscripciones a Azure deben tener una alerta de registro de actividad para crear una asignación de políticas	`microsoft.insights/activitylogalerts`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Las suscripciones a Azure deben tener una alerta de registro de actividad para eliminar la asignación de políticas	`microsoft.insights/activitylogalerts`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Las suscripciones a Azure deben tener una alerta de registro de actividad para crear o actualizar las operaciones de un grupo de seguridad de red	`microsoft.insights/activitylogalerts`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Las suscripciones a Azure deberían tener una alerta de registro de actividad si se elimina un grupo de seguridad de red	`microsoft.insights/activitylogalerts`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Las suscripciones a Azure deben tener una alerta de registro de actividad para crear o actualizar la solución de seguridad	`microsoft.insights/activitylogalerts`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI

Título de control	Tipo de recurso	Standard
Las suscripciones a Azure deben tener una alerta de registro de actividad si se elimina la solución de seguridad	`microsoft.insights/activitylogalerts`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Las suscripciones a Azure deben tener una alerta de registro de actividad para crear o actualizar las reglas de firewall de SQL Server	`microsoft.insights/activitylogalerts`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Las suscripciones a Azure deben tener una alerta de registro de actividad para eliminar las reglas de firewall de SQL Server	`microsoft.insights/activitylogalerts`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Las suscripciones a Azure deben tener configurada una alerta de registro de actividad para las operaciones de creación o actualización de direcciones IP públicas	`microsoft.insights/activitylogalerts`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Las suscripciones a Azure deben tener una alerta de registro de actividad si se elimina una dirección IP pública	`microsoft.insights/activitylogalerts`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Las suscripciones a Azure deben tener una alerta de registro de actividad para los incidentes de Service Health	`microsoft.insights/activitylogalerts`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Las suscripciones a Azure deben tener configurado al menos un componente de Application Insights	`microsoft.insights/components`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI

Título de control	Tipo de recurso	Standard
Azure Key Vaults debería tener habilitada la protección de eliminación temporal y purga	`microsoft.keyvault/vaults`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Azure Key Vaults debería tener habilitado el control de acceso basado en roles	`microsoft.keyvault/vaults`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Los almacenes de claves de Azure deberían tener inhabilitado el acceso a la red pública cuando se utilizan puntos de conexión privados	`microsoft.keyvault/vaults`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Azure Key Vaults debe usar puntos de conexión privados	`microsoft.keyvault/vaults`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Azure Key Vaults debería tener habilitada la protección contra purgas	`microsoft.keyvault/vaults`	Prácticas recomendadas fundamentales de Azure
Azure Key Vaults debería restringir el acceso a la red	`microsoft.keyvault/vaults`	Prácticas recomendadas fundamentales de Azure
Azure Key Vaults debería tener habilitado el registro AuditEvent	`microsoft.keyvault/vaults`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI

Título de control	Tipo de recurso	Standard
Las claves de Azure Key Vault en las bóvedas RBAC deben tener una fecha de caducidad establecida	`microsoft.keyvault/vaults/keys`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Las claves de Azure Key Vault en almacenes que no sean RBAC deben tener una fecha de caducidad establecida	`microsoft.keyvault/vaults/keys`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Los secretos de Azure Key Vault guardados en RBAC-enabled las bóvedas deben tener una fecha de caducidad establecida	`microsoft.keyvault/vaults/secrets`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Los secretos de Azure Key Vault en almacenes que no sean de RBAC deben tener una fecha de caducidad establecida	`microsoft.keyvault/vaults/secrets`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Las claves de Azure Key Vault deben tener habilitada la rotación automática	`microsoft.keyvault/vaults/keys`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Los grupos de seguridad de red de Azure deberían restringir el acceso RDP entrante desde Internet	`microsoft.network/networksecuritygroups`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Los grupos de seguridad de red de Azure deberían restringir el acceso UDP entrante desde Internet	`microsoft.network/networksecuritygroups`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI

Título de control	Tipo de recurso	Standard
Los grupos de seguridad de red de Azure deberían restringir el acceso HTTP entrante desde Internet	`microsoft.network/networksecuritygroups`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Las subredes de Azure Application Gateway no deberían tener acceso ilimitado a NSG	`microsoft.network/networksecuritygroups`	Prácticas recomendadas fundamentales de Azure
Los grupos de seguridad de red de Azure deben tener una regla explícita que prohíba todo	`microsoft.network/networksecuritygroups`	Prácticas recomendadas fundamentales de Azure
Los grupos de seguridad de red de Azure no deben permitir el acceso entrante sin restricciones a puertos restringidos	`microsoft.network/networksecuritygroups`	Prácticas recomendadas fundamentales de Azure
Los registros de flujo de Azure Network Watcher deben tener habilitado el registro de flujo de red virtual y el análisis de tráfico debe enviarse a Log Analytics	`microsoft.network/networkwatchers/flowlogs`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Los grupos de seguridad de red de Azure deberían restringir el acceso a SSH desde Internet	`microsoft.network/networksecuritygroups`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Las suscripciones a Azure deben tener al menos un host de Azure Bastion	`microsoft.network/bastionhosts`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Las suscripciones a Azure deben tener habilitado Microsoft Defender para servidores	`microsoft.security/pricings`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI

Título de control	Tipo de recurso	Standard
Las máquinas deben tener una solución de evaluación de vulnerabilidades en buen estado implementada en Microsoft Defender for Cloud	`microsoft.security/assessments`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Las suscripciones a Azure deben tener habilitada la integración de protección de puntos finales con Microsoft Defender for Cloud	`microsoft.security/settings`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Las suscripciones a Azure deben tener habilitado el análisis sin agente de máquinas en Microsoft Defender for Servers	`microsoft.security/pricings`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Las suscripciones a Azure deben tener habilitada la supervisión de la integridad de los archivos en Defender for Servers	`microsoft.security/pricings`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
La suscripción a Azure debe tener habilitado Microsoft Defender for Containers	`microsoft.security/pricings`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Las suscripciones a Azure deben tener habilitado Microsoft Defender for Storage	`microsoft.security/pricings`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Las suscripciones a Azure deben tener habilitado Microsoft Defender for App Service	`microsoft.security/pricings`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI

Título de control	Tipo de recurso	Standard
Las suscripciones a Azure deben tener habilitado Microsoft Defender para Azure Cosmos DB	`microsoft.security/pricings`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Las suscripciones a Azure deben tener habilitado Microsoft Defender para bases de datos relacionales de código abierto	`microsoft.security/pricings`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Las suscripciones a Azure deben tener habilitado Microsoft Defender para bases de datos SQL de Azure	`microsoft.security/pricings`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Las suscripciones a Azure deben tener habilitado Microsoft Defender para SQL Servers on Machines	`microsoft.security/pricings`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Las suscripciones a Azure deben tener habilitado Microsoft Defender para Key Vault	`microsoft.security/pricings`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Las suscripciones a Azure deben tener habilitado Microsoft Defender for Resource Manager	`microsoft.security/pricings`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Las evaluaciones de actualización del sistema de las máquinas virtuales deben ser declaradas en buen estado por Microsoft Defender for Cloud	`microsoft.security/assessments`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI

Título de control	Tipo de recurso	Standard
Los contactos de seguridad de Microsoft Defender for Cloud deben notificar las alertas al rol de propietario	`microsoft.security/securitycontacts`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Los contactos de seguridad de Microsoft Defender for Cloud deben tener configurada una dirección de correo electrónico adicional	`microsoft.security/securitycontacts`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Los contactos de seguridad de Azure deben tener habilitadas las notificac iones de alerta por correo electrónico con una gravedad mínima suficientemente inclusiva	`microsoft.security/securitycontacts`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Los contactos de seguridad de Azure deben tener habilitadas las notificac iones por correo electrónico de la ruta de ataque con un nivel de riesgo configura do	`microsoft.security/securitycontacts`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Las suscripciones a Azure deben tener habilitado Microsoft Defender para IoT	`microsoft.security/iotsecuritysoluti ons`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Los servidores Azure SQL deberían tener deshabilitado el acceso a la red pública	`microsoft.sql/serv ers`	Prácticas recomenda das fundamentales de Azure
Los servidores SQL deben tener configurado un administrador de Azure Active Directory	`microsoft.sql/serv ers`	Prácticas recomenda das fundamentales de Azure

Título de control	Tipo de recurso	Standard
Las bases de datos SQL de Azure deben tener habilitada la copia de seguridad georedundante	`microsoft.sql/servers/databases`	Prácticas recomendadas fundamentales de Azure
Los servidores SQL de Azure no deben usar nombres de cuenta de administrador predeterminados	`microsoft.sql/servers`	Prácticas recomendadas fundamentales de Azure
Las instancias administradas de Azure SQL deberían tener habilitada la actualización automática de las versiones secundarias	`microsoft.sql/managedinstances`	Prácticas recomendadas fundamentales de Azure
Las cuentas de Azure Storage deben usar claves administradas por el cliente para el cifrado	`microsoft.storage/storageaccounts`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Los servicios de archivos de cuentas de Azure Storage deberían tener habilitada la eliminación temporal de los archivos compartidos	`microsoft.storage/storageaccounts/fileservices`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Los archivos compartidos de cuentas de Azure Storage deberían restringir las versiones del protocolo SMB a SMB 3.1.1	`microsoft.storage/storageaccounts/fileservices`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Las cuentas de Azure Storage deben usar un algoritmo de cifrado de canales SMB seguro para los archivos compartidos	`microsoft.storage/storageaccounts/fileservices`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI

Título de control	Tipo de recurso	Standard
Las cuentas de Azure Storage deberían tener configurado un recordatorio de rotación de claves	`microsoft.storage/storageaccounts`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Las cuentas de Azure Storage deberían tener deshabilitado el acceso a claves compartidas	`microsoft.storage/storageaccounts`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Las cuentas de Azure Storage deben usar puntos de conexión privados para acceder	`microsoft.storage/storageaccounts`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Las cuentas de Azure Storage deberían tener deshabilitado el acceso a la red pública	`microsoft.storage/storageaccounts`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Las cuentas de Azure Storage deberían tener el acceso a la red predeterminado configurado como denegado	`microsoft.storage/storageaccounts`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Las cuentas de almacenamiento deben tener de forma predeterminada la autorización de Microsoft Entra en el portal de Azure	`microsoft.storage/storageaccounts`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Las cuentas de Azure Storage deberían requerir una transferencia segura	`microsoft.storage/storageaccounts`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI

Título de control	Tipo de recurso	Standard
Las cuentas de almacenamiento de Azure deberían permitir que los servicios confiables de Azure eludan las reglas de red	`microsoft.storage/storageaccounts`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Las cuentas de Azure Storage deben configurarse con la versión TLS mínima requerida	`microsoft.storage/storageaccounts`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Las cuentas de Azure Storage deberían tener deshabilitada la replicación entre inquilinos	`microsoft.storage/storageaccounts`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Las cuentas de Azure Storage deberían tener deshabilitado el acceso anónimo a los blobs	`microsoft.storage/storageaccounts`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Las cuentas de Azure Storage deberían restringir la eliminación permanente de blobs	`microsoft.storage/storageaccounts/blobservices`	Prácticas recomendadas fundamentales de Azure
Las cuentas de almacenamiento de Azure que contienen registros de actividad deben cifrarse con una clave administrada por el cliente	`microsoft.storage/storageaccounts`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Los servicios de blob de cuentas de Azure Storage deberían tener habilitada la eliminación automática de blob	`microsoft.storage/storageaccounts/blobservices`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI

Título de control	Tipo de recurso	Standard
Los servicios blob de cuentas de Azure Storage deberían tener habilitado el control de versiones	`microsoft.storage/storageaccounts/blobservices`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Los servicios de blob de cuentas de Azure Storage deberían tener habilitada la eliminación temporal de blobs y contenedores	`microsoft.storage/storageaccounts/blobservices`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Las cuentas de Azure Storage deben tener aplicado un bloqueo de eliminación de Azure Resource Manager	`microsoft.storage/storageaccounts`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Las cuentas de Azure Storage deben tener un bloqueo de administrador ReadOnly de recursos	`microsoft.storage/storageaccounts`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Las cuentas de Azure Storage deben usar almacenamiento con redundancia geográfica	`microsoft.storage/storageaccounts`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI
Las aplicaciones de Azure Function deberían restringir el acceso administrativo	`microsoft.web/sites/config`	Prácticas recomendadas fundamentales de Azure
Azure Functions no debe permitir la invocación anónima de activadores HTTP	`microsoft.web/sites/functions`	Prácticas recomendadas fundamentales de Azure

Título de control	Tipo de recurso	Standard
Las aplicaciones web y las aplicacio nes funcionales de Azure App Service no deben usar versiones de tiempo de ejecución no compatibles	`microsoft.web/sites`	Prácticas recomenda das fundamentales de Azure
Las aplicaciones de Azure Function de los planes Premium o Dedicado deben integrarse en una red virtual	`microsoft.web/sites`	Prácticas recomenda das fundamentales de Azure
Las aplicaciones web de Azure App Service deben tener habilitados los registros HTTP en la configuración de diagnóstico	`microsoft.web/sites`	Punto de referencia para Microsoft Azure Foundations v4.0 de la CEI

Eliminar un conector de Microsoft Azure en Security Hub (CSPM)

Tras crear un conector de Microsoft Azure en AWS Security Hub CSPM, puede eliminarlo en cualquier momento. Si elimina un conector, Security Hub CSPM deja de realizar comprobaciones de administración de postura y supervisión de vulnerabilidades para su entorno de Azure. Security Hub CSPM también deja de generar nuevos hallazgos sobre su entorno. Sus hallazgos actuales se conservan durante 90 días. El inventario de recursos permanece como estaba cuando se eliminó el conector y se elimina después de 90 días.

Al eliminar un conector, tenga en cuenta lo siguiente:

- Security Hub CSPM no elimina el registro de aplicaciones de Azure ni la infraestructura de Event Hub en su entorno de Azure. Debe eliminarlos manualmente, directamente en Microsoft Azure. Para obtener información sobre cómo hacerlo, consulte Eliminar una aplicación en la documentación de Microsoft Azure.
- Si el conector es un conector administrado por el cliente y también existe un conector vinculado a un servicio, la eliminación del conector administrado por el cliente no afecta al conector vinculado al servicio. Security Hub CSPM sigue recibiendo los resultados de la gestión de la postura a través del conector vinculado al servicio.
- Los hallazgos existentes pasan a un estado archivado en un plazo de 3 a 5 días y se eliminan después del período de retención de 90 días.

Para eliminar un conector de Azure

1. Abra la consola CSPM de Security Hub.
2. En el panel de navegación, elija Integraciones.
3. Seleccione su conector.
4. Elija Eliminar.
5. Cuando se le solicite, confirme que desea eliminar el conector.

Tras la eliminación, si lo desea, puede limpiar los recursos de Azure que se crearon durante la configuración:

- Elimine el registro de la aplicación en Microsoft Entra ID.
- Elimine el espacio de nombres y el grupo de recursos de Event Hub.
- Elimine la configuración de diagnóstico que exporta los registros de actividad y los registros de auditoría de Entra ID.

Creación y actualización de resultados en el CSPM de Security Hub

En AWS Security Hub CSPM, un hallazgo es un registro observable de una comprobación de seguridad o detección relacionada con la seguridad. Un resultado puede provenir de uno de los siguientes orígenes:

- Una comprobación de seguridad correspondiente a un control del CSPM de Security Hub.
- Una integración con otra. Servicio de AWS
- Una integración con un producto de terceros.
- Una integración personalizada.

El CSPM de Security Hub normaliza los resultados de todos los orígenes conforme a una sintaxis y un formato estándar denominados Formato de resultados de seguridad de AWS (ASFF). Para obtener información detallada sobre este formato, incluidas las descripciones de los campos individuales de ASFF, consulte AWS Formato de búsqueda de seguridad (ASFF). Si habilita la agregación entre regiones, el CSPM de Security Hub también consolida automáticamente los resultados nuevos y actualizados provenientes de todas las regiones vinculadas en la región de

agregación que especifique. Para obtener más información, consulte Descripción de la agregación entre regiones en el CSPM de Security Hub.

Una vez creado un resultado, se puede actualizar de la siguiente manera:

- Un proveedor de resultados puede usar la operación BatchImportFindings de la API del CSPM de Security Hub para actualizar información general sobre el resultado. Los proveedores de hallazgos solo pueden actualizar los hallazgos que hayan creado.
- Un cliente puede usar la consola del CSPM de Security Hub o la operación BatchUpdateFindings de la API del CSPM de Security Hub para actualizar el estado de la investigación relacionada con un resultado. La operación `BatchUpdateFindings` también puede ser utilizada por un SIEM, sistemas de gestión de tickets, herramientas de administración de incidentes, SOAR u otras soluciones en nombre de un cliente.

Para reducir el ruido de resultados y optimizar el seguimiento y análisis de resultados individuales, el CSPM de Security Hub elimina automáticamente los resultados que no se han actualizado recientemente. El momento en el que el CSPM de Security Hub realiza esta eliminación depende de si el resultado está activo o archivado:

- Un resultado activo es un resultado cuyo estado de registro (`RecordState`) es `ACTIVE`. El CSPM de Security Hub almacena los resultados activos durante 90 días. Si un resultado activo no se ha actualizado en 90 días, vence y el CSPM de Security Hub lo elimina de forma permanente.
- Un resultado archivado es un resultado cuyo estado de registro (`RecordState`) es `ARCHIVED`. El CSPM de Security Hub almacena los resultados archivados durante 30 días. Si un resultado archivado no se ha actualizado en 30 días, vence y el CSPM de Security Hub lo elimina de forma permanente.

Para los resultados de control, es decir aquellos que el CSPM de Security Hub genera a partir de las comprobaciones de seguridad de los controles, el CSPM de Security Hub determina si un resultado ha caducado según el valor del campo `UpdatedAt` del resultado. Si ese valor corresponde a más de 90 días para un resultado activo, el CSPM de Security Hub lo elimina de forma permanente. Si ese valor corresponde a más de 30 días para un resultado archivado, el CSPM de Security Hub también lo elimina de forma permanente.

Para cualquier otro tipo de resultado, el CSPM de Security Hub determina si ha caducado basándose en los valores de los campos `ProcessedAt` y `UpdatedAt` del resultado. El CSPM de Security Hub compara estos valores y determina cuál es el más reciente. Si el valor más reciente corresponde a

más de 90 días para un resultado activo, el CSPM de Security Hub lo elimina de forma permanente. Si el valor más reciente corresponde a más de 30 días para un resultado archivado, el CSPM de Security Hub lo elimina de forma permanente. Los proveedores de resultados pueden modificar el valor del campo `UpdatedAt` de uno o varios resultados mediante la operación BatchImportFindings de la API del CSPM de Security Hub.

Para retener los resultados durante más tiempo, puede exportarlos a un bucket de S3. Puedes hacerlo mediante una acción personalizada con una EventBridge regla de Amazon. Para obtener más información, consulte Uso EventBridge para respuesta y remediación automatizadas.

Temas

- BatchImportFindings para encontrar proveedores
- BatchUpdateFindings para los clientes
- Revisión de detalles e historial de resultados en el CSPM de Security Hub
- Filtrado de resultados en el CSPM de Security Hub
- Agrupación de resultados en el CSPM de Security Hub
- Configuración del estado del flujo de trabajo de los resultados en el CSPM de Security Hub
- Envío de resultados a una acción personalizada del CSPM de Security Hub
- AWS Formato de búsqueda de seguridad (ASFF)

BatchImportFindings para encontrar proveedores

Los proveedores de resultados pueden usar la operación BatchImportFindings para crear nuevos resultados en el CSPM de AWS Security Hub. También pueden usar esta operación para actualizar resultados que ellos mismos hayan creado. Los proveedores de resultados no pueden actualizar resultados que no hayan creado.

Los clientes, los SIEM, las herramientas de ticketing, las soluciones SOAR y otros tipos de herramientas deben usar la operación BatchUpdateFindings para realizar actualizaciones relacionadas con la investigación de resultados provenientes de proveedores de resultados. Para obtener más información, consulte the section called “BatchUpdateFindings para los clientes”.

Cuando Security Hub CSPM recibe una `BatchImportFindings` solicitud para crear o actualizar un hallazgo, genera automáticamente un Security Hub Findings - Imported evento en Amazon. EventBridge Puede tomar medidas automatizadas en relación con ese evento. Para obtener más información, consulte the section called “Respuesta y corrección automatizadas”.

Requisitos previos para utilizar **`BatchImportFindings`**

`BatchImportFindings` debe ser llamada por una de las siguientes opciones:

- La cuenta que está asociada al resultado. El identificador de la cuenta asociada debe coincidir con el valor del atributo `AwsAccountId` del resultado.
- Una cuenta que figure en la lista de cuentas permitidas como integración oficial del CSPM de Security Hub.

El CSPM de Security Hub solo puede aceptar actualizaciones de resultados para cuentas que tengan habilitado el CSPM de Security Hub. El proveedor de hallazgos también debe estar habilitado. Si el CSPM de Security Hub está desactivado, o si la integración con el proveedor de resultados no está habilitada, los resultados se devuelven en la lista `FailedFindings` con un error `InvalidAccess`.

Determinación de si se debe crear o actualizar un hallazgo

Para determinar si debe crear o actualizar un resultado, el CSPM de Security Hub revisa el campo `ID`. Si el valor de `ID` no coincide con un resultado existente, el CSPM de Security Hub crea un resultado nuevo.

Si `ID` coincide con un resultado existente, el CSPM de Security Hub verifica el campo `UpdatedAt` de la actualización y procede de la siguiente manera:

- Si el valor de `UpdatedAt` en la actualización coincide con `UpdatedAt` o es anterior a este en el resultado existente, el CSPM de Security Hub ignora la solicitud de actualización.
- Si el valor de `UpdatedAt` en la actualización es posterior a `UpdatedAt` en el resultado existente, el CSPM de Security Hub actualiza el resultado.

Restricciones para la actualización de resultados con **`BatchImportFindings`**

Los proveedores de resultados no pueden utilizar `BatchImportFindings` para actualizar los siguientes atributos de un resultado existente:

- `Note`
- `UserDefinedFields`
- `VerificationState`
- `Workflow`

El CSPM de Security Hub ignora cualquier contenido incluido en una solicitud de `BatchImportFindings` para estos atributos. Los clientes o las entidades que actúan en su nombre (como las herramientas de creación de tickets) pueden utilizar `BatchUpdateFindings` para actualizar estos atributos.

Actualización de los hallazgos con FindingProviderFields

La búsqueda de proveedores tampoco debería utilizarse `BatchImportFindings` para actualizar los siguientes atributos de nivel superior en el formato de búsqueda AWS de seguridad (ASFF):

- `Confidence`
- `Criticality`
- `RelatedFindings`
- `Severity`
- `Types`

En su lugar, los proveedores de resultados deben utilizar el objeto `FindingProviderFields` para proporcionar valores para estos atributos.

Ejemplo

```
"FindingProviderFields": {
    "Confidence": 42,
    "Criticality": 99,
    "RelatedFindings":[
      {
        "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
        "Id": "123e4567-e89b-12d3-a456-426655440000"
      }
    ],
    "Severity": {
        "Label": "MEDIUM",
        "Original": "MEDIUM"
    },
    "Types": [ "Software and Configuration Checks/Vulnerabilities/CVE" ]
}
```

En el caso de las solicitudes `BatchImportFindings`, el CSPM de Security Hub maneja los valores de los atributos de nivel superior y los de `FindingProviderFields` de la siguiente forma:

(Opción preferida): **`BatchImportFindings`** proporciona un valor para un atributo en **`FindingProviderFields`**, pero no proporciona un valor para el atributo equivalente de nivel superior.

Por ejemplo, `BatchImportFindings` proporciona `FindingProviderFields.Confidence`, pero no proporciona `Confidence`. Esta es la opción preferida para las solicitudes `BatchImportFindings`.

El CSPM de Security Hub actualiza el valor del atributo en `FindingProviderFields`.

Replica el valor en el atributo de nivel superior solo si `BatchUpdateFindings` aún no actualizó el atributo.

`BatchImportFindings` proporciona un valor para un atributo de nivel superior, pero no proporciona un valor para el atributo correspondiente **`FindingProviderFields`**.

Por ejemplo, `BatchImportFindings` proporciona `Confidence`, pero no proporciona `FindingProviderFields.Confidence`.

El CSPM de Security Hub usa el valor para actualizar el atributo en `FindingProviderFields`. Sobrescribe cualquier valor existente.

El CSPM de Security Hub actualiza el atributo de nivel superior solo si `BatchUpdateFindings` aún no ha actualizado el atributo.

`BatchImportFindings` proporciona un valor tanto para un atributo de nivel superior como para el atributo correspondiente a **`FindingProviderFields`**.

Por ejemplo, `BatchImportFindings` proporciona tanto `Confidence` como `FindingProviderFields.Confidence`.

Si se trata de un resultado nuevo, el CSPM de Security Hub utiliza el valor dentro de `FindingProviderFields` para rellenar tanto el atributo de nivel superior como el atributo correspondiente dentro de `FindingProviderFields`. No utiliza el valor de atributo de nivel superior proporcionado.

En el caso de un resultado existente, el CSPM de Security Hub usa ambos valores. Sin embargo, actualiza el valor del atributo de nivel superior solo si `BatchUpdateFindings` aún no ha actualizado el atributo.

BatchUpdateFindings para los clientes

AWS Los clientes del CSPM de Security Hub y las entidades que actúen en su nombre pueden utilizar la BatchUpdateFindings operación para actualizar la información relacionada con el procesamiento de las conclusiones del CSPM de Security Hub procedentes de los proveedores que buscan. Como cliente, puede usar esta operación directamente. Las herramientas de SIEM, sistemas de tickets, soluciones de administración de incidentes y plataformas SOAR también pueden usar esta operación en nombre del cliente.

No puede usar la operación `BatchUpdateFindings` para crear resultados nuevos. Sin embargo, puede utilizarla para actualizar hasta 100 resultados existentes a la vez. En una `BatchUpdateFindings` solicitud, se especifican las conclusiones que se deben actualizar, los campos del formato de búsqueda de AWS seguridad (ASFF) que se deben actualizar para las conclusiones y los nuevos valores de los campos. El CSPM de Security Hub actualiza los resultados según lo especificado en la solicitud. Este proceso puede tardar varios minutos. Si actualiza resultados mediante la operación `BatchUpdateFindings`, las actualizaciones no afectan los valores existentes del campo `UpdatedAt` de los resultados.

Cuando Security Hub CSPM recibe una `BatchUpdateFindings` solicitud para actualizar un resultado, genera automáticamente un Security Hub Findings – Imported evento en Amazon. EventBridge Puede usar este evento para ejecutar acciones automáticas sobre el resultado especificado. Para obtener más información, consulte the section called “Respuesta y corrección automatizadas”.

Campos disponibles para BatchUpdateFindings

Si inicia sesión en una cuenta de administrador del CSPM de Security Hub, puede usar `BatchUpdateFindings` para actualizar los resultados generados por la cuenta de administrador o por las cuentas de miembro. Las cuentas de miembro pueden utilizar `BatchUpdateFindings` para actualizar los resultados solo para su cuenta.

Los clientes pueden usar `BatchUpdateFindings` para actualizar los siguientes campos y objetos:

- `Confidence`
- `Criticality`
- `Note`
- `RelatedFindings`
- `Severity`

- `Types`
- `UserDefinedFields`
- `VerificationState`
- `Workflow`

Configurar el acceso a BatchUpdateFindings

Puede configurar políticas AWS Identity and Access Management (IAM) para restringir el acceso y utilizarlas `BatchUpdateFindings` para actualizar los campos de búsqueda y los valores de los campos.

En una declaración para restringir el acceso a `BatchUpdateFindings`, utilice los siguientes valores:

- `Action` es `securityhub:BatchUpdateFindings`
- `Effect` es `Deny`
- Para `Condition`, puede denegar una solicitud `BatchUpdateFindings` en función de lo siguiente:
  - El resultado incluye un campo específico.
  - El resultado incluye un valor de campo específico.

Claves de condición

Estas son las claves de condición para restringir el acceso a `BatchUpdateFindings`.

Campo de ASFF

La clave de condición de un campo de ASFF es la siguiente:

```
securityhub:ASFFSyntaxPath/<fieldName>
```

Sustituya *`<fieldName>`* por el campo de ASFF. Al configurar el acceso a `BatchUpdateFindings`, incluya uno o más campos de ASFF específicos en su política de IAM en lugar de un campo de nivel principal. Por ejemplo, para restringir el acceso al campo `Workflow.Status`, debe incluir `securityhub:ASFFSyntaxPath/Workflow.Status` en su política en lugar del campo de nivel principal `Workflow`.

Cómo no permitir todas las actualizaciones de un campo

Para evitar que un usuario actualice un campo específico, utilice una condición como esta:

```
 "Condition": {
                "Null": {
                    "securityhub:ASFFSyntaxPath/<fieldName>": "false"
               }
}
```

Por ejemplo, la siguiente declaración indica que no se puede usar `BatchUpdateFindings` para actualizar el campo de resultados `Workflow.Status`.

```
{
    "Sid": "VisualEditor0",
    "Effect": "Deny",
    "Action": "securityhub:BatchUpdateFindings",
    "Resource": "*",
    "Condition": {
        "Null": {
            "securityhub:ASFFSyntaxPath/Workflow.Status": "false"
        }
    }
}
```

Cómo no permitir valores de campo específicos

Para evitar que un usuario establezca un campo en un valor específico, utilice una condición como esta:

```
"Condition": {
                "StringEquals": {
                    "securityhub:ASFFSyntaxPath/<fieldName>": "<fieldValue>"
               }
}
```

Por ejemplo, la siguiente declaración indica que no se puede usar `BatchUpdateFindings` para establecer `Workflow.Status` como `SUPPRESSED`.

```
{
    "Sid": "VisualEditor0",
```

```
    "Effect": "Deny",
    "Action": "securityhub:BatchUpdateFindings",
    "Resource": "*",
    "Condition": {
    "StringEquals": {
        "securityhub:ASFFSyntaxPath/Workflow.Status": "SUPPRESSED"
    }
}
```

También puede proporcionar una lista de valores que no están permitidos.

```
 "Condition": {
                "StringEquals": {
                    "securityhub:ASFFSyntaxPath/<fieldName>": [ "<fieldValue1>",
 "<fieldValue2>", "<fieldValuen>" ]
               }
}
```

Por ejemplo, la siguiente declaración indica que no se puede usar `BatchUpdateFindings` para establecer `Workflow.Status` como `RESOLVED` o `SUPPRESSED`.

```
{
    "Sid": "VisualEditor0",
    "Effect": "Deny",
    "Action": "securityhub:BatchUpdateFindings",
    "Resource": "*",
    "Condition": {
    "StringEquals": {
        "securityhub:ASFFSyntaxPath/Workflow.Status": [
            "RESOLVED",
            "NOTIFIED"
        ]
    }
}
```

Revisión de detalles e historial de resultados en el CSPM de Security Hub

En AWS Security Hub CSPM, un hallazgo es un registro observable de una comprobación de seguridad o detección relacionada con la seguridad. El CSPM de Security Hub genera un resultado cuando completa una comprobación de seguridad de un control o cuando ingiere un resultado proveniente de un Servicio de AWS o producto de terceros integrado. Cada resultado incluye un

historial de cambios y otros detalles, como una clasificación de gravedad e información sobre los recursos afectados.

Puede revisar el historial y otros detalles de resultados individuales en la consola del CSPM de Security Hub o mediante programación con la API del CSPM de Security Hub o la AWS CLI.

Para ayudar a agilizar el análisis, la consola del CSPM de Security Hub muestra un panel de resultado cuando selecciona un resultado específico. El panel incluye distintos menús y pestañas para revisar los detalles específicos de un resultado.

Menús de acciones

Desde este menú, puede revisar el JSON completo de un resultado o agregar notas. Un resultado puede tener solo una nota asociada a la vez. Este menú también ofrece opciones para establecer el estado del flujo de trabajo de un hallazgo o enviar un hallazgo a una acción personalizada en Amazon. EventBridge

Menú de investigación

Desde este menú, puede investigar un resultado en Amazon Detective. El detective extrae entidades, como direcciones IP y AWS usuarios, de un hallazgo y visualiza su actividad. Puede utilizar la actividad de la entidad como punto de partida para investigar la causa y el impacto de un resultado.

Pestaña Overview (Información general)

Esta pestaña ofrece un resumen del resultado. Por ejemplo, puede ver cuándo se creó y cuándo se actualizó por última vez, en qué cuenta existe y cuál es el origen del resultado. En el caso de los resultados de controles, esta pestaña también muestra el nombre de la regla de AWS Config asociada y un enlace a la guía de remediación en la documentación del CSPM de Security Hub.

En la instantánea de Recursos en la pestaña Descripción general, puede obtener una vista breve de los recursos involucrados en el resultado. En el caso de algunos recursos, esto incluye la opción Abrir recurso, que enlaza directamente con el recurso afectado en la Servicio de AWS consola correspondiente. La instantánea del Historial muestra hasta dos cambios realizados en el resultado en la fecha más reciente para la que se está rastreando el historial. Por ejemplo, si hizo un cambio ayer y otro hoy, la instantánea muestra el cambio más reciente. Para revisar entradas anteriores, cambie a la pestaña Historial.

La fila Conformidad se expande para mostrar más detalles. Por ejemplo, si un control incluye parámetros, puede revisar los valores del parámetro que el CSPM de Security Hub utiliza actualmente al realizar las comprobaciones de seguridad del control.

Pestaña recursos

En esta pestaña se proporcionan detalles sobre los recursos que intervienen en un resultado. Si has iniciado sesión en la cuenta que es propietaria de un recurso, puedes revisar el recurso en la Servicio de AWS consola correspondiente. Si no eres el propietario de un recurso, en esta pestaña se muestra el Cuenta de AWS ID del propietario.

La fila Detalles muestra información específica del recurso en un resultado. Incluye la sección ResourceDetails del resultado en formato JSON.

La fila Etiquetas muestra las claves y valores de etiquetas asignados a los recursos involucrados en un resultado. Los recursos que son compatibles con la operación GetResources de la API de etiquetado de Grupos de recursos de AWS se pueden etiquetar. El CSPM de Security Hub invoca esta operación mediante un rol vinculado al servicio cuando procesa resultados nuevos o actualizados, y recupera las etiquetas del recurso si el campo `Resource.Id` del Formato de resultados de seguridad de AWS (ASFF) contiene el ARN de un recurso. El CSPM de Security Hub ignora los ID de recurso que no son válidos. Para obtener más información sobre la inclusión de etiquetas de recursos en los resultados, consulte Tags.

Pestaña de historial

Esta pestaña rastrea el historial de un resultado. El historial de resultados está disponible para los resultados activos y archivados. Proporciona un registro inmutable de los cambios realizados en un resultado a lo largo del tiempo, incluidos los campos del ASFF que cambiaron, cuándo ocurrió el cambio y qué usuario lo realizó. Cada página de la pestaña muestra hasta 20 cambios. Los cambios más recientes se muestran primero.

En el caso de resultados activos, el historial está disponible por hasta 90 días. En el caso de resultados archivados, el historial está disponible por hasta 30 días. El historial incluye los cambios realizados manualmente o de forma automática por las reglas de automatización del CSPM de Security Hub. No incluye cambios en los campos de marcas de tiempo de nivel superior, como los campos `CreatedAt` y `UpdatedAt`.

Si inicia sesión en una cuenta de administrador del CSPM de Security Hub, el historial de resultados corresponde tanto a la cuenta de administrador como a todas las cuentas de miembro.

Pestaña de amenazas

Esta pestaña incluye datos de los objetos Action, Malware y ProcessDetails del ASFF, incluidos el tipo de amenaza y si un recurso es el objetivo o el actor. Estos detalles suelen aplicarse a los hallazgos que se originan en Amazon GuardDuty.

Pestaña de vulnerabilidades

Esta pestaña muestra los datos del objeto Vulnerability del ASFF, incluyendo si hay vulnerabilidades o correcciones disponibles asociadas a un resultado. Estos detalles también se aplican por lo general a resultados que se originan en Amazon Inspector.

Las filas de cada pestaña incluyen una opción para copiar o filtrar. Por ejemplo, si abre el panel de un resultado cuyo estado de flujo de trabajo es Notificado, puede elegir la opción de filtrado junto a Estado del flujo de trabajo. Si selecciona Mostrar todos los resultados con este valor, el CSPM de Security Hub filtra la tabla de resultados y muestra únicamente aquellos que tienen el mismo estado de flujo de trabajo.

Revisión de los detalles y el historial de resultados

Elija el método que prefiera y siga los pasos para revisar los detalles de los resultados en el CSPM de Security Hub.

Si activó la agregación entre regiones e inicia sesión en la región de agregación, los datos de resultados incluyen datos de la región de agregación y de las regiones vinculadas. En otras regiones, los datos de resultados son específicos únicamente de esa región. Para obtener más información sobre la agregación entre regiones, consulte the section called “Agregar datos en las regiones”.

Security Hub CSPM console

Revisión de los detalles y el historial de resultados

1. Abra la consola CSPM de AWS Security Hub en. https://console.aws.amazon.com/securityhub/
2. Para mostrar una lista de resultado, realice una de las acciones siguientes:
   - En el panel de navegación, seleccione Resultados. Agregue los filtros de búsqueda según sea necesario para acotar la lista de resultados.
   - En el panel de navegación, elija Insights. Elija una información. En la lista de resultados, seleccione un resultado de producto de información.
   - En el panel de navegación, elija Integraciones. Seleccione Ver los resultados de una integración.
   - En el panel de navegación, elija Controles.
3. Seleccione un resultado. El panel del resultado muestra todos los detalles correspondientes.

4. En ese panel, puede realizar cualquiera de las siguientes acciones:
   - Revisar detalles específicos del resultado. Para ello, seleccione una pestaña.
   - Tomar medidas con respecto al resultado. Para ello, seleccione una opción del menú Acciones.
   - Investigar el resultado en Amazon Detective. Para ello, sleccione la opción Investigar.

> **Note**
>
> Si se integra con una cuenta de miembro AWS Organizations y ha iniciado sesión en ella, el panel de búsqueda incluye el nombre de la cuenta. En cambio, para cuentas de miembro invitadas manualmente (en lugar de pertenecer a Organizations), el panel muestra únicamente el ID de la cuenta.

Security Hub CSPM API

Utilice el GetFindings funcionamiento de la API CSPM de Security Hub o, si está utilizando AWS CLI, ejecute el get-findings comando. Puede proporcionar uno o varios valores para el parámetro `Filters` con el fin de limitar los resultados que desea obtener.

Si el volumen de resultados es demasiado grande, puede utilizar el parámetro `MaxResults` para limitar los resultados a un número específico y el parámetro `NextToken` para paginar los resultados. Use el parámetro `SortCriteria` para ordenar los resultados por un campo específico.

Por ejemplo, el siguiente AWS CLI comando recupera los resultados que coinciden con los criterios de filtro especificados y ordena los resultados en orden descendente según el campo. `LastObservedAt` Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$ aws securityhub get-findings \
--filters '{"GeneratorId":[{"Value": "aws-
foundational","Comparison":"PREFIX"}],"WorkflowStatus": [{"Value":
 "NEW","Comparison":"EQUALS"}],"Confidence": [{"Gte": 85}]}' --sort-criteria
 '{"Field": "LastObservedAt","SortOrder": "desc"}' --page-size 5 --max-items 100
```

Para revisar el historial de resultados, utilice la operación GetFindingHistory. Si está utilizando el AWS CLI, ejecute el get-finding-history comando. Identifique el resultado del que desea obtener un historial con los campos `ProductArn` y `Id`. Para obtener información acerca de estos campos, consulte AwsSecurityFindingIdentifier. Cada solicitud puede recuperar el historial de un único resultado.

Por ejemplo, el AWS CLI comando siguiente recupera el historial de la búsqueda especificada. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$ aws securityhub get-finding-history \
--region us-west-2 \
--finding-identifier Id="a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",ProductArn="arn:aws:securityhub:us-
west-2:123456789012:product/123456789012/default" \
--max-results 2 \
--start-time "2021-09-30T15:53:35.573Z" \
--end-time "2021-09-31T15:53:35.573Z"
```

PowerShell

Utilice el cmdlet `Get-SHUBFinding`. De manera opcional, puede completar el parámetro `Filter` para acotar los resultados que desea recuperar.

Por ejemplo, el siguiente cmdlet recupera los resultados que coinciden con los filtros especificados.

```
Get-SHUBFinding -Filter @{AwsAccountId =
 [Amazon.SecurityHub.Model.StringFilter]@{Comparison = "EQUALS"; Value =
 "XXX"};ComplianceStatus = [Amazon.SecurityHub.Model.StringFilter]@{Comparison =
 "EQUALS"; Value = 'FAILED'}}
```

> **Note**
>
> Si filtra los resultados por `CompanyName` o por `ProductName`, el CSPM de Security Hub usa los valores que forman parte del objeto ASFF de `ProductFields`. El CSPM de Security Hub no usa los campos de nivel superior `CompanyName` y `ProductName`.

Filtrado de resultados en el CSPM de Security Hub

AWS Security Hub CSPM genera sus propias conclusiones a partir de las comprobaciones de seguridad y recibe las conclusiones de los productos integrados. Puede mostrar una lista de resultados en las páginas Resultados, Integraciones e Productos de información de la consola del CSPM de Security Hub. Puede agregar filtros para acotar una lista de resultados y hacer que sea relevante para la organización o caso de uso.

Para obtener información sobre cómo filtrar resultados de un control de seguridad específico, consulte the section called “Filtrado y clasificación de resultados de control”. La información de esta página se aplica a las páginas Resultados, Productos de información e Integraciones.

Filtros predeterminados en las listas de resultados

De forma predeterminada, las listas de resultados en la consola del CSPM de Security Hub se filtran según los campos `RecordState` y `Workflow.Status` del formato de resultados de seguridad de AWS (ASFF). Esto se suma a los filtros aplicados a un producto de información específico o a una integración.

El estado de registro indica si el resultado está activo o archivado. De forma predeterminada, las listas de hallazgos solo muestran los hallazgos activos. Un proveedor de resultados puede archivar un resultado si ya no está activo o no es importante. El CSPM de Security Hub también archiva automáticamente los resultados de controles si se elimina el recurso asociado.

El estado de flujo de trabajo indica el estado de una investigación sobre un resultado. De forma predeterminada, las listas de hallazgos solo muestran los hallazgos con estado de flujo de trabajo `NEW` o `NOTIFIED`. Puede actualizar el estado de flujo de trabajo de un resultado.

Instrucciones para agregar filtros

Puede filtrar una lista de resultados por hasta diez atributos. Para cada atributo, puede proporcionar hasta 20 valores de filtro.

Al filtrar la lista de resultados, el CSPM de Security Hub aplica la lógica `AND` al conjunto de filtros. Un resultado coincide únicamente si cumple todos los filtros proporcionados. Por ejemplo, si lo agrega GuardDuty como filtro por el nombre del producto y `AwsS3Bucket` como filtro por el tipo de recurso, el CSPM de Security Hub muestra los resultados que cumplen con estos dos criterios.

El CSPM de Security Hub aplica la lógica `OR` a los filtros que usan el mismo atributo pero valores diferentes. Por ejemplo, si añades ambos valores GuardDuty y Amazon Inspector como valores

de filtro para el nombre del producto, Security Hub CSPM mostrará los resultados generados por Amazon Inspector o GuardDuty por Amazon Inspector.

Para agregar filtros a una lista de resultados (consola)

1. Abra la consola AWS CSPM de Security Hub en. https://console.aws.amazon.com/securityhub/
2. Para mostrar una lista de resultados, realice una de las siguientes acciones desde el panel de navegación:
   - Elija Resultados.
   - Elija Información. Elija una información. A continuación, en la lista de resultados, seleccione un producto de información.
   - Seleccione Integraciones. Seleccione Ver los resultados de una integración.
3. En el cuadro Agregar filtros, seleccione uno o más campos por los cuales filtrar.

   Al filtrar por nombre de empresa o nombre de producto, la consola utiliza el nivel superior `CompanyName` y los `ProductName` campos del formato de búsqueda de AWS seguridad (ASFF). La API usa los valores que están anidados bajo `ProductFields`.
4. Elija el tipo de coincidencia de filtro.

   Para un filtro de tipo cadena, puede elegir entre las siguientes opciones:

   - es: busca un valor que coincida exactamente con el valor del filtro.
   - empieza por: busca un valor que empiece por el valor del filtro.
   - no es: busca un valor que no coincida con el valor del filtro.
   - no empieza por: busca un valor que no empiece por el valor del filtro.

   En el campo Etiquetas de recurso, puede filtrar según claves o valores específicos.

   Para un filtro numérico, puede elegir si desea proporcionar un solo número (Simple) o un rango de números (Range).

   Para un filtro de fecha y hora, puede elegir si desea proporcionar un período de tiempo a partir de la fecha y hora actuales (Rolling window) o de un intervalo de fechas específico (Fixed range).

   La adición de varios filtros tiene las siguientes interacciones:

- Los filtros es y empieza por van unidos por O. Un valor coincide si contiene alguno de los valores del filtro. Por ejemplo, si especifica que la Etiqueta de gravedad es CRÍTICA y la Etiqueta de gravedad es ALTA, los resultados incluyen tanto los resultados de gravedad crítica como de gravedad alta.
- Los filtros no es y no empieza por van unidos por AND. Un valor solo coincide si no contiene ninguno de esos valores de filtro. Por ejemplo, si especifica que la Etiqueta de gravedad no es BAJA y la Etiqueta de gravedad no es MEDIA, los resultados no incluyen los resultados de gravedad baja o media.

Si tiene un filtro es en un campo, no puede tener un filtro no es o no empieza por en el mismo campo.

5. Especifique el valor del filtro. Para los filtros de cadena, el valor del filtro distingue entre mayúsculas y minúsculas.
6. Seleccione Aplicar.

   Para un filtro existente, puede cambiar el tipo de coincidencia o el valor del filtro. En una lista de resultados filtrada, elija el filtro. En el cuadro Editar filtro, seleccione el nuevo tipo de coincidencia o valor y, luego, elija Aplicar.

   Para quitar un filtro, elija el icono x. La lista se actualiza automáticamente para reflejar el cambio.

Agrupación de resultados en el CSPM de Security Hub

Puede agrupar las conclusiones en el CSPM de AWS Security Hub en función de los valores de un atributo seleccionado.

Al agrupar los resultados, la lista de resultados se reemplaza por una lista de valores para el atributo seleccionado en los resultados coincidentes. Para cada valor, la lista muestra la cantidad de resultados coincidentes.

Por ejemplo, si agrupa las conclusiones por Cuenta de AWS ID, verá una lista de identificadores de cuentas con el número de conclusiones coincidentes para cada cuenta.

El CSPM de Security Hub puede mostrar hasta 100 valores para un atributo seleccionado. Si hay más de 100 valores, solo verá los primeros 100.

Cuando elige un valor de atributo, el CSPM de Security Hub muestra la lista de resultados coincidentes para ese valor.

Para agrupar los resultados en una lista de resultados (consola)

1. Abra la consola CSPM de AWS Security Hub en. https://console.aws.amazon.com/securityhub/
2. Para mostrar una lista de resultados, realice una de las siguientes acciones desde el panel de navegación:
   - Elija Resultados.
   - Elija Información. Elija una información. A continuación, en la lista de resultados, seleccione un producto de información.
   - Seleccione Integraciones. Seleccione Ver los resultados de una integración.
3. En la lista desplegable Agrupar por, elija el atributo que desea utilizar para la agrupación.

   Para eliminar un atributo de agrupación, elija el icono x. Cuando elimina el atributo de agrupación, la lista deja de mostrar los valores del atributo y pasa a mostrar una lista de resultados.

Configuración del estado del flujo de trabajo de los resultados en el CSPM de Security Hub

El estado de flujo de trabajo realiza un seguimiento del progreso de la investigación sobre un resultado. El estado del flujo de trabajo es específico de un resultado individual y no afecta la generación de nuevos resultados. Por ejemplo, si cambia el estado del flujo de trabajo de un resultado a `SUPPRESSED` o `RESOLVED`, ese cambio no impide que el CSPM de Security Hub genere un nuevo resultado para el mismo problema.

El estado del flujo de trabajo de un resultado puede tener uno de los siguientes valores.

NUEVO

Es el estado inicial de un resultado antes de revisarlo.

Los hallazgos que se ingieren de forma integrada Servicios de AWS, por ejemplo AWS Config, tienen `NEW` como estado inicial.

El CSPM de Security Hub también restablece el estado del flujo de trabajo de `NOTIFIED` o `RESOLVED` a `NEW` en los siguientes casos:

- `RecordState` cambia de `ARCHIVED` a `ACTIVE`.
- `Compliance.Status` cambia de `PASSED` a `FAILED`, `WARNING` o `NOT_AVAILABLE`.

Estos cambios implican que es necesaria una investigación adicional.

NOTIFICADO

Indica que informó sobre el problema de seguridad al propietario del recurso. Puede utilizar este estado cuando no sea el propietario del recurso y necesite la intervención del propietario para que se resuelva un problema de seguridad.

Si se produce una de las siguientes situaciones, el estado del flujo de trabajo cambia automáticamente de `NOTIFIED` a `NEW`:

- `RecordState` cambia de `ARCHIVED` a `ACTIVE`.
- `Compliance.Status` cambia de `PASSED` a `FAILED`, `WARNING` o `NOT_AVAILABLE`.

SUPRIMIDO

Indica que ha revisado el resultado y no cree que sea necesario realizar ninguna acción.

El estado del flujo de trabajo de un resultado del tipo `SUPPRESSED` no cambia si `RecordState` cambia de `ARCHIVED` a `ACTIVE`.

RESUELTO

El hallazgo se ha revisado y se ha corregido. Ahora se considera resuelto.

El resultado permanece como `RESOLVED` a menos que se produzca alguna de las siguientes situaciones:

- `RecordState` cambia de `ARCHIVED` a `ACTIVE`.
- `Compliance.Status` cambia de `PASSED` a `FAILED`, `WARNING` o `NOT_AVAILABLE`.

En esos casos, el estado del flujo de trabajo se restablece automáticamente a `NEW`.

Para los resultados provenientes de controles, si `Compliance.Status` es `PASSED`, el CSPM de Security Hub establece automáticamente el estado del flujo de trabajo en `RESOLVED`.

Configuración del estado de flujo de trabajo de los resultados

Para cambiar el estado del flujo de trabajo de uno o varios resultados, puede usar la consola del CSPM de Security Hub o la API del CSPM de Security Hub. Si cambia el estado del flujo de trabajo

de un resultado, tenga en cuenta que el CSPM de Security Hub puede tardar varios minutos en procesar la solicitud y actualizar el resultado.

> **Tip**
>
> También puede cambiar automáticamente el estado del flujo de trabajo de los resultados mediante reglas de automatización. Con las reglas de automatización, configura el CSPM de Security Hub para actualizar automáticamente el estado del flujo de trabajo de los resultados según los criterios que especifique. Para obtener más información, consulte Descripción de las reglas de automatización en el CSPM de Security Hub.

Para cambiar el estado del flujo de trabajo de uno o varios resultados, elija el método que prefiera y siga los pasos.

Security Hub CSPM console

Para cambiar el estado del flujo de trabajo de los resultados

1. Abra la consola CSPM de AWS Security Hub en. https://console.aws.amazon.com/securityhub/
2. En el panel de navegación, realice una de las siguientes acciones para mostrar una tabla de resultados:
   - Elija Resultados.
   - Elija Información. Luego, elija un producto de información. En la salida del producto de información, elija una de las salidas.
   - Seleccione Integraciones. Luego, en la sección de la integración, elija Ver resultados.
   - Elija Estándares de seguridad. Luego, en la sección del estándar, seleccione Ver salidas. En la tabla de controles, elija un control para mostrar los resultados correspondientes a ese control.
3. En la tabla de resultados, seleccione la casilla de cada resultado cuyo estado del flujo de trabajo desea cambiar.
4. En la parte superior de la página, elija Estado del flujo de trabajo y, después, elija el nuevo estado del flujo de trabajo para los resultados seleccionados.
5. En el cuadro de diálogo Establecer estado del flujo de trabajo, puede ingresar una nota que describa el motivo del cambio del estado del flujo de trabajo. Luego, elija Establecer estado.

Security Hub CSPM API

Utilice la operación BatchUpdateFindings. Proporcione el ID de resultado y el ARN del producto que generó el resultado. Puede obtener estos detalles mediante la GetFindings operación.

AWS CLI

Ejecute el comando batch-update-findings. Proporcione el ID de resultado y el ARN del producto que generó el resultado. Puede obtener estos detalles mediante la ejecución del comando get-findings.

```
batch-update-findings --finding-identifiers
 Id="<findingID>",ProductArn="<productARN>" --workflow Status="<workflowStatus>"
```

Ejemplo

```
aws securityhub batch-update-findings --finding-identifiers
 Id="arn:aws:securityhub:us-west-1:123456789012:subscription/
pci-dss/v/3.2.1/PCI.Lambda.2/finding/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",ProductArn="arn:aws:securityhub:us-west-1::product/aws/securityhub" --
workflow Status="RESOLVED"
```

Envío de resultados a una acción personalizada del CSPM de Security Hub

Puede crear acciones personalizadas AWS de Security Hub CSPM para automatizar Security Hub CSPM con Amazon. EventBridge Para las acciones personalizadas, el tipo de evento es Security Hub Findings - Custom Action. Después de configurar una acción personalizada, puede enviarle hallazgos. Para obtener más información y pasos detallados sobre cómo crear acciones personalizadas, consulte the section called “Respuesta y corrección automatizadas”.

Cómo enviar resultados a una acción personalizada (consola)

1. Abra la consola CSPM AWS de Security Hub en. https://console.aws.amazon.com/securityhub/
2. Para mostrar una lista de resultado, realice una de las acciones siguientes:
   - En el panel de navegación del CSPM de Security Hub, elija Resultados.
   - En el panel de navegación del CSPM de Security Hub, elija Productos de información. Elija una información. A continuación, en la lista de resultados, seleccione un resultado de información.

- En el panel de navegación del CSPM de Security Hub, seleccione Integraciones. Seleccione Ver los resultados de una integración.
- En el panel de navegación del CSPM de Security Hub, elija Estándares de seguridad. Seleccione Ver resultados para ver una lista de controles. A continuación, elija el nombre del control.

3. En la lista de resultados, seleccione la casilla de verificación de cada resultado que desee enviar a la acción personalizada.

   Puede seleccionar hasta 20 hallazgos a la vez.

4. En Acciones, elija la acción personalizada.

AWS Formato de búsqueda de seguridad (ASFF)

AWS Security Hub CSPM consume y agrega los hallazgos de productos integrados Servicios de AWS y de terceros. El CSPM de Security Hub procesa estos resultados mediante un formato estándar de resultados denominado Formato de resultados de seguridad de AWS (ASFF), lo que elimina la necesidad de llevar a cabo esfuerzos de conversión de datos que consumen mucho tiempo.

Esta página proporciona un resumen completo del JSON para realizar una búsqueda en el formato de búsqueda de AWS seguridad (ASFF). El formato se deriva del esquema JSON. Elija el nombre de un objeto vinculado para revisar un ejemplo de un resultado para ese objeto. Comparar los resultados del CSPM de Security Hub con los recursos y ejemplos que se muestran aquí puede ser útil a la hora de interpretar los resultados.

Para obtener descripciones de los atributos individuales del formato ASFF, consulte the section called “Atributos de nivel superior necesarios del ASFF” y the section called “Atributos de nivel superior opcionales del ASFF”.

```
"Findings": [
    {
     "Action": {
      "ActionType": "string",
      "AwsApiCallAction": {
       "AffectedResources": {
        "string": "string"
       },
       "Api": "string",
```

```
        "CallerType": "string",
        "DomainDetails": {
         "Domain": "string"
        },
        "FirstSeen": "string",
        "LastSeen": "string",
        "RemoteIpDetails": {
         "City": {
          "CityName": "string"
         },
         "Country": {
          "CountryCode": "string",
          "CountryName": "string"
         },
         "IpAddressV4": "string",
         "Geolocation": {
          "Lat": number,
          "Lon": number
         },
         "Organization": {
          "Asn": number,
          "AsnOrg": "string",
          "Isp": "string",
          "Org": "string"
         }
        },
        "ServiceName": "string"
       },
       "DnsRequestAction": {
        "Blocked": boolean,
        "Domain": "string",
        "Protocol": "string"
       },
       "NetworkConnectionAction": {
        "Blocked": boolean,
        "ConnectionDirection": "string",
        "LocalPortDetails": {
         "Port": number,
         "PortName": "string"
        },
        "Protocol": "string",
        "RemoteIpDetails": {
         "City": {
          "CityName": "string"
```

```
        },
        "Country": {
         "CountryCode": "string",
         "CountryName": "string"
        },
        "IpAddressV4": "string",
        "Geolocation": {
         "Lat": number,
         "Lon": number
        },
        "Organization": {
         "Asn": number,
         "AsnOrg": "string",
         "Isp": "string",
         "Org": "string"
        }
       },
       "RemotePortDetails": {
        "Port": number,
        "PortName": "string"
       }
      },
      "PortProbeAction": {
       "Blocked": boolean,
       "PortProbeDetails": [{
        "LocalIpDetails": {
         "IpAddressV4": "string"
        },
        "LocalPortDetails": {
         "Port": number,
         "PortName": "string"
        },
        "RemoteIpDetails": {
         "City": {
          "CityName": "string"
         },
         "Country": {
          "CountryCode": "string",
          "CountryName": "string"
         },
         "GeoLocation": {
          "Lat": number,
          "Lon": number
         },
```

```
          "IpAddressV4": "string",
          "Organization": {
           "Asn": number,
           "AsnOrg": "string",
           "Isp": "string",
           "Org": "string"
          }
         }
        }]
       }
      },
      "AwsAccountId": "string",
      "AwsAccountName": "string",
      "CompanyName": "string",
      "Compliance": {
       "AssociatedStandards": [{
        "StandardsId": "string"
       }],
       "RelatedRequirements": ["string"],
       "SecurityControlId": "string",
       "SecurityControlParameters": [
        {
         "Name": "string",
         "Value": ["string"]
        }
      ],
       "Status": "string",
       "StatusReasons": [
        {
         "Description": "string",
         "ReasonCode": "string"
        }
       ]
      },
      "Confidence": number,
      "CreatedAt": "string",
      "Criticality": number,
      "Description": "string",
      "Detection": {
       "Sequence": {
        "Uid": "string",
        "Actors": [{
         "Id": "string",
         "Session": {
```

```
          "Uid": "string",
          "MfAStatus": "string",
          "CreatedTime": "string",
          "Issuer": "string"
        },
        "User": {
          "CredentialUid": "string",
          "Name": "string",
          "Type": "string",
          "Uid": "string",
          "Account": {
            "Uid": "string",
            "Name": "string"
          }
        }
      }],
      "Endpoints": [{
        "Id": "string",
        "Ip": "string",
        "Domain": "string",
        "Port": number,
        "Location": {
          "City": "string",
          "Country": "string",
          "Lat": number,
          "Lon": number
        },
        "AutonomousSystem": {
          "Name": "string",
          "Number": number
        },
        "Connection": {
          "Direction": "string"
        }
      }],
      "Signals": [{
        "Id": "string",
        "Title": "string",
        "ActorIds": ["string"],
        "Count": number,
        "FirstSeenAt": number,
        "SignalIndicators": [
          {
            "Key": "string",
```

```
          "Title": "string",
          "Values": ["string"]
         },
         {
          "Key": "string",
          "Title": "string",
          "Values": ["string"]
         }
        ],
        "LastSeenAt": number,
        "Name": "string",
        "ResourceIds": ["string"],
        "Type": "string"
       }],
       "SequenceIndicators": [
        {
         "Key": "string",
         "Title": "string",
         "Values": ["string"]
        },
        {
         "Key": "string",
         "Title": "string",
         "Values": ["string"]
        }
       ]
      }
     },
     "FindingProviderFields": {
      "Confidence": number,
      "Criticality": number,
      "RelatedFindings": [{
       "ProductArn": "string",
       "Id": "string"
      }],
      "Severity": {
       "Label": "string",
       "Normalized": number,
       "Original": "string"
      },
      "Types": ["string"]
     },
     "FirstObservedAt": "string",
     "GeneratorId": "string",
```

```
      "Id": "string",
      "LastObservedAt": "string",
      "Malware": [{
       "Name": "string",
       "Path": "string",
       "State": "string",
       "Type": "string"
      }],
      "Network": {
       "DestinationDomain": "string",
       "DestinationIpV4": "string",
       "DestinationIpV6": "string",
       "DestinationPort": number,
       "Direction": "string",
       "OpenPortRange": {
        "Begin": integer,
        "End": integer
       },
       "Protocol": "string",
       "SourceDomain": "string",
       "SourceIpV4": "string",
       "SourceIpV6": "string",
       "SourceMac": "string",
       "SourcePort": number
      },
      "NetworkPath": [{
       "ComponentId": "string",
       "ComponentType": "string",
       "Egress": {
        "Destination": {
         "Address": ["string"],
         "PortRanges": [{
          "Begin": integer,
          "End": integer
         }]
        },
        "Protocol": "string",
        "Source": {
         "Address": ["string"],
         "PortRanges": [{
          "Begin": integer,
          "End": integer
         }]
        }
```

```
      },
      "Ingress": {
       "Destination": {
        "Address": ["string"],
        "PortRanges": [{
         "Begin": integer,
         "End": integer
        }]
       },
       "Protocol": "string",
       "Source": {
        "Address": ["string"],
        "PortRanges": [{
         "Begin": integer,
         "End": integer
        }]
       }
      }
     }],
     "Note": {
      "Text": "string",
      "UpdatedAt": "string",
      "UpdatedBy": "string"
     },
     "PatchSummary": {
      "FailedCount": number,
      "Id": "string",
      "InstalledCount": number,
      "InstalledOtherCount": number,
      "InstalledPendingReboot": number,
      "InstalledRejectedCount": number,
      "MissingCount": number,
      "Operation": "string",
      "OperationEndTime": "string",
      "OperationStartTime": "string",
      "RebootOption": "string"
     },
     "Process": {
      "LaunchedAt": "string",
      "Name": "string",
      "ParentPid": number,
      "Path": "string",
      "Pid": number,
      "TerminatedAt": "string"
```

```
    },
    "ProductArn": "string",
    "ProductFields": {
     "string": "string"
    },
    "ProductName": "string",
    "RecordState": "string",
    "Region": "string",
    "RelatedFindings": [{
     "Id": "string",
     "ProductArn": "string"
    }],
    "Remediation": {
     "Recommendation": {
      "Text": "string",
      "Url": "string"
     }
    },
    "Resources": [{
     "ApplicationArn": "string",
     "ApplicationName": "string",
     "DataClassification": {
      "DetailedResultsLocation": "string",
      "Result": {
       "AdditionalOccurrences": boolean,
       "CustomDataIdentifiers": {
        "Detections": [{
         "Arn": "string",
         "Count": integer,
         "Name": "string",
         "Occurrences": {
          "Cells": [{
           "CellReference": "string",
           "Column": integer,
           "ColumnName": "string",
           "Row": integer
          }],
          "LineRanges": [{
           "End": integer,
           "Start": integer,
           "StartColumn": integer
          }],
          "OffsetRanges": [{
           "End": integer,
```

```
            "Start": integer,
            "StartColumn": integer
          }],
          "Pages": [{
            "LineRange": {
              "End": integer,
              "Start": integer,
              "StartColumn": integer
            },
            "OffsetRange": {
              "End": integer,
              "Start": integer,
              "StartColumn": integer
            },
            "PageNumber": integer
          }],
          "Records": [{
            "JsonPath": "string",
            "RecordIndex": integer
          }]
        }
      }],
      "TotalCount": integer
    },
    "MimeType": "string",
    "SensitiveData": [{
      "Category": "string",
      "Detections": [{
        "Count": integer,
        "Occurrences": {
          "Cells": [{
            "CellReference": "string",
            "Column": integer,
            "ColumnName": "string",
            "Row": integer
          }],
          "LineRanges": [{
            "End": integer,
            "Start": integer,
            "StartColumn": integer
          }],
          "OffsetRanges": [{
            "End": integer,
            "Start": integer,
```

```
            "StartColumn": integer
           }],
           "Pages": [{
            "LineRange": {
             "End": integer,
             "Start": integer,
             "StartColumn": integer
            },
            "OffsetRange": {
             "End": integer,
             "Start": integer,
             "StartColumn": integer
            },
            "PageNumber": integer
           }],
           "Records": [{
            "JsonPath": "string",
            "RecordIndex": integer
           }]
          },
          "Type": "string"
         }],
         "TotalCount": integer
        }],
        "SizeClassified": integer,
        "Status": {
         "Code": "string",
         "Reason": "string"
        }
       }
      },
      "Details": {
       "AwsAmazonMQBroker": {
        "AutoMinorVersionUpgrade": boolean,
        "BrokerArn": "string",
        "BrokerId": "string",
        "BrokerName": "string",
        "Configuration": {
         "Id": "string",
         "Revision": integer
        },
        "DeploymentMode": "string",
        "EncryptionOptions": {
         "UseAwsOwnedKey": boolean
```

```
        },
        "EngineType": "string",
        "EngineVersion": "string",
        "HostInstanceType": "string",
        "Logs": {
         "Audit": boolean,
         "AuditLogGroup": "string",
         "General": boolean,
         "GeneralLogGroup": "string"
        },
        "MaintenanceWindowStartTime": {
         "DayOfWeek": "string",
         "TimeOfDay": "string",
         "TimeZone": "string"
        },
        "PubliclyAccessible": boolean,
        "SecurityGroups": [
         "string"
        ],
        "StorageType": "string",
        "SubnetIds": [
         "string",
         "string"
        ],
        "Users": [{
         "Username": "string"
        }]
       },
       "AwsApiGatewayRestApi": {
        "ApiKeySource": "string",
        "BinaryMediaTypes": [" string"],
        "CreatedDate": "string",
        "Description": "string",
        "EndpointConfiguration": {
         "Types": ["string"]
        },
        "Id": "string",
        "MinimumCompressionSize": number,
        "Name": "string",
        "Version": "string"
       },
       "AwsApiGatewayStage": {
        "AccessLogSettings": {
         "DestinationArn": "string",
```

```
          "Format": "string"
         },
         "CacheClusterEnabled": boolean,
         "CacheClusterSize": "string",
         "CacheClusterStatus": "string",
         "CanarySettings": {
          "DeploymentId": "string",
          "PercentTraffic": number,
          "StageVariableOverrides": [{
           "string": "string"
          }],
          "UseStageCache": boolean
         },
         "ClientCertificateId": "string",
         "CreatedDate": "string",
         "DeploymentId": "string",
         "Description": "string",
         "DocumentationVersion": "string",
         "LastUpdatedDate": "string",
         "MethodSettings": [{
          "CacheDataEncrypted": boolean,
          "CachingEnabled": boolean,
          "CacheTtlInSeconds": number,
          "DataTraceEnabled": boolean,
          "HttpMethod": "string",
          "LoggingLevel": "string",
          "MetricsEnabled": boolean,
          "RequireAuthorizationForCacheControl": boolean,
          "ResourcePath": "string",
          "ThrottlingBurstLimit": number,
          "ThrottlingRateLimit": number,
          "UnauthorizedCacheControlHeaderStrategy": "string"
         }],
         "StageName": "string",
         "TracingEnabled": boolean,
         "Variables": {
          "string": "string"
         },
         "WebAclArn": "string"
        },
        "AwsApiGatewayV2Api": {
         "ApiEndpoint": "string",
         "ApiId": "string",
         "ApiKeySelectionExpression": "string",
```

```
        "CorsConfiguration": {
         "AllowCredentials": boolean,
         "AllowHeaders": ["string"],
         "AllowMethods": ["string"],
         "AllowOrigins": ["string"],
         "ExposeHeaders": ["string"],
         "MaxAge": number
        },
        "CreatedDate": "string",
        "Description": "string",
        "Name": "string",
        "ProtocolType": "string",
        "RouteSelectionExpression": "string",
        "Version": "string"
       },
       "AwsApiGatewayV2Stage": {
        "AccessLogSettings": {
         "DestinationArn": "string",
         "Format": "string"
        },
        "ApiGatewayManaged": boolean,
        "AutoDeploy": boolean,
        "ClientCertificateId": "string",
        "CreatedDate": "string",
        "DefaultRouteSettings": {
         "DataTraceEnabled": boolean,
         "DetailedMetricsEnabled": boolean,
         "LoggingLevel": "string",
         "ThrottlingBurstLimit": number,
         "ThrottlingRateLimit": number
        },
        "DeploymentId": "string",
        "Description": "string",
        "LastDeploymentStatusMessage": "string",
        "LastUpdatedDate": "string",
        "RouteSettings": {
         "DetailedMetricsEnabled": boolean,
         "LoggingLevel": "string",
         "DataTraceEnabled": boolean,
         "ThrottlingBurstLimit": number,
         "ThrottlingRateLimit": number
        },
        "StageName": "string",
        "StageVariables": [{
```

```
          "string": "string"
         }]
        },
        "AwsAppSyncGraphQLApi": {
         "AwsAppSyncGraphQlApi": {
          "AdditionalAuthenticationProviders": [
          {
           "AuthenticationType": "string",
           "LambdaAuthorizerConfig": {
            "AuthorizerResultTtlInSeconds": integer,
            "AuthorizerUri": "string"
           }
          },
          {
           "AuthenticationType": "string"
          }
          ],
          "ApiId": "string",
          "Arn": "string",
          "AuthenticationType": "string",
          "Id": "string",
          "LogConfig": {
           "CloudWatchLogsRoleArn": "string",
           "ExcludeVerboseContent": boolean,
           "FieldLogLevel": "string"
          },
          "Name": "string",
          "XrayEnabled": boolean
         }
        },
        "AwsAthenaWorkGroup": {
         "Description": "string",
         "Name": "string",
         "WorkgroupConfiguration": {
          "ResultConfiguration": {
           "EncryptionConfiguration": {
            "EncryptionOption": "string",
            "KmsKey": "string"
           }
          }
         },
         "State": "string"
        },
        "AwsAutoScalingAutoScalingGroup": {
```

```
        "AvailabilityZones": [{
         "Value": "string"
        }],
        "CreatedTime": "string",
        "HealthCheckGracePeriod": integer,
        "HealthCheckType": "string",
        "LaunchConfigurationName": "string",
        "LoadBalancerNames": ["string"],
        "LaunchTemplate": {
                        "LaunchTemplateId": "string",
                        "LaunchTemplateName": "string",
                        "Version": "string"
                    },
        "MixedInstancesPolicy": {
         "InstancesDistribution": {
          "OnDemandAllocationStrategy": "string",
          "OnDemandBaseCapacity": number,
          "OnDemandPercentageAboveBaseCapacity": number,
          "SpotAllocationStrategy": "string",
          "SpotInstancePools": number,
          "SpotMaxPrice": "string"
         },
         "LaunchTemplate": {
          "LaunchTemplateSpecification": {
           "LaunchTemplateId": "string",
           "LaunchTemplateName": "string",
           "Version": "string"
          },
          "CapacityRebalance": boolean,
          "Overrides": [{
           "InstanceType": "string",
           "WeightedCapacity": "string"
          }]
         }
        }
       },
       "AwsAutoScalingLaunchConfiguration": {
        "AssociatePublicIpAddress": boolean,
        "BlockDeviceMappings": [{
         "DeviceName": "string",
         "Ebs": {
          "DeleteOnTermination": boolean,
          "Encrypted": boolean,
          "Iops": number,
```

```
          "SnapshotId": "string",
          "VolumeSize": number,
          "VolumeType": "string"
         },
         "NoDevice": boolean,
         "VirtualName": "string"
        }],
        "ClassicLinkVpcId": "string",
        "ClassicLinkVpcSecurityGroups": ["string"],
        "CreatedTime": "string",
        "EbsOptimized": boolean,
        "IamInstanceProfile": "string"
       },
       "ImageId": "string",
       "InstanceMonitoring": {
        "Enabled": boolean
       },
       "InstanceType": "string",
       "KernelId": "string",
       "KeyName": "string",
       "LaunchConfigurationName": "string",
       "MetadataOptions": {
        "HttpEndPoint": "string",
        "HttpPutReponseHopLimit": number,
        "HttpTokens": "string"
       },
       "PlacementTenancy": "string",
       "RamdiskId": "string",
       "SecurityGroups": ["string"],
       "SpotPrice": "string",
       "UserData": "string"
      },
      "AwsBackupBackupPlan": {
       "BackupPlan": {
        "AdvancedBackupSettings": [{
         "BackupOptions": {
          "WindowsVSS":"string"
         },
         "ResourceType":"string"
        }],
        "BackupPlanName": "string",
        "BackupPlanRule": [{
         "CompletionWindowMinutes": integer,
         "CopyActions": [{
```

```
          "DestinationBackupVaultArn": "string",
          "Lifecycle": {
           "DeleteAfterDays": integer,
           "MoveToColdStorageAfterDays": integer
          }
         }],
         "Lifecycle": {
          "DeleteAfterDays": integer
         },
         "RuleName": "string",
         "ScheduleExpression": "string",
         "StartWindowMinutes": integer,
         "TargetBackupVault": "string"
        }]
       },
       "BackupPlanArn": "string",
       "BackupPlanId": "string",
       "VersionId": "string"
      },
      "AwsBackupBackupVault": {
       "AccessPolicy": {
        "Statement": [{
         "Action": ["string"],
         "Effect": "string",
         "Principal": {
          "AWS": "string"
         },
         "Resource": "string"
        }],
        "Version": "string"
       },
       "BackupVaultArn": "string",
       "BackupVaultName": "string",
       "EncryptionKeyArn": "string",
       "Notifications": {
        "BackupVaultEvents": ["string"],
        "SNSTopicArn": "string"
       }
      },
      "AwsBackupRecoveryPoint": {
       "BackupSizeInBytes": integer,
       "BackupVaultName": "string",
       "BackupVaultArn": "string",
       "CalculatedLifecycle": {
```

```
          "DeleteAt": "string",
          "MoveToColdStorageAt": "string"
        },
        "CompletionDate": "string",
        "CreatedBy": {
          "BackupPlanArn": "string",
          "BackupPlanId": "string",
          "BackupPlanVersion": "string",
          "BackupRuleId": "string"
        },
        "CreationDate": "string",
        "EncryptionKeyArn": "string",
        "IamRoleArn": "string",
        "IsEncrypted": boolean,
        "LastRestoreTime": "string",
        "Lifecycle": {
          "DeleteAfterDays": integer,
          "MoveToColdStorageAfterDays": integer
        },
        "RecoveryPointArn": "string",
        "ResourceArn": "string",
        "ResourceType": "string",
        "SourceBackupVaultArn": "string",
        "Status": "string",
        "StatusMessage": "string",
        "StorageClass": "string"
      },
      "AwsCertificateManagerCertificate": {
        "CertificateAuthorityArn": "string",
        "CreatedAt": "string",
        "DomainName": "string",
        "DomainValidationOptions": [{
          "DomainName": "string",
          "ResourceRecord": {
            "Name": "string",
            "Type": "string",
            "Value": "string"
          },
          "ValidationDomain": "string",
          "ValidationEmails": ["string"],
          "ValidationMethod": "string",
          "ValidationStatus": "string"
        }],
        "ExtendedKeyUsages": [{
```

```
          "Name": "string",
          "OId": "string"
        }],
        "FailureReason": "string",
        "ImportedAt": "string",
        "InUseBy": ["string"],
        "IssuedAt": "string",
        "Issuer": "string",
        "KeyAlgorithm": "string",
        "KeyUsages": [{
          "Name": "string"
        }],
        "NotAfter": "string",
        "NotBefore": "string",
        "Options": {
          "CertificateTransparencyLoggingPreference": "string"
        },
        "RenewalEligibility": "string",
        "RenewalSummary": {
          "DomainValidationOptions": [{
            "DomainName": "string",
            "ResourceRecord": {
              "Name": "string",
              "Type": "string",
              "Value": "string"
            },
            "ValidationDomain": "string",
            "ValidationEmails": ["string"],
            "ValidationMethod": "string",
            "ValidationStatus": "string"
          }],
          "RenewalStatus": "string",
          "RenewalStatusReason": "string",
          "UpdatedAt": "string"
        },
        "Serial": "string",
        "SignatureAlgorithm": "string",
        "Status": "string",
        "Subject": "string",
        "SubjectAlternativeNames": ["string"],
        "Type": "string"
      },
      "AwsCloudFormationStack": {
        "Capabilities": ["string"],
```

```
        "CreationTime": "string",
        "Description": "string",
        "DisableRollback": boolean,
        "DriftInformation": {
         "StackDriftStatus": "string"
        },
        "EnableTerminationProtection": boolean,
        "LastUpdatedTime": "string",
        "NotificationArns": ["string"],
        "Outputs": [{
         "Description": "string",
         "OutputKey": "string",
         "OutputValue": "string"
        }],
        "RoleArn": "string",
        "StackId": "string",
        "StackName": "string",
        "StackStatus": "string",
        "StackStatusReason": "string",
        "TimeoutInMinutes": number
       },
       "AwsCloudFrontDistribution": {
        "CacheBehaviors": {
         "Items": [{
          "ViewerProtocolPolicy": "string"
         }]
        },
        "DefaultCacheBehavior": {
         "ViewerProtocolPolicy": "string"
        },
        "DefaultRootObject": "string",
        "DomainName": "string",
        "Etag": "string",
        "LastModifiedTime": "string",
        "Logging": {
         "Bucket": "string",
         "Enabled": boolean,
         "IncludeCookies": boolean,
         "Prefix": "string"
        },
        "OriginGroups": {
         "Items": [{
          "FailoverCriteria": {
           "StatusCodes": {
```

```
            "Items": [number],
            "Quantity": number
           }
          }
         }]
        },
        "Origins": {
         "Items": [{
          "CustomOriginConfig": {
           "HttpPort": number,
           "HttpsPort": number,
           "OriginKeepaliveTimeout": number,
           "OriginProtocolPolicy": "string",
           "OriginReadTimeout": number,
           "OriginSslProtocols": {
            "Items": ["string"],
            "Quantity": number
           }
          },
          "DomainName": "string",
          "Id": "string",
          "OriginPath": "string",
          "S3OriginConfig": {
           "OriginAccessIdentity": "string"
          }
         }]
        },
        "Status": "string",
        "ViewerCertificate": {
         "AcmCertificateArn": "string",
         "Certificate": "string",
         "CertificateSource": "string",
         "CloudFrontDefaultCertificate": boolean,
         "IamCertificateId": "string",
         "MinimumProtocolVersion": "string",
         "SslSupportMethod": "string"
        },
        "WebAclId": "string"
       },
       "AwsCloudTrailTrail": {
        "CloudWatchLogsLogGroupArn": "string",
        "CloudWatchLogsRoleArn": "string",
        "HasCustomEventSelectors": boolean,
        "HomeRegion": "string",
```

```
        "IncludeGlobalServiceEvents": boolean,
        "IsMultiRegionTrail": boolean,
        "IsOrganizationTrail": boolean,
        "KmsKeyId": "string",
        "LogFileValidationEnabled": boolean,
        "Name": "string",
        "S3BucketName": "string",
        "S3KeyPrefix": "string",
        "SnsTopicArn": "string",
        "SnsTopicName": "string",
        "TrailArn": "string"
      },
      "AwsCloudWatchAlarm": {
        "ActionsEnabled": boolean,
        "AlarmActions": ["string"],
        "AlarmArn": "string",
        "AlarmConfigurationUpdatedTimestamp": "string",
        "AlarmDescription": "string",
        "AlarmName": "string",
        "ComparisonOperator": "string",
        "DatapointsToAlarm": number,
        "Dimensions": [{
          "Name": "string",
          "Value": "string"
        }],
        "EvaluateLowSampleCountPercentile": "string",
        "EvaluationPeriods": number,
        "ExtendedStatistic": "string",
        "InsufficientDataActions": ["string"],
        "MetricName": "string",
        "Namespace": "string",
        "OkActions": ["string"],
        "Period": number,
        "Statistic": "string",
        "Threshold": number,
        "ThresholdMetricId": "string",
        "TreatMissingData": "string",
        "Unit": "string"
      },
      "AwsCodeBuildProject": {
        "Artifacts": [{
          "ArtifactIdentifier": "string",
          "EncryptionDisabled": boolean,
          "Location": "string",
```

```
         "Name": "string",
         "NamespaceType": "string",
         "OverrideArtifactName": boolean,
         "Packaging": "string",
         "Path": "string",
         "Type": "string"
        }],
        "SecondaryArtifacts": [{
                    "ArtifactIdentifier": "string",
                    "Type": "string",
                    "Location": "string",
                    "Name": "string",
                    "NamespaceType": "string",
                    "Packaging": "string",
                    "Path": "string",
                    "EncryptionDisabled": boolean,
                    "OverrideArtifactName": boolean
                 }],
        "EncryptionKey": "string",
        "Certificate": "string",
        "Environment": {
         "Certificate": "string",
         "EnvironmentVariables": [{
          "Name": "string",
          "Type": "string",
          "Value": "string"
         }],
         "ImagePullCredentialsType": "string",
         "PrivilegedMode": boolean,
         "RegistryCredential": {
          "Credential": "string",
          "CredentialProvider": "string"
         },
         "Type": "string"
        },
        "LogsConfig": {
         "CloudWatchLogs": {
          "GroupName": "string",
          "Status": "string",
          "StreamName": "string"
         },
         "S3Logs": {
          "EncryptionDisabled": boolean,
          "Location": "string",
```

```
          "Status": "string"
         }
        },
        "Name": "string",
        "ServiceRole": "string",
        "Source": {
         "Type": "string",
         "Location": "string",
         "GitCloneDepth": integer
        },
        "VpcConfig": {
         "VpcId": "string",
         "Subnets": ["string"],
         "SecurityGroupIds": ["string"]
        }
       },
       "AwsDmsEndpoint": {
        "CertificateArn": "string",
        "DatabaseName": "string",
        "EndpointArn": "string",
        "EndpointIdentifier": "string",
        "EndpointType": "string",
        "EngineName": "string",
        "KmsKeyId": "string",
        "Port": integer,
        "ServerName": "string",
        "SslMode": "string",
        "Username": "string"
       },
       "AwsDmsReplicationInstance": {
        "AllocatedStorage": integer,
        "AutoMinorVersionUpgrade": boolean,
        "AvailabilityZone": "string",
        "EngineVersion": "string",
        "KmsKeyId": "string",
        "MultiAZ": boolean,
        "PreferredMaintenanceWindow": "string",
        "PubliclyAccessible": boolean,
        "ReplicationInstanceClass": "string",
        "ReplicationInstanceIdentifier": "string",
        "ReplicationSubnetGroup": {
            "ReplicationSubnetGroupIdentifier": "string"
        },
        "VpcSecurityGroups": [
```

```
            {
                "VpcSecurityGroupId": "string"
            }
        ]
      },
      "AwsDmsReplicationTask": {
        "CdcStartPosition": "string",
        "Id": "string",
        "MigrationType": "string",
        "ReplicationInstanceArn": "string",
        "ReplicationTaskIdentifier": "string",
        "ReplicationTaskSettings": {
          "string": "string"
        },
        "SourceEndpointArn": "string",
        "TableMappings": {
          "string": "string"
        },
        "TargetEndpointArn": "string"
      },
      "AwsDynamoDbTable": {
        "AttributeDefinitions": [{
          "AttributeName": "string",
          "AttributeType": "string"
        }],
        "BillingModeSummary": {
          "BillingMode": "string",
          "LastUpdateToPayPerRequestDateTime": "string"
        },
        "CreationDateTime": "string",
        "DeletionProtectionEnabled": boolean,
        "GlobalSecondaryIndexes": [{
          "Backfilling": boolean,
          "IndexArn": "string",
          "IndexName": "string",
          "IndexSizeBytes": number,
          "IndexStatus": "string",
          "ItemCount": number,
          "KeySchema": [{
            "AttributeName": "string",
            "KeyType": "string"
          }],
          "Projection": {
            "NonKeyAttributes": ["string"],
```

```
          "ProjectionType": "string"
         },
         "ProvisionedThroughput": {
          "LastDecreaseDateTime": "string",
          "LastIncreaseDateTime": "string",
          "NumberOfDecreasesToday": number,
          "ReadCapacityUnits": number,
          "WriteCapacityUnits": number
         }
        }],
        "GlobalTableVersion": "string",
        "ItemCount": number,
        "KeySchema": [{
         "AttributeName": "string",
         "KeyType": "string"
        }],
        "LatestStreamArn": "string",
        "LatestStreamLabel": "string",
        "LocalSecondaryIndexes": [{
         "IndexArn": "string",
         "IndexName": "string",
         "KeySchema": [{
          "AttributeName": "string",
          "KeyType": "string"
         }],
         "Projection": {
          "NonKeyAttributes": ["string"],
          "ProjectionType": "string"
         }
        }],
        "ProvisionedThroughput": {
         "LastDecreaseDateTime": "string",
         "LastIncreaseDateTime": "string",
         "NumberOfDecreasesToday": number,
         "ReadCapacityUnits": number,
         "WriteCapacityUnits": number
        },
        "Replicas": [{
         "GlobalSecondaryIndexes": [{
          "IndexName": "string",
          "ProvisionedThroughputOverride": {
           "ReadCapacityUnits": number
          }
         }],
```

```
          "KmsMasterKeyId": "string",
          "ProvisionedThroughputOverride": {
           "ReadCapacityUnits": number
          },
          "RegionName": "string",
          "ReplicaStatus": "string",
          "ReplicaStatusDescription": "string"
         }],
         "RestoreSummary": {
          "RestoreDateTime": "string",
          "RestoreInProgress": boolean,
          "SourceBackupArn": "string",
          "SourceTableArn": "string"
         },
         "SseDescription": {
          "InaccessibleEncryptionDateTime": "string",
          "KmsMasterKeyArn": "string",
          "SseType": "string",
          "Status": "string"
         },
         "StreamSpecification": {
          "StreamEnabled": boolean,
          "StreamViewType": "string"
         },
         "TableId": "string",
         "TableName": "string",
         "TableSizeBytes": number,
         "TableStatus": "string"
        },
        "AwsEc2ClientVpnEndpoint": {
         "AuthenticationOptions": [
          {
           "MutualAuthentication": {
            "ClientRootCertificateChainArn": "string"
           },
           "Type": "string"
          }
         ],
         "ClientCidrBlock": "string",
         "ClientConnectOptions": {
          "Enabled": boolean
         },
         "ClientLoginBannerOptions": {
          "Enabled": boolean
```

```
        },
        "ClientVpnEndpointId": "string",
        "ConnectionLogOptions": {
         "Enabled": boolean
        },
        "Description": "string",
        "DnsServer": ["string"],
        "ServerCertificateArn": "string",
        "SecurityGroupIdSet": [
         "string"
        ],
        "SelfServicePortalUrl": "string",
        "SessionTimeoutHours": "integer",
        "SplitTunnel": boolean,
        "TransportProtocol": "string",
        "VpcId": "string",
        "VpnPort": integer
       },
       "AwsEc2Eip": {
        "AllocationId": "string",
        "AssociationId": "string",
        "Domain": "string",
        "InstanceId": "string",
        "NetworkBorderGroup": "string",
        "NetworkInterfaceId": "string",
        "NetworkInterfaceOwnerId": "string",
        "PrivateIpAddress": "string",
        "PublicIp": "string",
        "PublicIpv4Pool": "string"
       },
       "AwsEc2Instance": {
        "IamInstanceProfileArn": "string",
        "ImageId": "string",
        "IpV4Addresses": ["string"],
        "IpV6Addresses": ["string"],
        "KeyName": "string",
        "LaunchedAt": "string",
        "MetadataOptions": {
         "HttpEndpoint": "string",
         "HttpProtocolIpv6": "string",
         "HttpPutResponseHopLimit": number,
         "HttpTokens": "string",
         "InstanceMetadataTags": "string"
        },
```

```
        "Monitoring": {
         "State": "string"
        },
        "NetworkInterfaces": [{
         "NetworkInterfaceId": "string"
        }],
        "SubnetId": "string",
        "Type": "string",
        "VirtualizationType": "string",
        "VpcId": "string"
       },
       "AwsEc2LaunchTemplate": {
        "DefaultVersionNumber": "string",
        "ElasticGpuSpecifications": ["string"],
        "ElasticInferenceAccelerators": ["string"],
        "Id": "string",
        "ImageId": "string",
        "LatestVersionNumber": "string",
        "LaunchTemplateData": {
         "BlockDeviceMappings": [{
          "DeviceName": "string",
          "Ebs": {
           "DeleteonTermination": boolean,
           "Encrypted": boolean,
           "SnapshotId": "string",
           "VolumeSize": number,
           "VolumeType": "string"
          }
         }],
         "MetadataOptions": {
          "HttpTokens": "string",
          "HttpPutResponseHopLimit" : number
         },
         "Monitoring": {
          "Enabled": boolean
         },
         "NetworkInterfaces": [{
          "AssociatePublicIpAddress" : boolean
         }]
        },
        "LaunchTemplateName": "string",
        "LicenseSpecifications": ["string"],
        "SecurityGroupIds": ["string"],
        "SecurityGroups": ["string"],
```

```
        "TagSpecifications": ["string"]
      },
      "AwsEc2NetworkAcl": {
        "Associations": [{
          "NetworkAclAssociationId": "string",
          "NetworkAclId": "string",
          "SubnetId": "string"
        }],
        "Entries": [{
          "CidrBlock": "string",
          "Egress": boolean,
          "IcmpTypeCode": {
            "Code": number,
            "Type": number
          },
          "Ipv6CidrBlock": "string",
          "PortRange": {
            "From": number,
            "To": number
          },
          "Protocol": "string",
          "RuleAction": "string",
          "RuleNumber": number
        }],
        "IsDefault": boolean,
        "NetworkAclId": "string",
        "OwnerId": "string",
        "VpcId": "string"
      },
      "AwsEc2NetworkInterface": {
        "Attachment": {
          "AttachmentId": "string",
          "AttachTime": "string",
          "DeleteOnTermination": boolean,
          "DeviceIndex": number,
          "InstanceId": "string",
          "InstanceOwnerId": "string",
          "Status": "string"
        },
        "Ipv6Addresses": [{
          "Ipv6Address": "string"
        }],
        "NetworkInterfaceId": "string",
        "PrivateIpAddresses": [{
```

```
          "PrivateDnsName": "string",
          "PrivateIpAddress": "string"
        }],
        "PublicDnsName": "string",
        "PublicIp": "string",
        "SecurityGroups": [{
          "GroupId": "string",
          "GroupName": "string"
        }],
        "SourceDestCheck": boolean
      },
      "AwsEc2RouteTable": {
        "AssociationSet": [{
          "AssociationState": {
            "State": "string"
          },
          "Main": boolean,
          "RouteTableAssociationId": "string",
          "RouteTableId": "string"
        }],
        "PropogatingVgwSet": [],
        "RouteTableId": "string",
        "RouteSet": [
          {
            "DestinationCidrBlock": "string",
            "GatewayId": "string",
            "Origin": "string",
            "State": "string"
          },
          {
            "DestinationCidrBlock": "string",
            "GatewayId": "string",
            "Origin": "string",
            "State": "string"
          }
        ],
        "VpcId": "string"
      },
      "AwsEc2SecurityGroup": {
        "GroupId": "string",
        "GroupName": "string",
        "IpPermissions": [{
          "FromPort": number,
          "IpProtocol": "string",
```

```
        "IpRanges": [{
         "CidrIp": "string"
        }],
        "Ipv6Ranges": [{
         "CidrIpv6": "string"
        }],
        "PrefixListIds": [{
         "PrefixListId": "string"
        }],
        "ToPort": number,
        "UserIdGroupPairs": [{
         "GroupId": "string",
         "GroupName": "string",
         "PeeringStatus": "string",
         "UserId": "string",
         "VpcId": "string",
         "VpcPeeringConnectionId": "string"
        }]
       }],
       "IpPermissionsEgress": [{
        "FromPort": number,
        "IpProtocol": "string",
        "IpRanges": [{
         "CidrIp": "string"
        }],
        "Ipv6Ranges": [{
         "CidrIpv6": "string"
        }],
        "PrefixListIds": [{
         "PrefixListId": "string"
        }],
        "ToPort": number,
        "UserIdGroupPairs": [{
         "GroupId": "string",
         "GroupName": "string",
         "PeeringStatus": "string",
         "UserId": "string",
         "VpcId": "string",
         "VpcPeeringConnectionId": "string"
        }]
       }],
       "OwnerId": "string",
       "VpcId": "string"
      },
```

```
      "AwsEc2Subnet": {
       "AssignIpv6AddressOnCreation": boolean,
       "AvailabilityZone": "string",
       "AvailabilityZoneId": "string",
       "AvailableIpAddressCount": number,
       "CidrBlock": "string",
       "DefaultForAz": boolean,
       "Ipv6CidrBlockAssociationSet": [{
        "AssociationId": "string",
        "Ipv6CidrBlock": "string",
        "CidrBlockState": "string"
       }],
       "MapPublicIpOnLaunch": boolean,
       "OwnerId": "string",
       "State": "string",
       "SubnetArn": "string",
       "SubnetId": "string",
       "VpcId": "string"
      },
      "AwsEc2TransitGateway": {
       "AmazonSideAsn": number,
       "AssociationDefaultRouteTableId": "string",
       "AutoAcceptSharedAttachments": "string",
       "DefaultRouteTableAssociation": "string",
       "DefaultRouteTablePropagation": "string",
       "Description": "string",
       "DnsSupport": "string",
       "Id": "string",
       "MulticastSupport": "string",
       "PropagationDefaultRouteTableId": "string",
       "TransitGatewayCidrBlocks": ["string"],
       "VpnEcmpSupport": "string"
      },
      "AwsEc2Volume": {
       "Attachments": [{
        "AttachTime": "string",
        "DeleteOnTermination": boolean,
        "InstanceId": "string",
        "Status": "string"
       }],
       "CreateTime": "string",
       "DeviceName": "string",
       "Encrypted": boolean,
       "KmsKeyId": "string",
```

```
        "Size": number,
        "SnapshotId": "string",
        "Status": "string",
        "VolumeId": "string",
        "VolumeScanStatus": "string",
        "VolumeType": "string"
      },
      "AwsEc2Vpc": {
        "CidrBlockAssociationSet": [{
          "AssociationId": "string",
          "CidrBlock": "string",
          "CidrBlockState": "string"
        }],
        "DhcpOptionsId": "string",
        "Ipv6CidrBlockAssociationSet": [{
          "AssociationId": "string",
          "CidrBlockState": "string",
          "Ipv6CidrBlock": "string"
        }],
        "State": "string"
      },
      "AwsEc2VpcEndpointService": {
        "AcceptanceRequired": boolean,
        "AvailabilityZones": ["string"],
        "BaseEndpointDnsNames": ["string"],
        "ManagesVpcEndpoints": boolean,
        "GatewayLoadBalancerArns": ["string"],
        "NetworkLoadBalancerArns": ["string"],
        "PrivateDnsName": "string",
        "ServiceId": "string",
        "ServiceName": "string",
        "ServiceState": "string",
        "ServiceType": [{
          "ServiceType": "string"
        }]
      },
      "AwsEc2VpcPeeringConnection": {
        "AccepterVpcInfo": {
          "CidrBlock": "string",
          "CidrBlockSet": [{
            "CidrBlock": "string"
          }],
          "Ipv6CidrBlockSet": [{
            "Ipv6CidrBlock": "string"
```

```
        }],
        "OwnerId": "string",
        "PeeringOptions": {
         "AllowDnsResolutionFromRemoteVpc": boolean,
         "AllowEgressFromLocalClassicLinkToRemoteVpc": boolean,
         "AllowEgressFromLocalVpcToRemoteClassicLink": boolean
        },
        "Region": "string",
        "VpcId": "string"
       },
       "ExpirationTime": "string",
       "RequesterVpcInfo": {
        "CidrBlock": "string",
        "CidrBlockSet": [{
         "CidrBlock": "string"
        }],
        "Ipv6CidrBlockSet": [{
         "Ipv6CidrBlock": "string"
        }],
        "OwnerId": "string",
        "PeeringOptions": {
         "AllowDnsResolutionFromRemoteVpc": boolean,
         "AllowEgressFromLocalClassicLinkToRemoteVpc": boolean,
         "AllowEgressFromLocalVpcToRemoteClassicLink": boolean
        },
        "Region": "string",
        "VpcId": "string"
       },
       "Status": {
        "Code": "string",
        "Message": "string"
       },
       "VpcPeeringConnectionId": "string"
      },
      "AwsEcrContainerImage": {
       "Architecture": "string",
       "ImageDigest": "string",
       "ImagePublishedAt": "string",
       "ImageTags": ["string"],
       "RegistryId": "string",
       "RepositoryName": "string"
      },
      "AwsEcrRepository": {
       "Arn": "string",
```

```
        "ImageScanningConfiguration": {
         "ScanOnPush": boolean
        },
        "ImageTagMutability": "string",
        "LifecyclePolicy": {
         "LifecyclePolicyText": "string",
         "RegistryId": "string"
        },
        "RepositoryName": "string",
        "RepositoryPolicyText": "string"
       },
       "AwsEcsCluster": {
        "ActiveServicesCount": number,
        "CapacityProviders": ["string"],
        "ClusterArn": "string",
        "ClusterName": "string",
        "ClusterSettings": [{
         "Name": "string",
         "Value": "string"
        }],
        "Configuration": {
         "ExecuteCommandConfiguration": {
          "KmsKeyId": "string",
          "LogConfiguration": {
           "CloudWatchEncryptionEnabled": boolean,
           "CloudWatchLogGroupName": "string",
           "S3BucketName": "string",
           "S3EncryptionEnabled": boolean,
           "S3KeyPrefix": "string"
          },
          "Logging": "string"
         }
        },
        "DefaultCapacityProviderStrategy": [{
         "Base": number,
         "CapacityProvider": "string",
         "Weight": number
        }],
        "RegisteredContainerInstancesCount": number,
        "RunningTasksCount": number,
        "Status": "string"
       },
       "AwsEcsContainer": {
        "Image": "string",
```

```
        "MountPoints": [{
         "ContainerPath": "string",
         "SourceVolume": "string"
        }],
        "Name": "string",
        "Privileged": boolean
       },
       "AwsEcsService": {
        "CapacityProviderStrategy": [{
         "Base": number,
         "CapacityProvider": "string",
         "Weight": number
        }],
        "Cluster": "string",
        "DeploymentConfiguration": {
         "DeploymentCircuitBreaker": {
          "Enable": boolean,
          "Rollback": boolean
         },
         "MaximumPercent": number,
         "MinimumHealthyPercent": number
        },
        "DeploymentController": {
         "Type": "string"
        },
        "DesiredCount": number,
        "EnableEcsManagedTags": boolean,
        "EnableExecuteCommand": boolean,
        "HealthCheckGracePeriodSeconds": number,
        "LaunchType": "string",
        "LoadBalancers": [{
         "ContainerName": "string",
         "ContainerPort": number,
         "LoadBalancerName": "string",
         "TargetGroupArn": "string"
        }],
        "Name": "string",
        "NetworkConfiguration": {
         "AwsVpcConfiguration": {
          "AssignPublicIp": "string",
          "SecurityGroups": ["string"],
          "Subnets": ["string"]
         }
        },
```

```
        "PlacementConstraints": [{
         "Expression": "string",
         "Type": "string"
        }],
        "PlacementStrategies": [{
         "Field": "string",
         "Type": "string"
        }],
        "PlatformVersion": "string",
        "PropagateTags": "string",
        "Role": "string",
        "SchedulingStrategy": "string",
        "ServiceArn": "string",
        "ServiceName": "string",
        "ServiceRegistries": [{
         "ContainerName": "string",
         "ContainerPort": number,
         "Port": number,
         "RegistryArn": "string"
        }],
        "TaskDefinition": "string"
       },
       "AwsEcsTask": {
        "CreatedAt": "string",
        "ClusterArn": "string",
        "Group": "string",
        "StartedAt": "string",
        "StartedBy": "string",
        "TaskDefinitionArn": "string",
        "Version": number,
        "Volumes": [{
         "Name": "string",
         "Host": {
          "SourcePath": "string"
         }
        }],
        "Containers": [{
         "Image": "string",
         "MountPoints": [{
          "ContainerPath": "string",
          "SourceVolume": "string"
         }],
         "Name": "string",
         "Privileged": boolean
```

```
        }]
      },
      "AwsEcsTaskDefinition": {
       "ContainerDefinitions": [{
        "Command": ["string"],
        "Cpu": number,
        "DependsOn": [{
         "Condition": "string",
         "ContainerName": "string"
        }],
        "DisableNetworking": boolean,
        "DnsSearchDomains": ["string"],
        "DnsServers": ["string"],
        "DockerLabels": {
         "string": "string"
        },
        "DockerSecurityOptions": ["string"],
        "EntryPoint": ["string"],
        "Environment": [{
         "Name": "string",
         "Value": "string"
        }],
        "EnvironmentFiles": [{
         "Type": "string",
         "Value": "string"
        }],
        "Essential": boolean,
        "ExtraHosts": [{
         "Hostname": "string",
         "IpAddress": "string"
        }],
        "FirelensConfiguration": {
         "Options": {
          "string": "string"
         },
         "Type": "string"
        },
        "HealthCheck": {
         "Command": ["string"],
         "Interval": number,
         "Retries": number,
         "StartPeriod": number,
         "Timeout": number
        },
```

```
        "Hostname": "string",
        "Image": "string",
        "Interactive": boolean,
        "Links": ["string"],
        "LinuxParameters": {
         "Capabilities": {
          "Add": ["string"],
          "Drop": ["string"]
         },
         "Devices": [{
          "ContainerPath": "string",
          "HostPath": "string",
          "Permissions": ["string"]
         }],
         "InitProcessEnabled": boolean,
         "MaxSwap": number,
         "SharedMemorySize": number,
         "Swappiness": number,
         "Tmpfs": [{
          "ContainerPath": "string",
          "MountOptions": ["string"],
          "Size": number
         }]
        },
        "LogConfiguration": {
         "LogDriver": "string",
         "Options": {
          "string": "string"
         },
         "SecretOptions": [{
          "Name": "string",
          "ValueFrom": "string"
         }]
        },
        "Memory": number,
        "MemoryReservation": number,
        "MountPoints": [{
         "ContainerPath": "string",
         "ReadOnly": boolean,
         "SourceVolume": "string"
        }],
        "Name": "string",
        "PortMappings": [{
         "ContainerPort": number,
```

```
          "HostPort": number,
          "Protocol": "string"
         }],
         "Privileged": boolean,
         "PseudoTerminal": boolean,
         "ReadonlyRootFilesystem": boolean,
         "RepositoryCredentials": {
          "CredentialsParameter": "string"
         },
         "ResourceRequirements": [{
          "Type": "string",
          "Value": "string"
         }],
         "Secrets": [{
          "Name": "string",
          "ValueFrom": "string"
         }],
         "StartTimeout": number,
         "StopTimeout": number,
         "SystemControls": [{
          "Namespace": "string",
          "Value": "string"
         }],
         "Ulimits": [{
          "HardLimit": number,
          "Name": "string",
          "SoftLimit": number
         }],
         "User": "string",
         "VolumesFrom": [{
          "ReadOnly": boolean,
          "SourceContainer": "string"
         }],
         "WorkingDirectory": "string"
        }],
        "Cpu": "string",
        "ExecutionRoleArn": "string",
        "Family": "string",
        "InferenceAccelerators": [{
         "DeviceName": "string",
         "DeviceType": "string"
        }],
        "IpcMode": "string",
        "Memory": "string",
```

```
        "NetworkMode": "string",
        "PidMode": "string",
        "PlacementConstraints": [{
         "Expression": "string",
         "Type": "string"
        }],
        "ProxyConfiguration": {
         "ContainerName": "string",
         "ProxyConfigurationProperties": [{
          "Name": "string",
          "Value": "string"
         }],
         "Type": "string"
        },
        "RequiresCompatibilities": ["string"],
        "Status": "string",
        "TaskRoleArn": "string",
        "Volumes": [{
         "DockerVolumeConfiguration": {
          "Autoprovision": boolean,
          "Driver": "string",
          "DriverOpts": {
           "string": "string"
          },
          "Labels": {
           "string": "string"
          },
          "Scope": "string"
         },
         "EfsVolumeConfiguration": {
          "AuthorizationConfig": {
           "AccessPointId": "string",
           "Iam": "string"
          },
          "FilesystemId": "string",
          "RootDirectory": "string",
          "TransitEncryption": "string",
          "TransitEncryptionPort": number
         },
         "Host": {
          "SourcePath": "string"
         },
         "Name": "string"
        }]
```

```
      },
      "AwsEfsAccessPoint": {
       "AccessPointId": "string",
       "Arn": "string",
       "ClientToken": "string",
       "FileSystemId": "string",
       "PosixUser": {
        "Gid": "string",
        "SecondaryGids": ["string"],
        "Uid": "string"
       },
       "RootDirectory": {
        "CreationInfo": {
         "OwnerGid": "string",
         "OwnerUid": "string",
         "Permissions": "string"
        },
        "Path": "string"
       }
      },
      "AwsEksCluster": {
       "Arn": "string",
       "CertificateAuthorityData": "string",
       "ClusterStatus": "string",
       "Endpoint": "string",
       "Logging": {
        "ClusterLogging": [{
         "Enabled": boolean,
         "Types": ["string"]
        }]
       },
       "Name": "string",
       "ResourcesVpcConfig": {
        "EndpointPublicAccess": boolean,
        "SecurityGroupIds": ["string"],
        "SubnetIds": ["string"]
       },
       "RoleArn": "string",
       "Version": "string"
      },
      "AwsElasticBeanstalkEnvironment": {
       "ApplicationName": "string",
       "Cname": "string",
       "DateCreated": "string",
```

```
        "DateUpdated": "string",
        "Description": "string",
        "EndpointUrl": "string",
        "EnvironmentArn": "string",
        "EnvironmentId": "string",
        "EnvironmentLinks": [{
         "EnvironmentName": "string",
         "LinkName": "string"
        }],
        "EnvironmentName": "string",
        "OptionSettings": [{
         "Namespace": "string",
         "OptionName": "string",
         "ResourceName": "string",
         "Value": "string"
        }],
        "PlatformArn": "string",
        "SolutionStackName": "string",
        "Status": "string",
        "Tier": {
         "Name": "string",
         "Type": "string",
         "Version": "string"
        },
        "VersionLabel": "string"
       },
       "AwsElasticSearchDomain": {
        "AccessPolicies": "string",
        "DomainStatus": {
         "DomainId": "string",
         "DomainName": "string",
         "Endpoint": "string",
         "Endpoints": {
          "string": "string"
         }
        },
        "DomainEndpointOptions": {
         "EnforceHTTPS": boolean,
         "TLSSecurityPolicy": "string"
        },
        "ElasticsearchClusterConfig": {
         "DedicatedMasterCount": number,
         "DedicatedMasterEnabled": boolean,
         "DedicatedMasterType": "string",
```

```
          "InstanceCount": number,
          "InstanceType": "string",
          "ZoneAwarenessConfig": {
           "AvailabilityZoneCount": number
          },
          "ZoneAwarenessEnabled": boolean
         },
         "ElasticsearchVersion": "string",
         "EncryptionAtRestOptions": {
          "Enabled": boolean,
          "KmsKeyId": "string"
         },
         "LogPublishingOptions": {
          "AuditLogs": {
           "CloudWatchLogsLogGroupArn": "string",
           "Enabled": boolean
          },
          "IndexSlowLogs": {
           "CloudWatchLogsLogGroupArn": "string",
           "Enabled": boolean
          },
          "SearchSlowLogs": {
           "CloudWatchLogsLogGroupArn": "string",
           "Enabled": boolean
          }
         },
         "NodeToNodeEncryptionOptions": {
          "Enabled": boolean
         },
         "ServiceSoftwareOptions": {
          "AutomatedUpdateDate": "string",
          "Cancellable": boolean,
          "CurrentVersion": "string",
          "Description": "string",
          "NewVersion": "string",
          "UpdateAvailable": boolean,
          "UpdateStatus": "string"
         },
         "VPCOptions": {
          "AvailabilityZones": [
           "string"
          ],
          "SecurityGroupIds": [
           "string"
```

```
        ],
        "SubnetIds": [
         "string"
        ],
        "VPCId": "string"
       }
      },
      "AwsElbLoadBalancer": {
       "AvailabilityZones": ["string"],
       "BackendServerDescriptions": [{
        "InstancePort": number,
        "PolicyNames": ["string"]
       }],
       "CanonicalHostedZoneName": "string",
       "CanonicalHostedZoneNameID": "string",
       "CreatedTime": "string",
       "DnsName": "string",
       "HealthCheck": {
        "HealthyThreshold": number,
        "Interval": number,
        "Target": "string",
        "Timeout": number,
        "UnhealthyThreshold": number
       },
       "Instances": [{
        "InstanceId": "string"
       }],
       "ListenerDescriptions": [{
        "Listener": {
         "InstancePort": number,
         "InstanceProtocol": "string",
         "LoadBalancerPort": number,
         "Protocol": "string",
         "SslCertificateId": "string"
        },
        "PolicyNames": ["string"]
       }],
       "LoadBalancerAttributes": {
        "AccessLog": {
         "EmitInterval": number,
         "Enabled": boolean,
         "S3BucketName": "string",
         "S3BucketPrefix": "string"
        },
```

```
        "ConnectionDraining": {
         "Enabled": boolean,
         "Timeout": number
        },
        "ConnectionSettings": {
         "IdleTimeout": number
        },
        "CrossZoneLoadBalancing": {
         "Enabled": boolean
        },
        "AdditionalAttributes": [{
                        "Key": "string",
                        "Value": "string"
                    }]
       },
       "LoadBalancerName": "string",
       "Policies": {
        "AppCookieStickinessPolicies": [{
         "CookieName": "string",
         "PolicyName": "string"
        }],
        "LbCookieStickinessPolicies": [{
         "CookieExpirationPeriod": number,
         "PolicyName": "string"
        }],
        "OtherPolicies": ["string"]
       },
       "Scheme": "string",
       "SecurityGroups": ["string"],
       "SourceSecurityGroup": {
        "GroupName": "string",
        "OwnerAlias": "string"
       },
       "Subnets": ["string"],
       "VpcId": "string"
      },
      "AwsElbv2LoadBalancer": {
       "AvailabilityZones": {
        "SubnetId": "string",
        "ZoneName": "string"
       },
       "CanonicalHostedZoneId": "string",
       "CreatedTime": "string",
       "DNSName": "string",
```

```
        "IpAddressType": "string",
        "LoadBalancerAttributes": [{
         "Key": "string",
         "Value": "string"
        }],
        "Scheme": "string",
        "SecurityGroups": ["string"],
        "State": {
         "Code": "string",
         "Reason": "string"
        },
        "Type": "string",
        "VpcId": "string"
       },
       "AwsEventSchemasRegistry": {
        "Description": "string",
        "RegistryArn": "string",
        "RegistryName": "string"
       },
       "AwsEventsEndpoint": {
        "Arn": "string",
        "Description": "string",
        "EndpointId": "string",
        "EndpointUrl": "string",
        "EventBuses": [
            {
                "EventBusArn": "string"
            },
            {
                "EventBusArn": "string"
            }
        ],
        "Name": "string",
        "ReplicationConfig": {
            "State": "string"
        },
        "RoleArn": "string",
        "RoutingConfig": {
            "FailoverConfig": {
                "Primary": {
                    "HealthCheck": "string"
                },
                "Secondary": {
                    "Route": "string"
```

```
                }
            }
        },
        "State": "string"
      },
      "AwsEventsEventBus": {
        "Arn": "string",
        "Name": "string",
        "Policy": "string"
      },
      "AwsGuardDutyDetector": {
        "FindingPublishingFrequency": "string",
        "ServiceRole": "string",
        "Status": "string",
        "DataSources": {
          "CloudTrail": {
            "Status": "string"
          },
          "DnsLogs": {
            "Status": "string"
          },
          "FlowLogs": {
            "Status": "string"
          },
          "S3Logs": {
            "Status": "string"
          },
          "Kubernetes": {
            "AuditLogs": {
              "Status": "string"
            }
          },
          "MalwareProtection": {
            "ScanEc2InstanceWithFindings": {
              "EbsVolumes": {
                "Status": "string"
              }
            },
            "ServiceRole": "string"
          }
        }
      },
      "AwsIamAccessKey": {
        "AccessKeyId": "string",
```

```
        "AccountId": "string",
        "CreatedAt": "string",
        "PrincipalId": "string",
        "PrincipalName": "string",
        "PrincipalType": "string",
        "SessionContext": {
         "Attributes": {
          "CreationDate": "string",
          "MfaAuthenticated": boolean
         },
         "SessionIssuer": {
          "AccountId": "string",
          "Arn": "string",
          "PrincipalId": "string",
          "Type": "string",
          "UserName": "string"
         }
        },
        "Status": "string"
       },
       "AwsIamGroup": {
        "AttachedManagedPolicies": [{
         "PolicyArn": "string",
         "PolicyName": "string"
        }],
        "CreateDate": "string",
        "GroupId": "string",
        "GroupName": "string",
        "GroupPolicyList": [{
         "PolicyName": "string"
        }],
        "Path": "string"
       },
       "AwsIamPolicy": {
        "AttachmentCount": number,
        "CreateDate": "string",
        "DefaultVersionId": "string",
        "Description": "string",
        "IsAttachable": boolean,
        "Path": "string",
        "PermissionsBoundaryUsageCount": number,
        "PolicyId": "string",
        "PolicyName": "string",
        "PolicyVersionList": [{
```

```
          "CreateDate": "string",
          "IsDefaultVersion": boolean,
          "VersionId": "string"
        }],
        "UpdateDate": "string"
      },
      "AwsIamRole": {
        "AssumeRolePolicyDocument": "string",
        "AttachedManagedPolicies": [{
          "PolicyArn": "string",
          "PolicyName": "string"
        }],
        "CreateDate": "string",
        "InstanceProfileList": [{
          "Arn": "string",
          "CreateDate": "string",
          "InstanceProfileId": "string",
          "InstanceProfileName": "string",
          "Path": "string",
          "Roles": [{
            "Arn": "string",
            "AssumeRolePolicyDocument": "string",
            "CreateDate": "string",
            "Path": "string",
            "RoleId": "string",
            "RoleName": "string"
          }]
        }],
        "MaxSessionDuration": number,
        "Path": "string",
        "PermissionsBoundary": {
          "PermissionsBoundaryArn": "string",
          "PermissionsBoundaryType": "string"
        },
        "RoleId": "string",
        "RoleName": "string",
        "RolePolicyList": [{
          "PolicyName": "string"
        }]
      },
      "AwsIamUser": {
        "AttachedManagedPolicies": [{
          "PolicyArn": "string",
          "PolicyName": "string"
```

```
        }],
        "CreateDate": "string",
        "GroupList": ["string"],
        "Path": "string",
        "PermissionsBoundary": {
         "PermissionsBoundaryArn": "string",
         "PermissionsBoundaryType": "string"
        },
        "UserId": "string",
        "UserName": "string",
        "UserPolicyList": [{
         "PolicyName": "string"
        }]
       },
       "AwsKinesisStream": {
        "Arn": "string",
        "Name": "string",
        "RetentionPeriodHours": number,
        "ShardCount": number,
        "StreamEncryption": {
         "EncryptionType": "string",
         "KeyId": "string"
        }
       },
       "AwsKmsKey": {
        "AWSAccountId": "string",
        "CreationDate": "string",
        "Description": "string",
        "KeyId": "string",
        "KeyManager": "string",
        "KeyRotationStatus": boolean,
        "KeyState": "string",
        "Origin": "string"
       },
       "AwsLambdaFunction": {
        "Architectures": [
         "string"
        ],
        "Code": {
         "S3Bucket": "string",
         "S3Key": "string",
         "S3ObjectVersion": "string",
         "ZipFile": "string"
        },
```

```
        "CodeSha256": "string",
        "DeadLetterConfig": {
         "TargetArn": "string"
        },
        "Environment": {
         "Variables": {
          "Stage": "string"
         },
         "Error": {
          "ErrorCode": "string",
          "Message": "string"
         }
        },
        "FunctionName": "string",
        "Handler": "string",
        "KmsKeyArn": "string",
        "LastModified": "string",
        "Layers": {
         "Arn": "string",
         "CodeSize": number
        },
        "PackageType": "string",
        "RevisionId": "string",
        "Role": "string",
        "Runtime": "string",
        "Timeout": integer,
        "TracingConfig": {
         "Mode": "string"
        },
        "Version": "string",
        "VpcConfig": {
         "SecurityGroupIds": ["string"],
         "SubnetIds": ["string"]
        },
        "MasterArn": "string",
        "MemorySize": number
       },
       "AwsLambdaLayerVersion": {
        "CompatibleRuntimes": [
         "string"
        ],
        "CreatedDate": "string",
        "Version": number
       },
```

```
      "AwsMskCluster": {
       "ClusterInfo": {
        "ClientAuthentication": {
         "Sasl": {
          "Scram": {
           "Enabled": boolean
          },
          "Iam": {
           "Enabled": boolean
          }
         },
         "Tls": {
          "CertificateAuthorityArnList": [],
          "Enabled": boolean
         },
         "Unauthenticated": {
          "Enabled": boolean
         }
        },
        "ClusterName": "string",
        "CurrentVersion": "string",
        "EncryptionInfo": {
         "EncryptionAtRest": {
          "DataVolumeKMSKeyId": "string"
         },
         "EncryptionInTransit": {
          "ClientBroker": "string",
          "InCluster": boolean
         }
        },
        "EnhancedMonitoring": "string",
        "NumberOfBrokerNodes": integer
       }
      },
      "AwsNetworkFirewallFirewall": {
       "DeleteProtection": boolean,
       "Description": "string",
       "FirewallArn": "string",
       "FirewallId": "string",
       "FirewallName": "string",
       "FirewallPolicyArn": "string",
       "FirewallPolicyChangeProtection": boolean,
       "SubnetChangeProtection": boolean,
       "SubnetMappings": [{
```

```
          "SubnetId": "string"
         }],
         "VpcId": "string"
        },
        "AwsNetworkFirewallFirewallPolicy": {
         "Description": "string",
         "FirewallPolicy": {
          "StatefulRuleGroupReferences": [{
           "ResourceArn": "string"
          }],
          "StatelessCustomActions": [{
           "ActionDefinition": {
            "PublishMetricAction": {
             "Dimensions": [{
              "Value": "string"
             }]
            }
           },
           "ActionName": "string"
          }],
          "StatelessDefaultActions": ["string"],
          "StatelessFragmentDefaultActions": ["string"],
          "StatelessRuleGroupReferences": [{
           "Priority": number,
           "ResourceArn": "string"
          }]
         },
         "FirewallPolicyArn": "string",
         "FirewallPolicyId": "string",
         "FirewallPolicyName": "string"
        },
        "AwsNetworkFirewallRuleGroup": {
         "Capacity": number,
         "Description": "string",
         "RuleGroup": {
          "RulesSource": {
           "RulesSourceList": {
            "GeneratedRulesType": "string",
            "Targets": ["string"],
            "TargetTypes": ["string"]
           },
           "RulesString": "string",
           "StatefulRules": [{
            "Action": "string",
```

```
          "Header": {
           "Destination": "string",
           "DestinationPort": "string",
           "Direction": "string",
           "Protocol": "string",
           "Source": "string",
           "SourcePort": "string"
          },
          "RuleOptions": [{
           "Keyword": "string",
           "Settings": ["string"]
          }]
         }],
         "StatelessRulesAndCustomActions": {
          "CustomActions": [{
           "ActionDefinition": {
            "PublishMetricAction": {
             "Dimensions": [{
              "Value": "string"
             }]
            }
           },
           "ActionName": "string"
          }],
          "StatelessRules": [{
           "Priority": number,
           "RuleDefinition": {
            "Actions": ["string"],
            "MatchAttributes": {
             "DestinationPorts": [{
              "FromPort": number,
              "ToPort": number
             }],
             "Destinations": [{
              "AddressDefinition": "string"
             }],
             "Protocols": [number],
             "SourcePorts": [{
              "FromPort": number,
              "ToPort": number
             }],
             "Sources": [{
              "AddressDefinition": "string"
             }],
```

```
            "TcpFlags": [{
             "Flags": ["string"],
             "Masks": ["string"]
            }]
           }
          }
         }]
        }
       },
       "RuleVariables": {
        "IpSets": {
         "Definition": ["string"]
        },
        "PortSets": {
         "Definition": ["string"]
        }
       }
      },
      "RuleGroupArn": "string",
      "RuleGroupId": "string",
      "RuleGroupName": "string",
      "Type": "string"
     },
     "AwsOpenSearchServiceDomain": {
      "AccessPolicies": "string",
      "AdvancedSecurityOptions": {
       "Enabled": boolean,
       "InternalUserDatabaseEnabled": boolean,
       "MasterUserOptions": {
        "MasterUserArn": "string",
        "MasterUserName": "string",
        "MasterUserPassword": "string"
       }
      },
      "Arn": "string",
      "ClusterConfig": {
       "DedicatedMasterCount": number,
       "DedicatedMasterEnabled": boolean,
       "DedicatedMasterType": "string",
       "InstanceCount": number,
       "InstanceType": "string",
       "WarmCount": number,
       "WarmEnabled": boolean,
       "WarmType": "string",
```

```
        "ZoneAwarenessConfig": {
         "AvailabilityZoneCount": number
        },
        "ZoneAwarenessEnabled": boolean
       },
       "DomainEndpoint": "string",
       "DomainEndpointOptions": {
        "CustomEndpoint": "string",
        "CustomEndpointCertificateArn": "string",
        "CustomEndpointEnabled": boolean,
        "EnforceHTTPS": boolean,
        "TLSSecurityPolicy": "string"
       },
       "DomainEndpoints": {
        "string": "string"
       },
       "DomainName": "string",
       "EncryptionAtRestOptions": {
        "Enabled": boolean,
        "KmsKeyId": "string"
       },
       "EngineVersion": "string",
       "Id": "string",
       "LogPublishingOptions": {
        "AuditLogs": {
         "CloudWatchLogsLogGroupArn": "string",
         "Enabled": boolean
        },
        "IndexSlowLogs": {
         "CloudWatchLogsLogGroupArn": "string",
         "Enabled": boolean
        },
        "SearchSlowLogs": {
         "CloudWatchLogsLogGroupArn": "string",
         "Enabled": boolean
        }
       },
       "NodeToNodeEncryptionOptions": {
        "Enabled": boolean
       },
       "ServiceSoftwareOptions": {
        "AutomatedUpdateDate": "string",
        "Cancellable": boolean,
        "CurrentVersion": "string",
```

```
          "Description": "string",
          "NewVersion": "string",
          "OptionalDeployment": boolean,
          "UpdateAvailable": boolean,
          "UpdateStatus": "string"
        },
        "VpcOptions": {
          "SecurityGroupIds": ["string"],
          "SubnetIds": ["string"]
        }
      },
      "AwsRdsDbCluster": {
        "ActivityStreamStatus": "string",
        "AllocatedStorage": number,
        "AssociatedRoles": [{
          "RoleArn": "string",
          "Status": "string"
        }],
        "AutoMinorVersionUpgrade": boolean,
        "AvailabilityZones": ["string"],
        "BackupRetentionPeriod": integer,
        "ClusterCreateTime": "string",
        "CopyTagsToSnapshot": boolean,
        "CrossAccountClone": boolean,
        "CustomEndpoints": ["string"],
        "DatabaseName": "string",
        "DbClusterIdentifier": "string",
        "DbClusterMembers": [{
          "DbClusterParameterGroupStatus": "string",
          "DbInstanceIdentifier": "string",
          "IsClusterWriter": boolean,
          "PromotionTier": integer
        }],
        "DbClusterOptionGroupMemberships": [{
          "DbClusterOptionGroupName": "string",
          "Status": "string"
        }],
        "DbClusterParameterGroup": "string",
        "DbClusterResourceId": "string",
        "DbSubnetGroup": "string",
        "DeletionProtection": boolean,
        "DomainMemberships": [{
          "Domain": "string",
          "Fqdn": "string",
```

```
          "IamRoleName": "string",
          "Status": "string"
         }],
         "EnabledCloudwatchLogsExports": ["string"],
         "Endpoint": "string",
         "Engine": "string",
         "EngineMode": "string",
         "EngineVersion": "string",
         "HostedZoneId": "string",
         "HttpEndpointEnabled": boolean,
         "IamDatabaseAuthenticationEnabled": boolean,
         "KmsKeyId": "string",
         "MasterUsername": "string",
         "MultiAz": boolean,
         "Port": integer,
         "PreferredBackupWindow": "string",
         "PreferredMaintenanceWindow": "string",
         "ReaderEndpoint": "string",
         "ReadReplicaIdentifiers": ["string"],
         "Status": "string",
         "StorageEncrypted": boolean,
         "VpcSecurityGroups": [{
          "Status": "string",
          "VpcSecurityGroupId": "string"
         }]
        },
        "AwsRdsDbClusterSnapshot": {
         "AllocatedStorage": integer,
         "AvailabilityZones": ["string"],
         "ClusterCreateTime": "string",
         "DbClusterIdentifier": "string",
         "DbClusterSnapshotAttributes": [{
          "AttributeName": "string",
          "AttributeValues": ["string"]
         }],
         "DbClusterSnapshotIdentifier": "string",
         "Engine": "string",
         "EngineVersion": "string",
         "IamDatabaseAuthenticationEnabled": boolean,
         "KmsKeyId": "string",
         "LicenseModel": "string",
         "MasterUsername": "string",
         "PercentProgress": integer,
         "Port": integer,
```

```
        "SnapshotCreateTime": "string",
        "SnapshotType": "string",
        "Status": "string",
        "StorageEncrypted": boolean,
        "VpcId": "string"
      },
      "AwsRdsDbInstance": {
        "AllocatedStorage": number,
        "AssociatedRoles": [{
          "RoleArn": "string",
          "FeatureName": "string",
          "Status": "string"
        }],
        "AutoMinorVersionUpgrade": boolean,
        "AvailabilityZone": "string",
        "BackupRetentionPeriod": number,
        "CACertificateIdentifier": "string",
        "CharacterSetName": "string",
        "CopyTagsToSnapshot": boolean,
        "DBClusterIdentifier": "string",
        "DBInstanceClass": "string",
        "DBInstanceIdentifier": "string",
        "DbInstancePort": number,
        "DbInstanceStatus": "string",
        "DbiResourceId": "string",
        "DBName": "string",
        "DbParameterGroups": [{
          "DbParameterGroupName": "string",
          "ParameterApplyStatus": "string"
        }],
        "DbSecurityGroups": ["string"],
        "DbSubnetGroup": {
          "DbSubnetGroupArn": "string",
          "DbSubnetGroupDescription": "string",
          "DbSubnetGroupName": "string",
          "SubnetGroupStatus": "string",
          "Subnets": [{
            "SubnetAvailabilityZone": {
              "Name": "string"
            },
            "SubnetIdentifier": "string",
            "SubnetStatus": "string"
          }],
          "VpcId": "string"
```

```
        },
        "DeletionProtection": boolean,
        "Endpoint": {
         "Address": "string",
         "Port": number,
         "HostedZoneId": "string"
        },
        "DomainMemberships": [{
         "Domain": "string",
         "Fqdn": "string",
         "IamRoleName": "string",
         "Status": "string"
        }],
        "EnabledCloudwatchLogsExports": ["string"],
        "Engine": "string",
        "EngineVersion": "string",
        "EnhancedMonitoringResourceArn": "string",
        "IAMDatabaseAuthenticationEnabled": boolean,
        "InstanceCreateTime": "string",
        "Iops": number,
        "KmsKeyId": "string",
        "LatestRestorableTime": "string",
        "LicenseModel": "string",
        "ListenerEndpoint": {
         "Address": "string",
         "HostedZoneId": "string",
         "Port": number
        },
        "MasterUsername": "admin",
        "MaxAllocatedStorage": number,
        "MonitoringInterval": number,
        "MonitoringRoleArn": "string",
        "MultiAz": boolean,
        "OptionGroupMemberships": [{
         "OptionGroupName": "string",
         "Status": "string"
        }],
        "PendingModifiedValues": {
         "AllocatedStorage": number,
         "BackupRetentionPeriod": number,
         "CaCertificateIdentifier": "string",
         "DbInstanceClass": "string",
         "DbInstanceIdentifier": "string",
         "DbSubnetGroupName": "string",
```

```
        "EngineVersion": "string",
        "Iops": number,
        "LicenseModel": "string",
        "MasterUserPassword": "string",
        "MultiAZ": boolean,
        "PendingCloudWatchLogsExports": {
         "LogTypesToDisable": ["string"],
         "LogTypesToEnable": ["string"]
        },
        "Port": number,
        "ProcessorFeatures": [{
         "Name": "string",
         "Value": "string"
        }],
        "StorageType": "string"
       },
       "PerformanceInsightsEnabled": boolean,
       "PerformanceInsightsKmsKeyId": "string",
       "PerformanceInsightsRetentionPeriod": number,
       "PreferredBackupWindow": "string",
       "PreferredMaintenanceWindow": "string",
       "ProcessorFeatures": [{
        "Name": "string",
        "Value": "string"
       }],
       "PromotionTier": number,
       "PubliclyAccessible": boolean,
       "ReadReplicaDBClusterIdentifiers": ["string"],
       "ReadReplicaDBInstanceIdentifiers": ["string"],
       "ReadReplicaSourceDBInstanceIdentifier": "string",
       "SecondaryAvailabilityZone": "string",
       "StatusInfos": [{
        "Message": "string",
        "Normal": boolean,
        "Status": "string",
        "StatusType": "string"
       }],
       "StorageEncrypted": boolean,
       "TdeCredentialArn": "string",
       "Timezone": "string",
       "VpcSecurityGroups": [{
        "VpcSecurityGroupId": "string",
        "Status": "string"
       }]
```

```
      },
      "AwsRdsDbSecurityGroup": {
       "DbSecurityGroupArn": "string",
       "DbSecurityGroupDescription": "string",
       "DbSecurityGroupName": "string",
       "Ec2SecurityGroups": [{
        "Ec2SecurityGroupuId": "string",
        "Ec2SecurityGroupName": "string",
        "Ec2SecurityGroupOwnerId": "string",
        "Status": "string"
       }],
       "IpRanges": [{
        "CidrIp": "string",
        "Status": "string"
       }],
       "OwnerId": "string",
       "VpcId": "string"
      },
      "AwsRdsDbSnapshot": {
       "AllocatedStorage": integer,
       "AvailabilityZone": "string",
       "DbInstanceIdentifier": "string",
       "DbiResourceId": "string",
       "DbSnapshotIdentifier": "string",
       "Encrypted": boolean,
       "Engine": "string",
       "EngineVersion": "string",
       "IamDatabaseAuthenticationEnabled": boolean,
       "InstanceCreateTime": "string",
       "Iops": number,
       "KmsKeyId": "string",
       "LicenseModel": "string",
       "MasterUsername": "string",
       "OptionGroupName": "string",
       "PercentProgress": integer,
       "Port": integer,
       "ProcessorFeatures": [],
       "SnapshotCreateTime": "string",
       "SnapshotType": "string",
       "SourceDbSnapshotIdentifier": "string",
       "SourceRegion": "string",
       "Status": "string",
       "StorageType": "string",
       "TdeCredentialArn": "string",
```

```
        "Timezone": "string",
        "VpcId": "string"
      },
      "AwsRdsEventSubscription": {
        "CustomerAwsId": "string",
        "CustSubscriptionId": "string",
        "Enabled": boolean,
        "EventCategoriesList": ["string"],
        "EventSubscriptionArn": "string",
        "SnsTopicArn": "string",
        "SourceIdsList": ["string"],
        "SourceType": "string",
        "Status": "string",
        "SubscriptionCreationTime": "string"
      },
      "AwsRedshiftCluster": {
        "AllowVersionUpgrade": boolean,
        "AutomatedSnapshotRetentionPeriod": number,
        "AvailabilityZone": "string",
        "ClusterAvailabilityStatus": "string",
        "ClusterCreateTime": "string",
        "ClusterIdentifier": "string",
        "ClusterNodes": [{
          "NodeRole": "string",
          "PrivateIPAddress": "string",
          "PublicIPAddress": "string"
        }],
        "ClusterParameterGroups": [{
          "ClusterParameterStatusList": [{
            "ParameterApplyErrorDescription": "string",
            "ParameterApplyStatus": "string",
            "ParameterName": "string"
          }],
          "ParameterApplyStatus": "string",
          "ParameterGroupName": "string"
        }],
        "ClusterPublicKey": "string",
        "ClusterRevisionNumber": "string",
        "ClusterSecurityGroups": [{
          "ClusterSecurityGroupName": "string",
          "Status": "string"
        }],
        "ClusterSnapshotCopyStatus": {
          "DestinationRegion": "string",
```

```
        "ManualSnapshotRetentionPeriod": number,
        "RetentionPeriod": number,
        "SnapshotCopyGrantName": "string"
       },
       "ClusterStatus": "string",
       "ClusterSubnetGroupName": "string",
       "ClusterVersion": "string",
       "DBName": "string",
       "DeferredMaintenanceWindows": [{
        "DeferMaintenanceEndTime": "string",
        "DeferMaintenanceIdentifier": "string",
        "DeferMaintenanceStartTime": "string"
       }],
       "ElasticIpStatus": {
        "ElasticIp": "string",
        "Status": "string"
       },
       "ElasticResizeNumberOfNodeOptions": "string",
       "Encrypted": boolean,
       "Endpoint": {
        "Address": "string",
        "Port": number
       },
       "EnhancedVpcRouting": boolean,
       "ExpectedNextSnapshotScheduleTime": "string",
       "ExpectedNextSnapshotScheduleTimeStatus": "string",
       "HsmStatus": {
        "HsmClientCertificateIdentifier": "string",
        "HsmConfigurationIdentifier": "string",
        "Status": "string"
       },
       "IamRoles": [{
        "ApplyStatus": "string",
        "IamRoleArn": "string"
       }],
       "KmsKeyId": "string",
       "LoggingStatus":{
                   "BucketName": "string",
                   "LastFailureMessage": "string",
                   "LastFailureTime": "string",
                   "LastSuccessfulDeliveryTime": "string",
                   "LoggingEnabled": boolean,
                   "S3KeyPrefix": "string"
               },
```

```
        "MaintenanceTrackName": "string",
        "ManualSnapshotRetentionPeriod": number,
        "MasterUsername": "string",
        "NextMaintenanceWindowStartTime": "string",
        "NodeType": "string",
        "NumberOfNodes": number,
        "PendingActions": ["string"],
        "PendingModifiedValues": {
         "AutomatedSnapshotRetentionPeriod": number,
         "ClusterIdentifier": "string",
         "ClusterType": "string",
         "ClusterVersion": "string",
         "EncryptionType": "string",
         "EnhancedVpcRouting": boolean,
         "MaintenanceTrackName": "string",
         "MasterUserPassword": "string",
         "NodeType": "string",
         "NumberOfNodes": number,
         "PubliclyAccessible": "string"
        },
        "PreferredMaintenanceWindow": "string",
        "PubliclyAccessible": boolean,
        "ResizeInfo": {
         "AllowCancelResize": boolean,
         "ResizeType": "string"
        },
        "RestoreStatus": {
         "CurrentRestoreRateInMegaBytesPerSecond": number,
         "ElapsedTimeInSeconds": number,
         "EstimatedTimeToCompletionInSeconds": number,
         "ProgressInMegaBytes": number,
         "SnapshotSizeInMegaBytes": number,
         "Status": "string"
        },
        "SnapshotScheduleIdentifier": "string",
        "SnapshotScheduleState": "string",
        "VpcId": "string",
        "VpcSecurityGroups": [{
         "Status": "string",
         "VpcSecurityGroupId": "string"
        }]
       },
       "AwsRoute53HostedZone": {
        "HostedZone": {
```

```
          "Id": "string",
          "Name": "string",
          "Config": {
           "Comment": "string"
          }
         },
         "NameServers": ["string"],
         "QueryLoggingConfig": {
          "CloudWatchLogsLogGroupArn": {
           "CloudWatchLogsLogGroupArn": "string",
           "Id": "string",
           "HostedZoneId": "string"
          }
         },
         "Vpcs": [
          {
           "Id": "string",
           "Region": "string"
          }
         ]
        },
        "AwsS3AccessPoint": {
         "AccessPointArn": "string",
         "Alias": "string",
         "Bucket": "string",
         "BucketAccountId": "string",
         "Name": "string",
         "NetworkOrigin": "string",
         "PublicAccessBlockConfiguration": {
          "BlockPublicAcls": boolean,
          "BlockPublicPolicy": boolean,
          "IgnorePublicAcls": boolean,
          "RestrictPublicBuckets": boolean
         },
         "VpcConfiguration": {
          "VpcId": "string"
         }
        },
        "AwsS3AccountPublicAccessBlock": {
         "BlockPublicAcls": boolean,
         "BlockPublicPolicy": boolean,
         "IgnorePublicAcls": boolean,
         "RestrictPublicBuckets": boolean
        },
```

```
      "AwsS3Bucket": {
       "AccessControlList": "string",
       "BucketLifecycleConfiguration": {
        "Rules": [{
         "AbortIncompleteMultipartUpload": {
          "DaysAfterInitiation": number
         },
         "ExpirationDate": "string",
         "ExpirationInDays": number,
         "ExpiredObjectDeleteMarker": boolean,
         "Filter": {
          "Predicate": {
           "Operands": [{
             "Prefix": "string",
             "Type": "string"
            },
            {
             "Tag": {
              "Key": "string",
              "Value": "string"
             },
             "Type": "string"
            }
           ],
           "Type": "string"
          }
         },
         "Id": "string",
         "NoncurrentVersionExpirationInDays": number,
         "NoncurrentVersionTransitions": [{
          "Days": number,
          "StorageClass": "string"
         }],
         "Prefix": "string",
         "Status": "string",
         "Transitions": [{
          "Date": "string",
          "Days": number,
          "StorageClass": "string"
         }]
        }]
       },
       "BucketLoggingConfiguration": {
        "DestinationBucketName": "string",
```

```
          "LogFilePrefix": "string"
        },
        "BucketName": "string",
        "BucketNotificationConfiguration": {
         "Configurations": [{
          "Destination": "string",
          "Events": ["string"],
          "Filter": {
           "S3KeyFilter": {
            "FilterRules": [{
             "Name": "string",
             "Value": "string"
            }]
           }
          },
          "Type": "string"
         }]
        },
        "BucketVersioningConfiguration": {
         "IsMfaDeleteEnabled": boolean,
         "Status": "string"
        },
        "BucketWebsiteConfiguration": {
         "ErrorDocument": "string",
         "IndexDocumentSuffix": "string",
         "RedirectAllRequestsTo": {
          "HostName": "string",
          "Protocol": "string"
         },
         "RoutingRules": [{
          "Condition": {
           "HttpErrorCodeReturnedEquals": "string",
           "KeyPrefixEquals": "string"
          },
          "Redirect": {
           "HostName": "string",
           "HttpRedirectCode": "string",
           "Protocol": "string",
           "ReplaceKeyPrefixWith": "string",
           "ReplaceKeyWith": "string"
          }
         }]
        },
        "CreatedAt": "string",
```

```
        "ObjectLockConfiguration": {
         "ObjectLockEnabled": "string",
         "Rule": {
          "DefaultRetention": {
           "Days": integer,
           "Mode": "string",
           "Years": integer
          }
         }
        },
        "OwnerAccountId": "string",
        "OwnerId": "string",
        "OwnerName": "string",
        "PublicAccessBlockConfiguration": {
         "BlockPublicAcls": boolean,
         "BlockPublicPolicy": boolean,
         "IgnorePublicAcls": boolean,
         "RestrictPublicBuckets": boolean
        },
        "ServerSideEncryptionConfiguration": {
         "Rules": [{
          "ApplyServerSideEncryptionByDefault": {
           "KMSMasterKeyID": "string",
           "SSEAlgorithm": "string"
          }
         }]
        }
       },
       "AwsS3Object": {
        "ContentType": "string",
        "ETag": "string",
        "LastModified": "string",
        "ServerSideEncryption": "string",
        "SSEKMSKeyId": "string",
        "VersionId": "string"
       },
       "AwsSagemakerNotebookInstance": {
        "DirectInternetAccess": "string",
        "InstanceMetadataServiceConfiguration": {
         "MinimumInstanceMetadataServiceVersion": "string"
        },
        "InstanceType": "string",
        "LastModifiedTime": "string",
        "NetworkInterfaceId": "string",
```

```
        "NotebookInstanceArn": "string",
        "NotebookInstanceName": "string",
        "NotebookInstanceStatus": "string",
        "PlatformIdentifier": "string",
        "RoleArn": "string",
        "RootAccess": "string",
        "SecurityGroups": ["string"],
        "SubnetId": "string",
        "Url": "string",
        "VolumeSizeInGB": number
      },
      "AwsSecretsManagerSecret": {
        "Deleted": boolean,
        "Description": "string",
        "KmsKeyId": "string",
        "Name": "string",
        "RotationEnabled": boolean,
        "RotationLambdaArn": "string",
        "RotationOccurredWithinFrequency": boolean,
        "RotationRules": {
          "AutomaticallyAfterDays": integer
        }
      },
      "AwsSnsTopic": {
        "ApplicationSuccessFeedbackRoleArn": "string",
        "FirehoseFailureFeedbackRoleArn": "string",
        "FirehoseSuccessFeedbackRoleArn": "string",
        "HttpFailureFeedbackRoleArn": "string",
        "HttpSuccessFeedbackRoleArn": "string",
        "KmsMasterKeyId": "string",
        "Owner": "string",
        "SqsFailureFeedbackRoleArn": "string",
        "SqsSuccessFeedbackRoleArn": "string",
        "Subscription": {
          "Endpoint": "string",
          "Protocol": "string"
        },
        "TopicName": "string"
      },
      "AwsSqsQueue": {
        "DeadLetterTargetArn": "string",
        "KmsDataKeyReusePeriodSeconds": number,
        "KmsMasterKeyId": "string",
        "QueueName": "string"
```

```
      },
      "AwsSsmPatchCompliance": {
       "Patch": {
        "ComplianceSummary": {
         "ComplianceType": "string",
         "CompliantCriticalCount": integer,
         "CompliantHighCount": integer,
         "CompliantInformationalCount": integer,
         "CompliantLowCount": integer,
         "CompliantMediumCount": integer,
         "CompliantUnspecifiedCount": integer,
         "ExecutionType": "string",
         "NonCompliantCriticalCount": integer,
         "NonCompliantHighCount": integer,
         "NonCompliantInformationalCount": integer,
         "NonCompliantLowCount": integer,
         "NonCompliantMediumCount": integer,
         "NonCompliantUnspecifiedCount": integer,
         "OverallSeverity": "string",
         "PatchBaselineId": "string",
         "PatchGroup": "string",
         "Status": "string"
        }
       }
      },
      "AwsStepFunctionStateMachine": {
       "StateMachineArn": "string",
       "Name": "string",
       "Status": "string",
       "RoleArn": "string",
       "Type": "string",
       "LoggingConfiguration": {
        "Level": "string",
        "IncludeExecutionData": boolean
       },
       "TracingConfiguration": {
        "Enabled": boolean
       }
      },
      "AwsWafRateBasedRule": {
       "MatchPredicates": [{
        "DataId": "string",
        "Negated": boolean,
        "Type": "string"
```

```
        }],
        "MetricName": "string",
        "Name": "string",
        "RateKey": "string",
        "RateLimit": number,
        "RuleId": "string"
      },
      "AwsWafRegionalRateBasedRule": {
        "MatchPredicates": [{
          "DataId": "string",
          "Negated": boolean,
          "Type": "string"
        }],
        "MetricName": "string",
        "Name": "string",
        "RateKey": "string",
        "RateLimit": number,
        "RuleId": "string"
      },
      "AwsWafRegionalRule": {
        "MetricName": "string",
        "Name": "string",
        "RuleId": "string",
        "PredicateList": [{
            "DataId": "string",
            "Negated": boolean,
            "Type": "string"
        }]
      },
      "AwsWafRegionalRuleGroup": {
        "MetricName": "string",
        "Name": "string",
        "RuleGroupId": "string",
        "Rules": [{
          "Action": {
            "Type": "string"
          },
          "Priority": number,
          "RuleId": "string",
          "Type": "string"
        }]
      },
      "AwsWafRegionalWebAcl": {
        "DefaultAction": "string",
```

```
        "MetricName" : "string",
        "Name": "string",
        "RulesList" : [{
         "Action": {
          "Type": "string"
         },
         "Priority": number,
         "RuleId": "string",
         "Type": "string",
         "ExcludedRules": [{
          "ExclusionType": "string",
          "RuleId": "string"
         }],
         "OverrideAction": {
          "Type": "string"
         }
        }],
        "WebAclId": "string"
       },
       "AwsWafRule": {
        "MetricName": "string",
        "Name": "string",
        "PredicateList": [{
         "DataId": "string",
         "Negated": boolean,
         "Type": "string"
        }],
        "RuleId": "string"
       },
       "AwsWafRuleGroup": {
        "MetricName": "string",
        "Name": "string",
        "RuleGroupId": "string",
        "Rules": [{
         "Action": {
          "Type": "string"
         },
         "Priority": number,
         "RuleId": "string",
         "Type": "string"
        }]
       },
       "AwsWafv2RuleGroup": {
        "Arn": "string",
```

```
        "Capacity": number,
        "Description": "string",
        "Id": "string",
        "Name": "string",
        "Rules": [{
         "Action": {
         "Allow": {
          "CustomRequestHandling": {
           "InsertHeaders": [
            {
            "Name": "string",
            "Value": "string"
            },
            {
            "Name": "string",
            "Value": "string"
            }
           ]
          }
         }
         },
         "Name": "string",
         "Priority": number,
         "VisibilityConfig": {
          "CloudWatchMetricsEnabled": boolean,
          "MetricName": "string",
          "SampledRequestsEnabled": boolean
         }
        }],
        "VisibilityConfig": {
         "CloudWatchMetricsEnabled": boolean,
         "MetricName": "string",
         "SampledRequestsEnabled": boolean
        }
       },
       "AwsWafWebAcl": {
        "DefaultAction": "string",
        "Name": "string",
        "Rules": [{
         "Action": {
          "Type": "string"
         },
         "ExcludedRules": [{
          "RuleId": "string"
```

```
        }],
        "OverrideAction": {
         "Type": "string"
        },
        "Priority": number,
        "RuleId": "string",
        "Type": "string"
       }],
       "WebAclId": "string"
      },
      "AwsWafv2WebAcl": {
       "Arn": "string",
       "Capacity": number,
       "CaptchaConfig": {
        "ImmunityTimeProperty": {
         "ImmunityTime": number
        }
       },
       "DefaultAction": {
        "Block": {}
       },
       "Description": "string",
       "ManagedbyFirewallManager": boolean,
       "Name": "string",
       "Rules": [{
        "Action": {
         "RuleAction": {
          "Block": {}
         }
        },
        "Name": "string",
        "Priority": number,
        "VisibilityConfig": {
         "SampledRequestsEnabled": boolean,
         "CloudWatchMetricsEnabled": boolean,
         "MetricName": "string"
        }
       }],
       "VisibilityConfig": {
        "SampledRequestsEnabled": boolean,
        "CloudWatchMetricsEnabled": boolean,
        "MetricName": "string"
       }
      },
```

```
      "AwsXrayEncryptionConfig": {
       "KeyId": "string",
       "Status": "string",
       "Type": "string"
      },
      "CodeRepository": {
       "CodeSecurityIntegrationArn": "string",
       "ProjectName": "string",
       "ProviderType": "string"
      },
      "Container": {
       "ContainerRuntime": "string",
       "ImageId": "string",
       "ImageName": "string",
       "LaunchedAt": "string",
       "Name": "string",
       "Privileged": boolean,
       "VolumeMounts": [{
        "Name": "string",
        "MountPath": "string"
       }]
      },
      "Other": {
       "string": "string"
      },
      "Id": "string",
      "Partition": "string",
      "Region": "string",
      "ResourceRole": "string",
      "Tags": {
       "string": "string"
      },
      "Type": "string"
     }],
     "SchemaVersion": "string",
     "Severity": {
      "Label": "string",
      "Normalized": number,
      "Original": "string"
     },
     "Sample": boolean,
     "SourceUrl": "string",
     "Threats": [{
      "FilePaths": [{
```

```
        "FileName": "string",
        "FilePath": "string",
        "Hash": "string",
        "ResourceId": "string"
       }],
       "ItemCount": number,
       "Name": "string",
       "Severity": "string"
      }],
      "ThreatIntelIndicators": [{
       "Category": "string",
       "LastObservedAt": "string",
       "Source": "string",
       "SourceUrl": "string",
       "Type": "string",
       "Value": "string"
      }],
      "Title": "string",
      "Types": ["string"],
      "UpdatedAt": "string",
      "UserDefinedFields": {
       "string": "string"
      },
      "VerificationState": "string",
      "Vulnerabilities": [{
       "CodeVulnerabilities": [{
        "Cwes": [
         "string",
         "string"
        ],
        "FilePath": {
         "EndLine": integer,
         "FileName": "string",
         "FilePath": "string",
         "StartLine": integer
        },
        "SourceArn":"string"
       }],
       "Cvss": [{
        "Adjustments": [{
         "Metric": "string",
         "Reason": "string"
        }],
        "BaseScore": number,
```

```
        "BaseVector": "string",
        "Source": "string",
        "Version": "string"
       }],
       "EpssScore": number,
       "ExploitAvailable": "string",
       "FixAvailable": "string",
       "Id": "string",
       "LastKnownExploitAt": "string",
       "ReferenceUrls": ["string"],
       "RelatedVulnerabilities": ["string"],
       "Vendor": {
        "Name": "string",
        "Url": "string",
        "VendorCreatedAt": "string",
        "VendorSeverity": "string",
        "VendorUpdatedAt": "string"
       },
       "VulnerablePackages": [{
        "Architecture": "string",
        "Epoch": "string",
        "FilePath": "string",
        "FixedInVersion": "string",
        "Name": "string",
        "PackageManager": "string",
        "Release": "string",
        "Remediation": "string",
        "SourceLayerArn": "string",
        "SourceLayerHash": "string",
        "Version": "string"
       }]
      }],
      "Workflow": {
       "Status": "string"
      },
      "WorkflowState": "string"
     }
]
```

Impacto de la consolidación en los campos y valores ASFF

AWS Security Hub CSPM ofrece dos tipos de consolidación para los controles:

- Vista consolidada de controles: con este tipo de consolidación, cada control usa un único identificador para todos los estándares. Además, en la consola del CSPM de Security Hub, la página Controles muestra todos los controles de todos los estándares.
- Resultados consolidados de controles: con este tipo de consolidación, el CSPM de Security Hub genera un único resultado para un control, incluso si dicho control se aplica a varios estándares habilitados. Esto puede reducir el ruido de los resultados.

No es posible habilitar o desactivar la vista de controles consolidados. Los resultados consolidados de controles se habilitan de manera predeterminada si habilitó el CSPM de Security Hub el 23 de febrero de 2023 o después de esa fecha. De lo contrario, permanecen desactivados de manera predeterminada. Sin embargo, en Organizations, los resultados consolidados de controles solo se habilitan para las cuentas de miembro del CSPM de Security Hub si primero están habilitados para la cuenta administradora. Para obtener más información sobre los resultados consolidados de controles, consulte Generación y actualización de los resultados de control.

Ambos tipos de consolidación afectan los campos y valores de los resultados de controles en el AWS Formato de búsqueda de seguridad (ASFF).

Temas

- Vista de controles consolidada: cambios en ASFF
- Resultados de control consolidados: cambios en ASFF
- Identificadores de generador antes y después de habilitar los resultados consolidados de controles
- Cómo afecta la consolidación a las identificaciones y títulos de control
- Actualización de los flujos de trabajo para la consolidación

Vista de controles consolidada: cambios en ASFF

La característica de vista consolidada de controles introdujo los siguientes cambios en los campos y valores de los resultados de controles en el formato ASFF. Si los flujos de trabajo no dependen de los valores de estos campos del formato ASFF, no se requiere ninguna acción. Si los flujos de trabajo sí dependen de valores específicos en estos campos, actualice los flujos de trabajo para usar los valores actuales.

Campo de ASFF	Valor de muestra antes de la vista de controles consolida dos	Valor de ejemplo después de la vista consolidada de controles y una descripción del cambio
Compliance.SecurityControlId	No aplicable (campo nuevo)	EC2.2 Introduzca un único identific ador de control en todos los estándares. `ProductFi elds.RuleId` sigue proporcionando el identific ador de control estándar para los controles CIS v1.2.0. `ProductFields.Cont rolId` sigue proporcio nando el identificador de control basado en estándare s para los controles de otros estándares.
Compliance.AssociatedStanda rds	No aplicable (campo nuevo)	[{» StandardsId «:" standards /aws -foundational-security- best- /1.0.0 «}] practices/v Muestra en qué estándares está activado un control.
ProductFields.ArchivalReaso ns:0/Description	No aplicable (campo nuevo)	“El resultado se encuentra ARCHIVADO porque los resultados del control consolidado se han activado o desactivado. Esto hace que los resultados del estado anterior se archiven cuando se generen nuevos resultados”.

Campo de ASFF	Valor de muestra antes de la vista de controles consolidados	Valor de ejemplo después de la vista consolidada de controles y una descripción del cambio
		Describe por qué el CSPM de Security Hub ha archivado resultados existentes.
ProductFields.ArchivalReasons:0/ReasonCode	No aplicable (campo nuevo)	“CONSOLIDATED_CONTROL_FINDINGS_UPDATE” Proporciona el motivo por el cual el CSPM de Security Hub ha archivado resultados existentes.
ProductFields.RecommendationUrl	https://docs.aws.amazon.com/console/securityhub/PCI.EC2.2/remediation	https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation Este campo ya no hace referencia a un estándar.
Remediation.Recommendation.Text	«Para obtener instrucciones sobre cómo solucionar este problema, consulte la documentación sobre PCI DSS de Security Hub CSPM». AWS	«Para obtener instrucciones sobre cómo corregir este problema, consulte la documentación sobre los controles del CSPM AWS de Security Hub». Este campo ya no hace referencia a un estándar.

Campo de ASFF	Valor de muestra antes de la vista de controles consolidados	Valor de ejemplo después de la vista consolidada de controles y una descripción del cambio
Remediation.Recommendation.Url	https://docs.aws.amazon.com/console/securityhub/PCI.EC2.2/remediation	https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation Este campo ya no hace referencia a un estándar.

Resultados de control consolidados: cambios en ASFF

Si habilita los resultados de controles consolidados, podría verse afectado por los siguientes cambios en los campos y valores de los resultados de controles en el formato ASFF. Estos cambios se suman a los cambios introducidos por la característica de vista consolidada de controles. Si los flujos de trabajo no dependen de los valores de estos campos del formato ASFF, no se requiere ninguna acción. Si los flujos de trabajo sí dependen de valores específicos en estos campos, actualice los flujos de trabajo para usar los valores actuales.

> **Tip**
>
> Si utiliza la solución Automated Security Response en la AWS versión 2.0.0, tenga en cuenta que es compatible con los resultados de los controles consolidados. Esto significa que puede mantener los flujos de trabajo actuales si habilita los resultados de controles consolidados.

Campo de ASFF	Valor de ejemplo antes de habilitar los resultados consolidados de controles	Valor de ejemplo después de habilitar los resultados consolidados de controles y una descripción del cambio.
GeneratorId	aws-foundational-security-best- /1.0. practices/v 0/Config1.	seguridad: control/Config 1.

Campo de ASFF	Valor de ejemplo antes de habilitar los resultados consolidados de controles	Valor de ejemplo después de habilitar los resultados consolidados de controles y una descripción del cambio.
		Este campo ya no hace referencia a un estándar.
Title	PCI.Config.1 AWS Config debe estar habilitado	AWS Config debe estar habilitado Este campo ya no hace referencia a información específica del estándar.
Id	arn:aws:securityhub:eu-central-1:123456789012: - /3.2. subscription/pci dss/v 1/PCI. IAM.5/finding/ab6d6a26-a156-48f0-9403-115983e5a956	arn:aws:securityhub:eu-central- 1:123456789012:security-. control/iam 9/finding/ab6d6a26-a156-48f0-9403-115983e5a956 Este campo ya no hace referencia a un estándar.
ProductFields.ControlId	PCI.EC2.2	Eliminado. En su lugar, consulte `Compliance.SecurityControlId` . Este campo se ha eliminado en favor de un único identificador de control independiente del estándar.
ProductFields.RuleId	1.3	Eliminado. En su lugar, consulte `Compliance.SecurityControlId` . Este campo se ha eliminado en favor de un único identificador de control independiente del estándar.

Campo de ASFF	Valor de ejemplo antes de habilitar los resultados consolidados de controles	Valor de ejemplo después de habilitar los resultados consolidados de controles y una descripción del cambio.
Description (Descripción)	Este control PCI DSS comprueba si está habilitado en la cuenta y la región actuales. AWS Config	Este AWS control comprueba si AWS Config está activado en la cuenta y la región actuales. Este campo ya no hace referencia a un estándar.

Gravedad	“Severity”: {
	
	“Product”: 90,
	
	“Label”: “CRÍTICO”,
	
	“Normalized”: 90,
	
	“Original”: “CRÍTICO”
	
	}
		“Severity”: {
		
		“Label”: “CRÍTICO”,
		
		“Normalized”: 90,
		
		“Original”: “CRÍTICO”
		
		}
		
		El CSPM de Security Hub ya no usa el campo Producto para describir la gravedad de un resultado.

Tipos	["Software, configuración Checks/Industry y normativa Standards/PCI-DSS «]	["Software y normas reglamentarias Checks/Industry y de configuración"] Este campo ya no hace referencia a un estándar.

Campo de ASFF	Valor de ejemplo antes de habilitar los resultados consolidados de controles	Valor de ejemplo después de habilitar los resultados consolidados de controles y una descripción del cambio.
Compliance.RelatedRequirements	[“PCI DSS 10.5.2”, “PCI DSS 11.5”, «CIS AWS Foundations 2.5"]	["PCI DSS v3.2. 1/105.2", «PCI DSS v3.2. 1/11.5", «CIS AWS Foundations Benchmark v1.2. 0/2.5"] Este campo muestra los requisitos relacionados en todos los estándares habilitados.
CreatedAt	2022-05-05 T08:18:13.138Z	2022-09-25 T08:18:13.138Z El formato permanece igual, pero el valor se restablece cuando habilita los resultados consolidados de controles.
FirstObservedAt	2022-05-07 T08:18:13.138Z	2022-09-28 T08:18:13.138Z El formato permanece igual, pero el valor se restablece cuando habilita los resultados consolidados de controles.
ProductFields.RecommendationUrl	https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation	Eliminado. En su lugar, consulte `Remediation.Recommendation.Url` .
ProductFields.StandardsArn	arn:aws:security hub:: - security-foundational-best - /1.0.0 standards/aws practices/v	Eliminado. En su lugar, consulte `Compliance.AssociatedStandards` .

Campo de ASFF	Valor de ejemplo antes de habilitar los resultados consolidados de controles	Valor de ejemplo después de habilitar los resultados consolidados de controles y una descripción del cambio.
ProductFields.StandardsControlArn	arn:aws:securityhub:us-east-1:123456789012: control/aws -foundational-security-best- /1.0. practices/v 0/Config1.	Eliminado. El CSPM de Security Hub genera un resultado para una comprobación de seguridad aplicable a varios estándares.
ProductFields.StandardsGuideArn	arn:aws:security hub: ‣ -aws-foundations- /1.2.0 ruleset/cis benchmark/v	Eliminado. En su lugar, consulte `Compliance.AssociatedStandards` .
ProductFields.StandardsGuideSubscriptionArn	arn:aws:security hub:us-east-2:123456789012: -aws-foundations subscription/cis - /1.2.0 benchmark/v	Eliminado. El CSPM de Security Hub genera un resultado para una comprobación de seguridad aplicable a varios estándares.
ProductFields.StandardsSubscriptionArn	arn:aws:securityhub:us-east-1:123456789012: -foundational-security-best- /1.0.0 subscription/aws practices/v	Eliminado. El CSPM de Security Hub genera un resultado para una comprobación de seguridad aplicable a varios estándares.
ProductFields.aws/securityhub/FindingId	arn:aws:securityhub:us-east-1:: /:aws:securityhub:us-east-1:123456789012product/aws: securityhub/arn -foundational-security-best- /1.0. subscription/aws practices/v 0/Config. 1/finding/751c2173-7372-4e12-8656-a5210dfb1d67	arn:aws:security hub:us-east-1:: /:aws:security hub:us-east- 1:123456789012:seguridad-. product/aws securityhub/arn control/Config 1/finding/751c2173-7372-4e12-8656-a5210dfb1d67 Este campo ya no hace referencia a un estándar.

Valores para los campos del ASFF proporcionados por el cliente tras activar los resultados de control consolidados

Si habilita los resultados consolidados de controles, el CSPM de Security Hub genera un único resultado aplicable a varios estándares y archiva los resultados originales (resultados separados para cada estándar).

Las actualizaciones que hizo a los resultados originales mediante la consola del CSPM de Security Hub o mediante la operación BatchUpdateFindings no se conservarán en los nuevos resultados. Si es necesario, puede recuperar estos datos al consultar los resultados archivados. Para revisar los resultados archivados, puede abrir la página Resultados en la consola del CSPM de Security Hub y aplicar el filtro Estado del registro para elegir ARCHIVADO. También puede usar la operación GetFindings en la API del CSPM de Security Hub.

Customer-provided Campo ASFF	Descripción del cambio después de habilitar los resultados consolidados de controles
Confianza	Se restablece al estado vacío.
Criticidad	Se restablece al estado vacío.
Nota	Se restablece al estado vacío.
RelatedFindings	Se restablece al estado vacío.
Gravedad	Gravedad predeterminada del resultado (coincide con la gravedad del control).
Tipos	Se restablece a un valor independiente del estándar.
UserDefinedFields	Se restablece al estado vacío.
VerificationState	Se restablece al estado vacío.
Flujo de trabajo	Los nuevos resultados fallidos tienen un valor predeterminado de `NEW`. Los nuevos resultado s aprobados tienen un valor predeterminado de `RESOLVED`.

Identificadores de generador antes y después de habilitar los resultados consolidados de controles

En la siguiente tabla, se enumeran los cambios en los valores de identificador de generador para los controles cuando habilita los resultados consolidados de controles. Estos cambios se aplican a los controles que el CSPM de Security Hub admitía al 15 de febrero de 2023.

Identificador de generador antes de habilitar los resultados consolidados de controles	Identificador de generador después de habilitar los resultados consolidados de controles
arn:aws:security hub: ⋆ - aws-foundations - /1.2. ruleset/cis benchmark/v 0/rule/1.1	seguridad- 1. control/CloudWatch
arn:aws:security hub: ⋆ - aws-foundations - /1.2. ruleset/cis benchmark/v 0/rule/1.10	seguridad- 1.6 control/IAM
arn:aws:security hub: ⋆ - aws-foundations - /1.2. ruleset/cis benchmark/v 0/rule/1.11	seguridad- 1.7 control/IAM
arn:aws:security hub: ⋆ - aws-foundations - /1.2. ruleset/cis benchmark/v 0/rule/1.12	seguridad- 4. control/IAM
arn:aws:security hub: ⋆ - aws-foundations - /1.2. ruleset/cis benchmark/v 0/rule/1.13	seguridad- 9. control/IAM
arn:aws:security hub: ⋆ - aws-foundations - /1.2. ruleset/cis benchmark/v 0/rule/1.14	seguridad- 6. control/IAM
arn:aws:security hub: ⋆ - aws-foundations - /1.2. ruleset/cis benchmark/v 0/rule/1.16	seguridad- 2. control/IAM
arn:aws:security hub: ⋆ - aws-foundations - /1.2. ruleset/cis benchmark/v 0/rule/1.2	seguridad- 5. control/IAM
arn:aws:security hub: ⋆ - aws-foundations - /1.2. ruleset/cis benchmark/v 0/rule/1.20	seguridad- 1.8 control/IAM
arn:aws:security hub: ⋆ - aws-foundations - /1.2. ruleset/cis benchmark/v 0/rule/1.22	seguridad- 1. control/IAM

Identificador de generador antes de habilitar los resultados consolidados de controles	Identificador de generador después de habilitar los resultados consolidados de controles
arn:aws:security hub: ⋆ - aws-foundations - /1.2. ruleset/cis benchmark/v 0/rule/1.3	seguridad- 8. control/IAM
arn:aws:security hub: ⋆ - aws-foundations - /1.2. ruleset/cis benchmark/v 0/rule/1.4	seguridad- 3. control/IAM
arn:aws:security hub: ⋆ - aws-foundations - /1.2. ruleset/cis benchmark/v 0/rule/1.5	seguridad- 1.1 control/IAM
arn:aws:security hub: ⋆ - aws-foundations - /1.2. ruleset/cis benchmark/v 0/rule/1.6	seguridad- 1.2 control/IAM
arn:aws:security hub: ⋆ - aws-foundations - /1.2. ruleset/cis benchmark/v 0/rule/1.7	seguridad- 1.3 control/IAM
arn:aws:security hub: ⋆ - aws-foundations - /1.2. ruleset/cis benchmark/v 0/rule/1.8	seguridad- 1.4 control/IAM
arn:aws:security hub: ⋆ - aws-foundations - /1.2. ruleset/cis benchmark/v 0/rule/1.9	seguridad- 1.5 control/IAM
arn:aws:security hub: ⋆ - aws-foundations - /1.2. ruleset/cis benchmark/v 0/rule/2.1	seguridad- 1. control/CloudTrail
arn:aws:security hub: ⋆ - aws-foundations - /1.2. ruleset/cis benchmark/v 0/rule/2.2	seguridad- 4. control/CloudTrail
arn:aws:security hub: ⋆ - aws-foundations - /1.2. ruleset/cis benchmark/v 0/rule/2.3	seguridad- 6. control/CloudTrail
arn:aws:security hub: ⋆ - aws-foundations - /1.2. ruleset/cis benchmark/v 0/rule/2.4	seguridad- 5. control/CloudTrail
arn:aws:security hub: ⋆ - aws-foundations - /1.2. ruleset/cis benchmark/v 0/rule/2.5	seguridad- 1. control/Config

Identificador de generador antes de habilitar los resultados consolidados de controles	Identificador de generador después de habilitar los resultados consolidados de controles
arn:aws:security hub: ⋆ - aws-foundations - /1.2. ruleset/cis benchmark/v 0/rule/2.6	seguridad- 7. control/CloudTrail
arn:aws:security hub: ⋆ - aws-foundations - /1.2. ruleset/cis benchmark/v 0/rule/2.7	seguridad- 2. control/CloudTrail
arn:aws:security hub: ⋆ - aws-foundations - /1.2. ruleset/cis benchmark/v 0/rule/2.8	seguridad- 4. control/KMS
arn:aws:security hub: ⋆ - aws-foundations - /1.2. ruleset/cis benchmark/v 0/rule/2.9	seguridad- 6. control/EC2
arn:aws:security hub: ⋆ - aws-foundations - /1.2. ruleset/cis benchmark/v 0/rule/3.1	seguridad- 2. control/CloudWatch
arn:aws:security hub: ⋆ - aws-foundations - /1.2. ruleset/cis benchmark/v 0/rule/3.2	seguridad- 3. control/CloudWatch
arn:aws:security hub: ⋆ - aws-foundations - /1.2. ruleset/cis benchmark/v 0/rule/3.3	seguridad- 1. control/CloudWatch
arn:aws:security hub: ⋆ - aws-foundations - /1.2. ruleset/cis benchmark/v 0/rule/3.4	seguridad- 4. control/CloudWatch
arn:aws:security hub: ⋆ - aws-foundations - /1.2. ruleset/cis benchmark/v 0/rule/3.5	seguridad- 5. control/CloudWatch
arn:aws:security hub: ⋆ - aws-foundations - /1.2. ruleset/cis benchmark/v 0/rule/3.6	seguridad- 6. control/CloudWatch
arn:aws:security hub: ⋆ - aws-foundations - /1.2. ruleset/cis benchmark/v 0/rule/3.7	seguridad- 7. control/CloudWatch
arn:aws:security hub: ⋆ - aws-foundations - /1.2. ruleset/cis benchmark/v 0/rule/3.8	seguridad- 8. control/CloudWatch

Identificador de generador antes de habilitar los resultados consolidados de controles	Identificador de generador después de habilitar los resultados consolidados de controles
arn:aws:security hub: ⋆ - aws-foundations - /1.2. ruleset/cis benchmark/v 0/rule/3.9	seguridad- 9. control/CloudWatch
arn:aws:security hub: ⋆ - aws-foundations - /1.2. ruleset/cis benchmark/v 0/rule/3.10	seguridad- 1.0 control/CloudWatch
arn:aws:security hub: ⋆ - aws-foundations - /1.2. ruleset/cis benchmark/v 0/rule/3.11	seguridad- 1.1 control/CloudWatch
arn:aws:security hub: ⋆ - aws-foundations - /1.2. ruleset/cis benchmark/v 0/rule/3.12	seguridad- 1.2 control/CloudWatch
arn:aws:security hub: ⋆ - aws-foundations - /1.2. ruleset/cis benchmark/v 0/rule/3.13	seguridad- 1.3 control/CloudWatch
arn:aws:security hub: ⋆ - aws-foundations - /1.2. ruleset/cis benchmark/v 0/rule/3.14	seguridad- 1.4 control/CloudWatch
arn:aws:security hub: ⋆ - aws-foundations - /1.2. ruleset/cis benchmark/v 0/rule/4.1	seguridad- 1.3 control/EC2
arn:aws:security hub: ⋆ - aws-foundations - /1.2. ruleset/cis benchmark/v 0/rule/4.2	seguridad- 1.4 control/EC2
arn:aws:security hub: ⋆ - aws-foundations - /1.2. ruleset/cis benchmark/v 0/rule/4.3	seguridad- 2. control/EC2
cis-aws-foundations- /1.4. benchmark/v 0/11.0	seguridad- 5. control/IAM
cis-aws-foundations- /1.4. benchmark/v 0/11.4	seguridad: 3. control/IAM
cis-aws-foundations- /1.4. benchmark/v 0/11.6	seguridad: 1. control/IAM
cis-aws-foundations- /1.4. benchmark/v 0/11.7	seguridad- 1.8 control/IAM
cis-aws-foundations- /1.4. benchmark/v 0/14.	seguridad- 4. control/IAM

Identificador de generador antes de habilitar los resultados consolidados de controles	Identificador de generador después de habilitar los resultados consolidados de controles
cis-aws-foundations- /1.4. benchmark/v 0/15.	seguridad- 9. control/IAM
cis-aws-foundations- /1.4. benchmark/v 0/16.	seguridad- 6. control/IAM
cis-aws-foundations- /1.4. benchmark/v 0/17.	seguridad- 1. control/CloudWatch
cis-aws-foundations- /1.4. benchmark/v 0/18.	seguridad- 1.5 control/IAM
cis-aws-foundations- /1.4. benchmark/v 0/19.	seguridad- 1.6 control/IAM
cis-aws-foundations- /1.4. benchmark/v 0/21.1.2	seguridad- 5. control/S3
cis-aws-foundations- /1.4. benchmark/v 0/21.5.1	seguridad- 1. control/S3
cis-aws-foundations- /1.4. benchmark/v 0/21.5.2	seguridad- 8. control/S3
cis-aws-foundations- /1.4. benchmark/v 0/21.2.1	seguridad- 7. control/EC2
cis-aws-foundations- /1.4. benchmark/v 0/21.3.1	seguridad- 3. control/RDS
cis-aws-foundations- /1.4. benchmark/v 0/31.	seguridad: control/CloudTrail 1.
cis-aws-foundations- /1.4. benchmark/v 0/32.	seguridad- 4control/CloudTrail.
cis-aws-foundations- /1.4. benchmark/v 0/34.	seguridad- 5. control/CloudTrail
cis-aws-foundations- /1.4. benchmark/v 0/35.	seguridad: 1. control/Config
cis-aws-foundations- /1.4. benchmark/v 0/36.	seguridad- 9. control/S3
cis-aws-foundations- /1.4. benchmark/v 0/37.	seguridad- 2. control/CloudTrail
cis-aws-foundations- /1.4. benchmark/v 0/38.	seguridad- 4. control/KMS

Identificador de generador antes de habilitar los resultados consolidados de controles	Identificador de generador después de habilitar los resultados consolidados de controles
cis-aws-foundations- /1.4. benchmark/v 0/39.	seguridad- 6. control/EC2
cis-aws-foundations- /1.4. benchmark/v 0/43.	seguridad: control/CloudWatch 1.
cis-aws-foundations- /1.4. benchmark/v 0/44.	seguridad- 4. control/CloudWatch
cis-aws-foundations- /1.4. benchmark/v 0/45.	seguridad- 5. control/CloudWatch
cis-aws-foundations- /1.4. benchmark/v 0/46.	seguridad- 6. control/CloudWatch
cis-aws-foundations- /1.4. benchmark/v 0/47.	seguridad- 7. control/CloudWatch
cis-aws-foundations- /1.4. benchmark/v 0/48.	seguridad- 8. control/CloudWatch
cis-aws-foundations- /1.4. benchmark/v 0/49.	seguridad- 9. control/CloudWatch
cis-aws-foundations- /1.4. benchmark/v 0/41.0	seguridad- .10 control/CloudWatch
cis-aws-foundations- /1.4. benchmark/v 0/41.1	seguridad- 1.1 control/CloudWatch
cis-aws-foundations- /1.4. benchmark/v 0/41.2	seguridad- 1.2 control/CloudWatch
cis-aws-foundations- /1.4. benchmark/v 0/41.3	seguridad- 1.3 control/CloudWatch
cis-aws-foundations- /1.4. benchmark/v 0/41.4	seguridad- 1.4 control/CloudWatch
cis-aws-foundations- /1.4. benchmark/v 0/51.	seguridad- control/EC2 2.1
cis-aws-foundations- /1.4. benchmark/v 0/53.	seguridad- control/EC2 2.
aws-foundational-security-best- /1.0. practices/v 0/Account1.	seguridad: control/Account 1.
aws-foundational-security-best- /1.0. practices/v 0/ACM1.	seguridad: control/ACM 1.
aws-foundational-security-best- /1.0. practices/v 0/APIGateway1.	seguridad: control/APIGateway 1.

Identificador de generador antes de habilitar los resultados consolidados de controles	Identificador de generador después de habilitar los resultados consolidados de controles
aws-foundational-security-best- /1.0. practices/v 0/APIGateway2.	seguridad- control/APIGateway 2.
aws-foundational-security-best- /1.0. practices/v 0/APIGateway3.	seguridad: control/APIGateway 3.
aws-foundational-security-best- /1.0. practices/v 0/APIGateway4.	seguridad- 4. control/APIGateway
aws-foundational-security-best- /1.0. practices/v 0/APIGateway5.	seguridad- 5. control/APIGateway
aws-foundational-security-best- /1.0. practices/v 0/APIGateway8.	seguridad- 8. control/APIGateway
aws-foundational-security-best- /1.0. practices/v 0/APIGateway9.	seguridad- 9. control/APIGateway
aws-foundational-security-best- /1.0. practices/v 0/AutoScaling1.	seguridad: control/AutoScaling 1.
aws-foundational-security-best- /1.0. practices/v 0/AutoScaling2.	seguridad- control/AutoScaling 2.
aws-foundational-security-best- /1.0. practices/v 0/AutoScaling3.	seguridad: control/AutoScaling 3.
aws-foundational-security-best- /1.0. practices/v 0/Autoscaling5.	seguridad- 5. control/Autoscaling
aws-foundational-security-best- /1.0. practices/v 0/AutoScaling6.	seguridad- 6. control/AutoScaling
aws-foundational-security-best- /1.0. practices/v 0/AutoScaling9.	seguridad- 9. control/AutoScaling

Identificador de generador antes de habilitar los resultados consolidados de controles	Identificador de generador después de habilitar los resultados consolidados de controles
aws-foundational-security-best- /1.0. practices/v 0/CloudFront1.	seguridad: control/CloudFront 1.
aws-foundational-security-best- /1.0. practices/v 0/CloudFront3.	seguridad: control/CloudFront 3.
aws-foundational-security-best- /1.0. practices/v 0/CloudFront4.	seguridad- 4. control/CloudFront
aws-foundational-security-best- /1.0. practices/v 0/CloudFront5.	seguridad- 5. control/CloudFront
aws-foundational-security-best- /1.0. practices/v 0/CloudFront6.	seguridad- 6. control/CloudFront
aws-foundational-security-best- /1.0. practices/v 0/CloudFront7.	seguridad- 7. control/CloudFront
aws-foundational-security-best- /1.0. practices/v 0/CloudFront8.	seguridad- 8. control/CloudFront
aws-foundational-security-best- /1.0. practices/v 0/CloudFront9.	seguridad- 9. control/CloudFront
aws-foundational-security-best- /1.0. practices/v 0/CloudFront1.0	seguridad- .10 control/CloudFront
aws-foundational-security-best- /1.0. practices/v 0/CloudFront1.2	seguridad- 1.2 control/CloudFront
aws-foundational-security-best- /1.0. practices/v 0/CloudTrail1.	seguridad: control/CloudTrail 1.
aws-foundational-security-best- /1.0. practices/v 0/CloudTrail2.	seguridad- control/CloudTrail 2.

Identificador de generador antes de habilitar los resultados consolidados de controles	Identificador de generador después de habilitar los resultados consolidados de controles
aws-foundational-security-best- /1.0. practices/v 0/CloudTrail4.	seguridad- 4. control/CloudTrail
aws-foundational-security-best- /1.0. practices/v 0/CloudTrail5.	seguridad- 5. control/CloudTrail
aws-foundational-security-best- /1.0. practices/v 0/CodeBuild1.	seguridad: control/CodeBuild 1.
aws-foundational-security-best- /1.0. practices/v 0/CodeBuild2.	seguridad- control/CodeBuild 2.
aws-foundational-security-best- /1.0. practices/v 0/CodeBuild3.	seguridad: control/CodeBuild 3.
aws-foundational-security-best- /1.0. practices/v 0/CodeBuild4.	seguridad- 4. control/CodeBuild
aws-foundational-security-best- /1.0. practices/v 0/Config1.	seguridad: control/Config 1.
aws-foundational-security-best- /1.0. practices/v 0/DMS1.	seguridad: control/DMS 1.
aws-foundational-security-best- /1.0. practices/v 0/DynamoDB1.	seguridad: control/DynamoDB 1.
aws-foundational-security-best- /1.0. practices/v 0/DynamoDB2.	seguridad- control/DynamoDB 2.
aws-foundational-security-best- /1.0. practices/v 0/DynamoDB3.	seguridad: control/DynamoDB 3.
aws-foundational-security-best- /1.0. practices/v 0/EC21.	seguridad: control/EC2 1.

Identificador de generador antes de habilitar los resultados consolidados de controles	Identificador de generador después de habilitar los resultados consolidados de controles
aws-foundational-security-best- /1.0. practices/v 0/EC23.	seguridad: control/EC2 3.
aws-foundational-security-best- /1.0. practices/v 0/EC24.	seguridad- 4. control/EC2
aws-foundational-security-best- /1.0. practices/v 0/EC26.	seguridad- 6. control/EC2
aws-foundational-security-best- /1.0. practices/v 0/EC27.	seguridad- 7. control/EC2
aws-foundational-security-best- /1.0. practices/v 0/EC28.	seguridad- 8. control/EC2
aws-foundational-security-best- /1.0. practices/v 0/EC29.	seguridad- 9. control/EC2
aws-foundational-security-best- /1.0. practices/v 0/EC21.0	seguridad- .10 control/EC2
aws-foundational-security-best- /1.0. practices/v 0/EC21.5	seguridad- 1.5 control/EC2
aws-foundational-security-best- /1.0. practices/v 0/EC21.6	seguridad- .16 control/EC2
aws-foundational-security-best- /1.0. practices/v 0/EC21.7	seguridad- 1.7 control/EC2
aws-foundational-security-best- /1.0. practices/v 0/EC21.8	seguridad- 1.8 control/EC2
aws-foundational-security-best- /1.0. practices/v 0/EC21.9	seguridad- .19 control/EC2

Identificador de generador antes de habilitar los resultados consolidados de controles	Identificador de generador después de habilitar los resultados consolidados de controles
aws-foundational-security-best- /1.0. practices/v 0/EC22.	seguridad- control/EC2 2.
aws-foundational-security-best- /1.0. practices/v 0/EC22.0	seguridad- 2.0 control/EC2
aws-foundational-security-best- /1.0. practices/v 0/EC22.1	seguridad- 2.1 control/EC2
aws-foundational-security-best- /1.0. practices/v 0/EC22.3	seguridad- 2.3 control/EC2
aws-foundational-security-best- /1.0. practices/v 0/EC22.4	seguridad- 2.4 control/EC2
aws-foundational-security-best- /1.0. practices/v 0/EC22.5	seguridad- 2.5 control/EC2
aws-foundational-security-best- /1.0. practices/v 0/ECR1.	seguridad: control/ECR 1.
aws-foundational-security-best- /1.0. practices/v 0/ECR2.	seguridad- control/ECR 2.
aws-foundational-security-best- /1.0. practices/v 0/ECR3.	seguridad: control/ECR 3.
aws-foundational-security-best- /1.0. practices/v 0/ECS1.0	seguridad- .10 control/ECS
aws-foundational-security-best- /1.0. practices/v 0/ECS1.2	seguridad- 1.2 control/ECS
aws-foundational-security-best- /1.0. practices/v 0/ECS2.	seguridad- control/ECS 2.

Identificador de generador antes de habilitar los resultados consolidados de controles	Identificador de generador después de habilitar los resultados consolidados de controles
aws-foundational-security-best- /1.0. practices/v 0/ECS3.	seguridad: control/ECS 3.
aws-foundational-security-best- /1.0. practices/v 0/ECS4.	seguridad- 4. control/ECS
aws-foundational-security-best- /1.0. practices/v 0/ECS5.	seguridad- 5. control/ECS
aws-foundational-security-best- /1.0. practices/v 0/ECS8.	seguridad- 8. control/ECS
aws-foundational-security-best- /1.0. practices/v 0/EFS1.	seguridad: control/EFS 1.
aws-foundational-security-best- /1.0. practices/v 0/EFS2.	seguridad- control/EFS 2.
aws-foundational-security-best- /1.0. practices/v 0/EFS3.	seguridad: control/EFS 3.
aws-foundational-security-best- /1.0. practices/v 0/EFS4.	seguridad- 4. control/EFS
aws-foundational-security-best- /1.0. practices/v 0/EKS2.	seguridad- control/EKS 2.
aws-foundational-security-best- /1.0. practices/v 0/ElasticBeanstalk1.	seguridad: control/ElasticBeanstalk 1.
aws-foundational-security-best- /1.0. practices/v 0/ElasticBeanstalk2.	seguridad- control/ElasticBeanstalk 2.
aws-foundational-security-best- /1.0. practices/v 0/ELBv21.	seguridad: control/ELB 1.

Identificador de generador antes de habilitar los resultados consolidados de controles	Identificador de generador después de habilitar los resultados consolidados de controles
aws-foundational-security-best- /1.0. practices/v 0/ELB2.	seguridad- control/ELB 2.
aws-foundational-security-best- /1.0. practices/v 0/ELB3.	seguridad: control/ELB 3.
aws-foundational-security-best- /1.0. practices/v 0/ELB4.	seguridad- 4. control/ELB
aws-foundational-security-best- /1.0. practices/v 0/ELB5.	seguridad- 5. control/ELB
aws-foundational-security-best- /1.0. practices/v 0/ELB6.	seguridad- 6. control/ELB
aws-foundational-security-best- /1.0. practices/v 0/ELB7.	seguridad- 7. control/ELB
aws-foundational-security-best- /1.0. practices/v 0/ELB8.	seguridad- 8. control/ELB
aws-foundational-security-best- /1.0. practices/v 0/ELB9.	seguridad- 9. control/ELB
aws-foundational-security-best- /1.0. practices/v 0/ELB1.0	seguridad- .10 control/ELB
aws-foundational-security-best- /1.0. practices/v 0/ELB1.1	seguridad- 1.1 control/ELB
aws-foundational-security-best- /1.0. practices/v 0/ELB1.2	seguridad- 1.2 control/ELB
aws-foundational-security-best- /1.0. practices/v 0/ELB1.3	seguridad- 1.3 control/ELB

Identificador de generador antes de habilitar los resultados consolidados de controles	Identificador de generador después de habilitar los resultados consolidados de controles
aws-foundational-security-best- /1.0. practices/v 0/ELB1.4	seguridad- 1.4 control/ELB
aws-foundational-security-best- /1.0. practices/v 0/EMR1.	seguridad: control/EMR 1.
aws-foundational-security-best- /1.0. practices/ v 0/ES1.	seguridad: control/ES 1.
aws-foundational-security-best- /1.0. practices/ v 0/ES2.	seguridad- control/ES 2.
aws-foundational-security-best- /1.0. practices/ v 0/ES3.	seguridad: control/ES 3.
aws-foundational-security-best- /1.0. practices/ v 0/ES4.	seguridad- 4. control/ES
aws-foundational-security-best- /1.0. practices/ v 0/ES5.	seguridad- 5. control/ES
aws-foundational-security-best- /1.0. practices/ v 0/ES6.	seguridad- 6. control/ES
aws-foundational-security-best- /1.0. practices/ v 0/ES7.	seguridad- 7. control/ES
aws-foundational-security-best- /1.0. practices/ v 0/ES8.	seguridad- 8. control/ES
aws-foundational-security-best- /1.0. practices/v 0/GuardDuty1.	seguridad: control/GuardDuty 1.
aws-foundational-security-best- /1.0. practices/v 0/IAM1.	seguridad: control/IAM 1.

Identificador de generador antes de habilitar los resultados consolidados de controles	Identificador de generador después de habilitar los resultados consolidados de controles
aws-foundational-security-best- /1.0. practices/v 0/IAM2.	seguridad- control/IAM 2.
aws-foundational-security-best- /1.0. practices/v 0/IAM2.1	seguridad- 2.1 control/IAM
aws-foundational-security-best- /1.0. practices/v 0/IAM3.	seguridad: control/IAM 3.
aws-foundational-security-best- /1.0. practices/v 0/IAM4.	seguridad- 4. control/IAM
aws-foundational-security-best- /1.0. practices/v 0/IAM5.	seguridad- 5. control/IAM
aws-foundational-security-best- /1.0. practices/v 0/IAM6.	seguridad- 6. control/IAM
aws-foundational-security-best- /1.0. practices/v 0/IAM7.	seguridad- 7. control/IAM
aws-foundational-security-best- /1.0. practices/v 0/IAM8.	seguridad- 8. control/IAM
aws-foundational-security-best- /1.0. practices/v 0/Kinesis1.	seguridad: control/Kinesis 1.
aws-foundational-security-best- /1.0. practices/v 0/KMS1.	seguridad: control/KMS 1.
aws-foundational-security-best- /1.0. practices/v 0/KMS2.	seguridad- control/KMS 2.
aws-foundational-security-best- /1.0. practices/v 0/KMS3.	seguridad: control/KMS 3.

Identificador de generador antes de habilitar los resultados consolidados de controles	Identificador de generador después de habilitar los resultados consolidados de controles
aws-foundational-security-best- /1.0. practices/v 0/Lambda1.	seguridad: control/Lambda 1.
aws-foundational-security-best- /1.0. practices/v 0/Lambda2.	seguridad- control/Lambda 2.
aws-foundational-security-best- /1.0. practices/v 0/Lambda5.	seguridad- 5. control/Lambda
aws-foundational-security-best- /1.0. practices/v 0/NetworkFirewall3.	seguridad: control/NetworkFirewall 3.
aws-foundational-security-best- /1.0. practices/v 0/NetworkFirewall4.	seguridad- 4. control/NetworkFirewall
aws-foundational-security-best- /1.0. practices/v 0/NetworkFirewall5.	seguridad- 5. control/NetworkFirewall
aws-foundational-security-best- /1.0. practices/v 0/NetworkFirewall6.	seguridad- 6. control/NetworkFirewall
aws-foundational-security-best- /1.0. practices/v 0/Opensearch1.	seguridad: control/Opensearch 1.
aws-foundational-security-best- /1.0. practices/v 0/Opensearch2.	seguridad- control/Opensearch 2.
aws-foundational-security-best- /1.0. practices/v 0/Opensearch3.	seguridad: control/Opensearch 3.
aws-foundational-security-best- /1.0. practices/v 0/Opensearch4.	seguridad- 4. control/Opensearch
aws-foundational-security-best- /1.0. practices/v 0/Opensearch5.	seguridad- 5. control/Opensearch

Identificador de generador antes de habilitar los resultados consolidados de controles	Identificador de generador después de habilitar los resultados consolidados de controles
aws-foundational-security-best- /1.0. practices/v 0/Opensearch6.	seguridad- 6. control/Opensearch
aws-foundational-security-best- /1.0. practices/v 0/Opensearch7.	seguridad- 7. control/Opensearch
aws-foundational-security-best- /1.0. practices/v 0/Opensearch8.	seguridad- 8. control/Opensearch
aws-foundational-security-best- /1.0. practices/v 0/RDS1.	seguridad: control/RDS 1.
aws-foundational-security-best- /1.0. practices/v 0/RDS1.0	seguridad- .10 control/RDS
aws-foundational-security-best- /1.0. practices/v 0/RDS1.1	seguridad- 1.1 control/RDS
aws-foundational-security-best- /1.0. practices/v 0/RDS1.2	seguridad- 1.2 control/RDS
aws-foundational-security-best- /1.0. practices/v 0/RDS1.3	seguridad- 1.3 control/RDS
aws-foundational-security-best- /1.0. practices/v 0/RDS1.4	seguridad- 1.4 control/RDS
aws-foundational-security-best- /1.0. practices/v 0/RDS1.5	seguridad- 1.5 control/RDS
aws-foundational-security-best- /1.0. practices/v 0/RDS1.6	seguridad- .16 control/RDS
aws-foundational-security-best- /1.0. practices/v 0/RDS1.7	seguridad- 1.7 control/RDS

Identificador de generador antes de habilitar los resultados consolidados de controles	Identificador de generador después de habilitar los resultados consolidados de controles
aws-foundational-security-best- /1.0. practices/v 0/RDS1.9	seguridad- .19 control/RDS
aws-foundational-security-best- /1.0. practices/v 0/RDS2.	seguridad- control/RDS 2.
aws-foundational-security-best- /1.0. practices/v 0/RDS2.0	seguridad- 2.0 control/RDS
aws-foundational-security-best- /1.0. practices/v 0/RDS2.1	seguridad- 2.1 control/RDS
aws-foundational-security-best- /1.0. practices/v 0/RDS2.2	seguridad- 2.2 control/RDS
aws-foundational-security-best- /1.0. practices/v 0/RDS2.3	seguridad- 2.3 control/RDS
aws-foundational-security-best- /1.0. practices/v 0/RDS2.4	seguridad- 2.4 control/RDS
aws-foundational-security-best- /1.0. practices/v 0/RDS2.5	seguridad- 2.5 control/RDS
aws-foundational-security-best- /1.0. practices/v 0/RDS3.	seguridad: control/RDS 3.
aws-foundational-security-best- /1.0. practices/v 0/RDS4.	seguridad- 4. control/RDS
aws-foundational-security-best- /1.0. practices/v 0/RDS5.	seguridad- 5. control/RDS
aws-foundational-security-best- /1.0. practices/v 0/RDS6.	seguridad- 6. control/RDS

Identificador de generador antes de habilitar los resultados consolidados de controles	Identificador de generador después de habilitar los resultados consolidados de controles
aws-foundational-security-best- /1.0. practices/v 0/RDS7.	seguridad- 7. control/RDS
aws-foundational-security-best- /1.0. practices/v 0/RDS8.	seguridad- 8. control/RDS
aws-foundational-security-best- /1.0. practices/v 0/RDS9.	seguridad- 9. control/RDS
aws-foundational-security-best- /1.0. practices/v 0/Redshift1.	seguridad: control/Redshift 1.
aws-foundational-security-best- /1.0. practices/v 0/Redshift2.	seguridad- control/Redshift 2.
aws-foundational-security-best- /1.0. practices/v 0/Redshift3.	seguridad: control/Redshift 3.
aws-foundational-security-best- /1.0. practices/v 0/Redshift4.	seguridad- 4. control/Redshift
aws-foundational-security-best- /1.0. practices/v 0/Redshift6.	seguridad- 6. control/Redshift
aws-foundational-security-best- /1.0. practices/v 0/Redshift7.	seguridad- 7. control/Redshift
aws-foundational-security-best- /1.0. practices/v 0/Redshift8.	seguridad- 8. control/Redshift
aws-foundational-security-best- /1.0. practices/ v 0/S31.	seguridad: control/S3 1.
aws-foundational-security-best- /1.0. practices/v 0/S31.2	seguridad- 1.2 control/S3

Identificador de generador antes de habilitar los resultados consolidados de controles	Identificador de generador después de habilitar los resultados consolidados de controles
aws-foundational-security-best- /1.0. practices/v 0/S31.3	seguridad- 1.3 control/S3
aws-foundational-security-best- /1.0. practices/ v 0/S32.	seguridad- control/S3 2.
aws-foundational-security-best- /1.0. practices/ v 0/S33.	seguridad: control/S3 3.
aws-foundational-security-best- /1.0. practices/ v 0/S35.	seguridad- 5. control/S3
aws-foundational-security-best- /1.0. practices/ v 0/S36.	seguridad- 6. control/S3
aws-foundational-security-best- /1.0. practices/ v 0/S38.	seguridad- 8. control/S3
aws-foundational-security-best- /1.0. practices/ v 0/S39.	seguridad- 9. control/S3
aws-foundational-security-best- /1.0. practices/v 0/SageMaker1.	seguridad: control/SageMaker 1.
aws-foundational-security-best- /1.0. practices/v 0/SageMaker2.	seguridad- control/SageMaker 2.
aws-foundational-security-best- /1.0. practices/v 0/SageMaker3.	seguridad: control/SageMaker 3.
aws-foundational-security-best- /1.0. practices/v 0/SecretsManager1.	seguridad: control/SecretsManager 1.
aws-foundational-security-best- /1.0. practices/v 0/SecretsManager2.	seguridad- control/SecretsManager 2.

Identificador de generador antes de habilitar los resultados consolidados de controles	Identificador de generador después de habilitar los resultados consolidados de controles
aws-foundational-security-best- /1.0. practices/v 0/SecretsManager3.	seguridad: control/SecretsManager 3.
aws-foundational-security-best- /1.0. practices/v 0/SecretsManager4.	seguridad- 4. control/SecretsManager
aws-foundational-security-best- /1.0. practices/v 0/SQS1.	seguridad: control/SQS 1.
aws-foundational-security-best- /1.0. practices/v 0/SSM1.	seguridad: control/SSM 1.
aws-foundational-security-best- /1.0. practices/v 0/SSM2.	seguridad- control/SSM 2.
aws-foundational-security-best- /1.0. practices/v 0/SSM3.	seguridad: control/SSM 3.
aws-foundational-security-best- /1.0. practices/v 0/SSM4.	seguridad- 4. control/SSM
aws-foundational-security-best- /1.0. practices/v 0/WAF1.	seguridad: control/WAF 1.
aws-foundational-security-best- /1.0. practices/v 0/WAF2.	seguridad- control/WAF 2.
aws-foundational-security-best- /1.0. practices/v 0/WAF3.	seguridad: control/WAF 3.
aws-foundational-security-best- /1.0. practices/v 0/WAF4.	seguridad- 4. control/WAF
aws-foundational-security-best- /1.0. practices/v 0/WAF6.	seguridad- 6. control/WAF

Identificador de generador antes de habilitar los resultados consolidados de controles	Identificador de generador después de habilitar los resultados consolidados de controles
aws-foundational-security-best- /1.0. practices/v 0/WAF7.	seguridad- 7. control/WAF
aws-foundational-security-best- /1.0. practices/v 0/WAF8.	seguridad- 8. control/WAF
aws-foundational-security-best- /1.0. practices/v 0/WAF1.0	seguridad- .10 control/WAF
pci- /3.2. dss/v 1/PCI. AutoScaling.1	seguridad-1control/AutoScaling.
pci- /3.2. dss/v 1/PCI. CloudTrail.1	seguridad- control/CloudTrail 2.
pci- /3.2. dss/v 1/PCI. CloudTrail.2	seguridad-3control/CloudTrail.
pci- /3.2. dss/v 1/PCI. CloudTrail.3	seguridad- 4control/CloudTrail.
pci- /3.2. dss/v 1/PCI. CloudTrail.4	seguridad- 5control/CloudTrail.
pci- /3.2. dss/v 1/PCI. CodeBuild.1	seguridad-1control/CodeBuild.
pci- /3.2. dss/v 1/PCI. CodeBuild.2	seguridad- control/CodeBuild 2.
pci- /3.2. dss/v 1/PCI. Config.1	seguridad-1control/Config.
pci- /3.2. dss/v 1/PCI. CW.1	seguridad-1control/CloudWatch.
pci- /3.2. dss/v 1/PCI. DMS.1	seguridad-1control/DMS.
pci- /3.2. dss/v 1/PCI. EC2.1	seguridad-1control/EC2.
pci- /3.2. dss/v 1/PCI. EC2.2	seguridad- control/EC2 2.
pci- /3.2. dss/v 1/PCI. EC2.4	seguridad- control/EC2 1.2
pci- /3.2. dss/v 1/PCI. EC2.5	seguridad- control/EC2 1.3
pci- /3.2. dss/v 1/PCI. EC2.6	seguridad- 6control/EC2.

Identificador de generador antes de habilitar los resultados consolidados de controles	Identificador de generador después de habilitar los resultados consolidados de controles
pci- /3.2. dss/v 1/PCI. ELBv2.1	seguridad-1control/ELB.
pci- /3.2. dss/v 1/PCI. ES.1	seguridad- control/ES 2.
pci- /3.2. dss/v 1/PCI. ES.2	seguridad-1control/ES.
pci- /3.2. dss/v 1/PCI. GuardDuty.1	seguridad-1control/GuardDuty.
pci- /3.2. dss/v 1/PCI. IAM.1	seguridad- 4control/IAM.
pci- /3.2. dss/v 1/PCI. IAM.2	seguridad- control/IAM 2.
pci- /3.2. dss/v 1/PCI. IAM.3	seguridad-1control/IAM.
pci-/3.2. dss/v 1/PCI. IAM.4	seguridad- 6control/IAM.
pci- /3.2. dss/v 1/PCI. IAM.5	seguridad- 9control/IAM.
pci- /3.2. dss/v 1/PCI. IAM.6	seguridad- control/IAM .19
pci- /3.2. dss/v 1/PCI. IAM.7	seguridad- 8control/IAM.
pci- /3.2. dss/v 1/PCI. IAM.8	seguridad- control/IAM .10
pci- /3.2. dss/v 1/PCI. KMS.1	seguridad- 4control/KMS.
pci- /3.2. dss/v 1/PCI. Lambda.1	seguridad-1control/Lambda.
pci- /3.2. dss/v 1/PCI. Lambda.2	seguridad-3control/Lambda.
pci- /3.2. dss/v 1/PCI. Opensearch.1	seguridad- control/Opensearch 2.
pci- /3.2. dss/v 1/PCI. Opensearch.2	seguridad-1control/Opensearch.
pci- /3.2. dss/v 1/PCI. RDS.1	seguridad-1control/RDS.
pci- /3.2. dss/v 1/PCI. RDS.2	seguridad- control/RDS 2.
pci- /3.2. dss/v 1/PCI. Redshift.1	seguridad-1control/Redshift.

Identificador de generador antes de habilitar los resultados consolidados de controles	Identificador de generador después de habilitar los resultados consolidados de controles
pci- /3.2. dss/v 1/PCI. S3.1	seguridad-3control/S3.
pci- /3.2. dss/v 1/PCI. S3.2	seguridad- control/S3 2.
pci- /3.2. dss/v 1/PCI. S3.3	seguridad- 7control/S3.
pci- /3.2. dss/v 1/PCI. S3.5	seguridad- 5control/S3.
pci- /3.2. dss/v 1/PCI. S3.6	seguridad-1control/S3.
pci- /3.2. dss/v 1/PCI. SageMaker.1	seguridad-1control/SageMaker.
pci- /3.2. dss/v 1/PCI. SSM.1	seguridad- control/SSM 2.
pci- /3.2. dss/v 1/PCI. SSM.2	seguridad-3control/SSM.
pci- /3.2. dss/v 1/PCI. SSM.3	seguridad-1control/SSM.
service-managed-aws-control- /1.0. tower/v 0/ ACM1.	seguridad: control/ACM 1.
service-managed-aws-control- /1.0. tower/v 0/ APIGateway1.	seguridad: control/APIGateway 1.
service-managed-aws-control- /1.0. tower/v 0/ APIGateway2.	seguridad- control/APIGateway 2.
control de AWS administrado por servicio-/1.0. tower/v 0/APIGateway3.	seguridad: control/APIGateway 3.
control de AWS administrado por servicio-/1.0. tower/v 0/APIGateway4.	seguridad- 4. control/APIGateway
control de AWS administrado por servicio-/1.0. tower/v 0/APIGateway5.	seguridad- 5. control/APIGateway
control de AWS administrado por servicio-/1.0. tower/v 0/AutoScaling1.	seguridad: control/AutoScaling 1.

Identificador de generador antes de habilitar los resultados consolidados de controles	Identificador de generador después de habilitar los resultados consolidados de controles
service-managed-aws-control- /1.0. tower/v 0/ AutoScaling2.	seguridad- control/AutoScaling 2.
control de AWS administrado por servicio-/1.0. tower/v 0/AutoScaling3.	seguridad: control/AutoScaling 3.
control de AWS administrado por servicio-/1.0. tower/v 0/AutoScaling4.	seguridad- 4. control/AutoScaling
control de AWS administrado por servicio-/1.0. tower/v 0/Autoscaling5.	seguridad- 5. control/Autoscaling
control de AWS administrado por servicio-/1.0. tower/v 0/AutoScaling6.	seguridad- 6. control/AutoScaling
control de AWS administrado por servicio-/1.0. tower/v 0/AutoScaling9.	seguridad- 9. control/AutoScaling
control de AWS administrado por servicio-/1.0. tower/v 0/CloudTrail1.	seguridad: control/CloudTrail 1.
service-managed-aws-control- /1.0. tower/v 0/ CloudTrail2.	seguridad- control/CloudTrail 2.
control de AWS administrado por servicio-/1.0. tower/v 0/CloudTrail4.	seguridad- 4. control/CloudTrail
control de AWS administrado por servicio-/1.0. tower/v 0/CloudTrail5.	seguridad- 5. control/CloudTrail
control de AWS administrado por servicio-/1.0. tower/v 0/CodeBuild1.	seguridad: control/CodeBuild 1.
service-managed-aws-control- /1.0. tower/v 0/ CodeBuild2.	seguridad- control/CodeBuild 2.

Identificador de generador antes de habilitar los resultados consolidados de controles	Identificador de generador después de habilitar los resultados consolidados de controles
control de AWS administrado por servicio-/1.0. tower/v 0/CodeBuild4.	seguridad- 4. control/CodeBuild
control de AWS administrado por servicio-/1.0. tower/v 0/CodeBuild5.	seguridad- 5. control/CodeBuild
control de AWS administrado por servicio-/1.0. tower/v 0/DMS1.	seguridad: control/DMS 1.
service-managed-aws-control- /1.0. tower/v 0/ DynamoDB1.	seguridad: control/DynamoDB 1.
service-managed-aws-control- /1.0. tower/v 0/ DynamoDB2.	seguridad- control/DynamoDB 2.
control de AWS administrado por servicio-/1.0. tower/v 0/EC21.	seguridad: control/EC2 1.
service-managed-aws-control- /1.0. tower/v 0/ EC22.	seguridad- control/EC2 2.
control de AWS administrado por servicio-/1.0. tower/v 0/EC23.	seguridad: control/EC2 3.
control de AWS administrado por servicio-/1.0. tower/v 0/EC24.	seguridad- 4. control/EC2
control de AWS administrado por servicio-/1.0. tower/v 0/EC26.	seguridad- 6. control/EC2
control de AWS administrado por servicio-/1.0. tower/v 0/EC27.	seguridad- 7. control/EC2
control de AWS administrado por servicio-/1.0. tower/v 0/EC28.	seguridad- 8. control/EC2

Identificador de generador antes de habilitar los resultados consolidados de controles	Identificador de generador después de habilitar los resultados consolidados de controles
control de AWS administrado por servicio-/1.0. tower/v 0/EC29.	seguridad- 9. control/EC2
control de AWS administrado por servicio-/1.0. tower/v 0/EC21.0	seguridad- .10 control/EC2
control de AWS administrado por servicio-/1.0. tower/v 0/EC21.5	seguridad- 1.5 control/EC2
control de AWS administrado por servicio-/1.0. tower/v 0/EC21.6	seguridad- .16 control/EC2
control de AWS administrado por servicio-/1.0. tower/v 0/EC21.7	seguridad- 1.7 control/EC2
control de AWS administrado por servicio-/1.0. tower/v 0/EC21.8	seguridad- 1.8 control/EC2
control de AWS administrado por servicios : /1.0. tower/v 0/EC21.9	seguridad- .19 control/EC2
control de AWS administrado por servicios : /1.0. tower/v 0/EC22.0	seguridad- 2.0 control/EC2
control de AWS administrado por servicio-/1.0. tower/v 0/EC22.1	seguridad- 2.1 control/EC2
control de AWS administrado por servicio-/1.0. tower/v 0/EC22.2	seguridad- 2.2 control/EC2
control de AWS administrado por servicio-/1.0. tower/v 0/ECR1.	seguridad: control/ECR 1.
service-managed-aws-control- /1.0. tower/v 0/ ECR2.	seguridad- control/ECR 2.

Identificador de generador antes de habilitar los resultados consolidados de controles	Identificador de generador después de habilitar los resultados consolidados de controles
control de AWS administrado por servicio-/1.0. tower/v 0/ECR3.	seguridad: control/ECR 3.
control de AWS administrado por servicio-/1.0. tower/v 0/ECS2.	seguridad- control/ECS 2.
control de AWS administrado por servicio-/1.0. tower/v 0/ECS3.	seguridad: control/ECS 3.
control de AWS administrado por servicio-/1.0. tower/v 0/ECS4.	seguridad- 4. control/ECS
control de AWS administrado por servicio-/1.0. tower/v 0/ECS5.	seguridad- 5. control/ECS
control de AWS administrado por servicio-/1.0. tower/v 0/ECS8.	seguridad- 8. control/ECS
control de AWS administrado por servicio-/1.0. tower/v 0/ECS1.0	seguridad- .10 control/ECS
control de AWS administrado por servicio-/1.0. tower/v 0/ECS1.2	seguridad- 1.2 control/ECS
control de AWS administrado por servicio-/1.0. tower/v 0/EFS1.	seguridad: control/EFS 1.
service-managed-aws-control- /1.0. tower/v 0/ EFS2.	seguridad- control/EFS 2.
control de AWS administrado por servicio-/1.0. tower/v 0/EFS3.	seguridad: control/EFS 3.
control de AWS administrado por servicio-/1.0. tower/v 0/EFS4.	seguridad- 4. control/EFS

Identificador de generador antes de habilitar los resultados consolidados de controles	Identificador de generador después de habilitar los resultados consolidados de controles
control de AWS administrado por servicio-/1.0. tower/v 0/EKS2.	seguridad- control/EKS 2.
control de AWS administrado por servicio-/1.0. tower/v 0/ELB2.	seguridad- control/ELB 2.
control de AWS administrado por servicio-/1.0. tower/v 0/ELB3.	seguridad: control/ELB 3.
control de AWS administrado por servicio-/1.0. tower/v 0/ELB4.	seguridad- 4. control/ELB
control de AWS administrado por servicio-/1.0. tower/v 0/ELB5.	seguridad- 5. control/ELB
control de AWS administrado por servicio-/1.0. tower/v 0/ELB6.	seguridad- 6. control/ELB
control de AWS administrado por servicio-/1.0. tower/v 0/ELB7.	seguridad- 7. control/ELB
control de AWS administrado por servicio-/1.0. tower/v 0/ELB8.	seguridad- 8. control/ELB
control de AWS administrado por servicio-/1.0. tower/v 0/ELB9.	seguridad- 9. control/ELB
control de AWS administrado por servicio-/1.0. tower/v 0/ELB1.0	seguridad- .10 control/ELB
control de AWS administrado por servicio-/1.0. tower/v 0/ELB1.2	seguridad- 1.2 control/ELB
control de AWS administrado por servicio-/1.0. tower/v 0/ELB1.3	seguridad- 1.3 control/ELB

Identificador de generador antes de habilitar los resultados consolidados de controles	Identificador de generador después de habilitar los resultados consolidados de controles
control de AWS administrado por servicio-/1.0. tower/v 0/ELB1.4	seguridad- 1.4 control/ELB
control de AWS administrado por servicio-/1.0. tower/v 0/ELBv21.	seguridad: control/ELBv2 1.
service-managed-aws-control- /1.0. tower/v 0/ EMR1.	seguridad: control/EMR 1.
service-managed-aws-control- /1.0. tower/v 0/ ES1.	seguridad: control/ES 1.
service-managed-aws-control- /1.0. tower/v 0/ ES2.	seguridad- control/ES 2.
control de AWS administrado por servicio-/1.0. tower/v 0/ES3.	seguridad: control/ES 3.
control de AWS administrado por servicio-/1.0. tower/v 0/ES4.	seguridad- 4. control/ES
control de AWS administrado por servicio-/1.0. tower/v 0/ES5.	seguridad- 5. control/ES
control de AWS administrado por servicio-/1.0. tower/v 0/ES6.	seguridad- 6. control/ES
control de AWS administrado por servicio-/1.0. tower/v 0/ES7.	seguridad- 7. control/ES
control de AWS administrado por servicio-/1.0. tower/v 0/ES8.	seguridad- 8. control/ES
control de AWS administrado por servicio-/1.0. tower/v 0/ElasticBeanstalk1.	seguridad: control/ElasticBeanstalk 1.

Identificador de generador antes de habilitar los resultados consolidados de controles	Identificador de generador después de habilitar los resultados consolidados de controles
service-managed-aws-control- /1.0. tower/v 0/ ElasticBeanstalk2.	seguridad- control/ElasticBeanstalk 2.
control de AWS administrado por servicio-/1.0. tower/v 0/GuardDuty1.	seguridad: control/GuardDuty 1.
service-managed-aws-control- /1.0. tower/v 0/ IAM1.	seguridad: control/IAM 1.
service-managed-aws-control- /1.0. tower/v 0/ IAM2.	seguridad- control/IAM 2.
control de AWS administrado por servicio-/1.0. tower/v 0/IAM3.	seguridad: control/IAM 3.
control de AWS administrado por servicio-/1.0. tower/v 0/IAM4.	seguridad- 4. control/IAM
control de AWS administrado por servicio-/1.0. tower/v 0/IAM5.	seguridad- 5. control/IAM
control de AWS administrado por servicio-/1.0. tower/v 0/IAM6.	seguridad- 6. control/IAM
control de AWS administrado por servicio-/1.0. tower/v 0/IAM7.	seguridad- 7. control/IAM
control de AWS administrado por servicio-/1.0. tower/v 0/IAM8.	seguridad- 8. control/IAM
control de AWS administrado por servicio-/1.0. tower/v 0/IAM2.1	seguridad- 2.1 control/IAM
control de AWS administrado por servicio-/1.0. tower/v 0/Kinesis1.	seguridad: control/Kinesis 1.

Identificador de generador antes de habilitar los resultados consolidados de controles	Identificador de generador después de habilitar los resultados consolidados de controles
service-managed-aws-control- /1.0. tower/v 0/KMS1.	seguridad: control/KMS 1.
service-managed-aws-control- /1.0. tower/v 0/KMS2.	seguridad- control/KMS 2.
control de AWS administrado por servicio-/1.0. tower/v 0/KMS3.	seguridad: control/KMS 3.
control de AWS administrado por servicio-/1.0. tower/v 0/Lambda1.	seguridad: control/Lambda 1.
service-managed-aws-control- /1.0. tower/v 0/Lambda2.	seguridad- control/Lambda 2.
control de AWS administrado por servicio-/1.0. tower/v 0/Lambda5.	seguridad- 5. control/Lambda
control de AWS administrado por servicio-/1.0. tower/v 0/NetworkFirewall3.	seguridad: control/NetworkFirewall 3.
control de AWS administrado por servicio-/1.0. tower/v 0/NetworkFirewall4.	seguridad- 4. control/NetworkFirewall
control de AWS administrado por servicio-/1.0. tower/v 0/NetworkFirewall5.	seguridad- 5. control/NetworkFirewall
control de AWS administrado por servicio-/1.0. tower/v 0/NetworkFirewall6.	seguridad- 6. control/NetworkFirewall
control de AWS administrado por servicio-/1.0. tower/v 0/Opensearch1.	seguridad: control/Opensearch 1.
service-managed-aws-control- /1.0. tower/v 0/Opensearch2.	seguridad- control/Opensearch 2.

Identificador de generador antes de habilitar los resultados consolidados de controles	Identificador de generador después de habilitar los resultados consolidados de controles
control de AWS administrado por servicio-/1.0. tower/v 0/Opensearch3.	seguridad: control/Opensearch 3.
control de AWS administrado por servicio-/1.0. tower/v 0/Opensearch4.	seguridad- 4. control/Opensearch
control de AWS administrado por servicio-/1.0. tower/v 0/Opensearch5.	seguridad- 5. control/Opensearch
control de AWS administrado por servicio-/1.0. tower/v 0/Opensearch6.	seguridad- 6. control/Opensearch
control de AWS administrado por servicio-/1.0. tower/v 0/Opensearch7.	seguridad- 7. control/Opensearch
control de AWS administrado por servicio-/1.0. tower/v 0/Opensearch8.	seguridad- 8. control/Opensearch
control de AWS administrado por servicio-/1.0. tower/v 0/RDS1.	seguridad: control/RDS 1.
service-managed-aws-control- /1.0. tower/v 0/ RDS2.	seguridad- control/RDS 2.
control de AWS administrado por servicio-/1.0. tower/v 0/RDS3.	seguridad: control/RDS 3.
control de AWS administrado por servicio-/1.0. tower/v 0/RDS4.	seguridad- 4. control/RDS
control de AWS administrado por servicio-/1.0. tower/v 0/RDS5.	seguridad- 5. control/RDS
control de AWS administrado por servicio-/1.0. tower/v 0/RDS6.	seguridad- 6. control/RDS

Identificador de generador antes de habilitar los resultados consolidados de controles	Identificador de generador después de habilitar los resultados consolidados de controles
control de AWS administrado por servicio-/1.0. tower/v 0/RDS8.	seguridad- 8. control/RDS
control de AWS administrado por servicio-/1.0. tower/v 0/RDS9.	seguridad- 9. control/RDS
control de AWS administrado por servicio-/1.0. tower/v 0/RDS1.0	seguridad- .10 control/RDS
control de AWS administrado por servicio-/1.0. tower/v 0/RDS1.1	seguridad- 1.1 control/RDS
control de AWS administrado por servicio-/1.0. tower/v 0/RDS1.3	seguridad- 1.3 control/RDS
control de AWS administrado por servicio-/1.0. tower/v 0/RDS1.7	seguridad- 1.7 control/RDS
control de AWS administrado por servicio-/1.0. tower/v 0/RDS1.9	seguridad- .19 control/RDS
control de AWS administrado por servicios : /1.0. tower/v 0/RDS2.0	seguridad- 2.0 control/RDS
control de AWS administrado por servicio-/1.0. tower/v 0/RDS2.1	seguridad- 2.1 control/RDS
control de AWS administrado por servicio-/1.0. tower/v 0/RDS2.2	seguridad- 2.2 control/RDS
control de AWS administrado por servicio-/1.0. tower/v 0/RDS2.3	seguridad- 2.3 control/RDS
control de AWS administrado por servicio-/1.0. tower/v 0/RDS2.5	seguridad- 2.5 control/RDS

Identificador de generador antes de habilitar los resultados consolidados de controles	Identificador de generador después de habilitar los resultados consolidados de controles
control de AWS administrado por servicio-/1.0. tower/v 0/Redshift1.	seguridad: control/Redshift 1.
control de AWS administrado por servicio-/1.0. tower/v 0/Redshift2.	seguridad- control/Redshift 2.
control de AWS administrado por servicio-/1.0. tower/v 0/Redshift4.	seguridad- 4. control/Redshift
control de AWS administrado por servicio-/1.0. tower/v 0/Redshift6.	seguridad- 6. control/Redshift
control de AWS administrado por servicio-/1.0. tower/v 0/Redshift7.	seguridad- 7. control/Redshift
control de AWS administrado por servicio-/1.0. tower/v 0/Redshift8.	seguridad- 8. control/Redshift
control de AWS administrado por servicio-/1.0. tower/v 0/S31.	seguridad: control/S3 1.
service-managed-aws-control- /1.0. tower/v 0/ S32.	seguridad- control/S3 2.
control de AWS administrado por servicio-/1.0. tower/v 0/S33.	seguridad: control/S3 3.
control de AWS administrado por servicio-/1.0. tower/v 0/S35.	seguridad- 5. control/S3
control de AWS administrado por servicio-/1.0. tower/v 0/S36.	seguridad- 6. control/S3
control de AWS administrado por servicio-/1.0. tower/v 0/S38.	seguridad- 8. control/S3

Identificador de generador antes de habilitar los resultados consolidados de controles	Identificador de generador después de habilitar los resultados consolidados de controles
control de AWS administrado por servicio-/1.0. tower/v 0/S39.	seguridad- 9. control/S3
control de AWS administrado por servicio-/1.0. tower/v 0/S31.2	seguridad- 1.2 control/S3
control de AWS administrado por servicio-/1.0. tower/v 0/S31.3	seguridad- 1.3 control/S3
control de AWS administrado por servicio-/1.0. tower/v 0/SageMaker1.	seguridad: control/SageMaker 1.
service-managed-aws-control- /1.0. tower/v 0/ SecretsManager1.	seguridad: control/SecretsManager 1.
service-managed-aws-control- /1.0. tower/v 0/ SecretsManager2.	seguridad- control/SecretsManager 2.
control de AWS administrado por servicio-/1.0. tower/v 0/SecretsManager3.	seguridad: control/SecretsManager 3.
control de AWS administrado por servicio-/1.0. tower/v 0/SecretsManager4.	seguridad- 4. control/SecretsManager
control de AWS administrado por servicio-/1.0. tower/v 0/SQS1.	seguridad: control/SQS 1.
service-managed-aws-control- /1.0. tower/v 0/ SSM1.	seguridad: control/SSM 1.
service-managed-aws-control- /1.0. tower/v 0/ SSM2.	seguridad- control/SSM 2.
control de AWS administrado por servicio-/1.0. tower/v 0/SSM3.	seguridad: control/SSM 3.

Identificador de generador antes de habilitar los resultados consolidados de controles	Identificador de generador después de habilitar los resultados consolidados de controles
control de AWS administrado por servicio-/1.0. tower/v 0/SSM4.	seguridad- 4. control/SSM
control de AWS administrado por servicio-/1.0. tower/v 0/WAF2.	seguridad- control/WAF 2.
control de AWS administrado por servicio-/1.0. tower/v 0/WAF3.	seguridad: control/WAF 3.
control de AWS administrado por servicio-/1.0. tower/v 0/WAF4.	seguridad- 4. control/WAF

Cómo afecta la consolidación a las identificaciones y títulos de control

La vista de los controles consolidados y los resultados de control consolidados estandarizan los identificadores y títulos de los controles en todos los estándares. Los términos Identificador de control de seguridad y título de control de seguridad se refieren a estos valores independientes de los estándares.

La consola del CSPM de Security Hub muestra identificadores y títulos de controles de seguridad que no dependen de un estándar, sin importar si la cuenta tiene habilitados o desactivados los resultados consolidados de controles. Sin embargo, los resultados del CSPM de Security Hub incluyen títulos de controles específicos de cada estándar (como PCI-DSS y CIS v1.2.0) cuando la cuenta tiene desactivados los resultados consolidados de controles. Además, los resultados del CSPM de Security Hub incluyen el identificador específico del estándar y el identificador del control de seguridad. Para ver ejemplos de cómo la consolidación afecta los resultados de controles, consulte Ejemplos de resultados de controles.

En el caso de los controles que forman parte del estándar administrado por el servicio:AWS Control Tower, el prefijo `CT.` se elimina del identificador y el título del control en los resultados cuando los resultados consolidados de controles están habilitados.

Para desactivar un control de seguridad en el CSPM de Security Hub, debe desactivar todos los controles del estándar que correspondan a ese control de seguridad. En la siguiente tabla se muestra la asignación de los identificadores y títulos de control de seguridad a los identificadores y títulos de control específicos de la norma. Los identificadores y títulos de los controles que pertenecen al

estándar AWS Fundational Security Best Practices (FSBP) ya son independientes del estándar. Para asignar los controles a los requisitos de Center for Internet Security (CIS) v3.0.0 (CIS), consulte Asignación de los controles a los requisitos del CIS en cada versión. Para ejecutar sus propios scripts con esta tabla, puede descargarla como un archivo .csv.

Standard	Identificador y título del control estándar	Identificador y título del control de seguridad
CIS v1.2.0	1.1 Evitar el uso del usuario raíz	[CloudWatch.1] Debe existir un registro, un filtro métrico y una alarma para el uso del usuario «raíz»
CIS v1.2.0	1.10 Asegurar que la política de contraseñas de IAM impide la reutilización de contraseñas	[IAM.16] Asegúrese de que la política de contraseñas de IAM impida la reutilización de contraseñas
CIS v1.2.0	1.11 Asegurar que la política de contraseñas de IAM haga caducar las contraseñas al cabo de 90 días o menos	[IAM.17] Asegúrese de que la política de contraseñas de IAM haga caducar las contraseñas en un plazo de 90 días o menos
CIS v1.2.0	1.12 Asegurar que no existe una clave de acceso del usuario raíz	[IAM.4] La clave de acceso del usuario raíz de IAM no debería existir
CIS v1.2.0	1.13 Asegurar que la MFA está activada para el usuario raíz	[IAM.9] La MFA debe estar habilitada para el usuario root
CIS v1.2.0	1.14 Asegurar que la MFA está activada para el usuario raíz	[IAM.6] La MFA de hardware debe estar habilitada para el usuario root
CIS v1.2.0	1.16 Asegurar que las políticas de IAM solo están asociadas a grupos o roles	[IAM.2] Los usuarios de IAM no deberían tener políticas de IAM adjuntas
CIS v1.2.0	1.2 Asegurar que la autenticación multifactor (MFA) está habilitada para todos los usuarios de IAM que tienen una contraseña de la consola	[IAM.5] La MFA debe estar habilitada para todos los usuarios de IAM que tengan una contraseña de consola

Standard	Identificador y título del control estándar	Identificador y título del control de seguridad
CIS v1.2.0	1.20 Asegurar que se ha creado un rol de soporte para administrar incidentes con Soporte	[IAM.18] Asegúrese de que se haya creado una función de soporte para gestionar los incidentes conAWS Support
CIS v1.2.0	1.22 Asegurar que no se crean políticas de IAM que permiten privilegios administrativos completos “*:*”	[IAM.1] Las políticas de IAM no deberían permitir todos los privilegios administrativos «*»
CIS v1.2.0	1.3 Asegurar que se deshabilitan las credenciales no usadas durante 90 días o más	[IAM.8] Se deben eliminar las credenciales de usuario de IAM no utilizadas
CIS v1.2.0	1.4 Asegurar que las claves de acceso se rotan cada 90 días o menos	[IAM.3] Las claves de acceso de los usuarios de IAM deben rotarse cada 90 días o menos
CIS v1.2.0	1.5 Asegurar que la política de contraseñas de IAM requiere al menos una letra mayúscula	[IAM.11] Asegúrese de que la política de contraseñas de IAM requiera al menos una letra mayúscula
CIS v1.2.0	1.6 Asegurar que la política de contraseñas de IAM requiere al menos una letra minúscula	[IAM.12] Asegúrese de que la política de contraseñas de IAM requiera al menos una letra minúscula
CIS v1.2.0	1.7 Asegurar que la política de contraseñas de IAM requiere al menos un símbolo	[IAM.13] Asegúrese de que la política de contraseñas de IAM requiera al menos un símbolo
CIS v1.2.0	1.8 Asegurar que la política de contraseñas de IAM requiere al menos un número	[IAM.14] Asegúrese de que la política de contraseñas de IAM requiera al menos un número

Standard	Identificador y título del control estándar	Identificador y título del control de seguridad
CIS v1.2.0	1.9 Asegurar que la política de contraseñas de IAM requiere una longitud mínima de 14 o más	[IAM.15] Asegúrese de que la política de contraseñas de IAM exija una longitud de contraseña mínima de 14 o más
CIS v1.2.0	2.1 Ensure está habilitado en todas las regiones CloudTrail	[CloudTrail.1] CloudTrail debe estar habilitado y configurado con al menos un registro multirregional que incluya eventos de administración de lectura y escritura
CIS v1.2.0	2.2 Asegúrese de que la validación de los archivos de CloudTrail registro esté habilitada	[CloudTrail.4] La validación del archivo de CloudTrail registro debe estar habilitada
CIS v1.2.0	2.3 Asegúrese de que el bucket de S3 utilizado para almacenar CloudTrail los registros no sea de acceso público	[CloudTrail.6] Asegúrese de que el depósito de S3 que se utiliza para almacenar CloudTrail los registros no sea de acceso público
CIS v1.2.0	2.4 Asegúrese de que las CloudTrai l rutas estén integradas con CloudWatch los registros	[CloudTrail.5] los CloudTrail senderos deben estar integrados con Amazon CloudWatch Logs
CIS v1.2.0	2.5 Asegúrese de que AWS Config esté activado	[Config.1] AWS Config deben estar habilitados y usar la función vinculada al servicio para el registro de recursos
CIS v1.2.0	2.6 Asegúrese de que el registro de acceso al bucket S3 esté habilitado en el bucket CloudTrail S3	[CloudTrail.7] Asegúrese de que el registro de acceso al bucket de S3 esté habilitado en el CloudTrail bucket de S3

Standard	Identificador y título del control estándar	Identificador y título del control de seguridad
CIS v1.2.0	2.7 Asegúrese de que CloudTrail los registros estén cifrados en reposo mediante las CMK de KMS	[CloudTrail.2] CloudTrail debe tener activado el cifrado en reposo
CIS v1.2.0	2.8 Asegurar que está habilitada la rotación de las CMK creadas por el cliente	[KMS.4]AWS KMSla rotación de claves debe estar habilitada
CIS v1.2.0	2.9 Asegurar que el registro de flujo de la VPC está habilitado en todas las VPC	[EC2.6] El registro de flujo de VPC debe estar habilitado en todas las VPC
CIS v1.2.0	3.1 Asegurar que haya un filtro de métricas de registro y alarma para las llamadas no autorizadas a la API	[CloudWatch.2] Asegúrese de que existan un registro, un filtro métrico y una alarma para las llamadas a la API no autorizadas
CIS v1.2.0	3.10 Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de grupos de seguridad	[CloudWatch.10] Asegúrese de que haya un registro, un filtro métrico y una alarma para los cambios en los grupos de seguridad
CIS v1.2.0	3.11 Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios en las listas de control de acceso a la red (NACL)	[CloudWatch.11] Asegúrese de que existan un filtro métrico de registro y una alarma para los cambios en las listas de control de acceso a la red (NACL)
CIS v1.2.0	3.12 Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios a las gateways de la red	[CloudWatch.12] Asegúrese de que haya un registro, un filtro métrico y una alarma para detectar los cambios en las pasarelas de red

Standard	Identificador y título del control estándar	Identificador y título del control de seguridad
CIS v1.2.0	3.13 Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios ala tabla de enrutamiento	[CloudWatch.13] Asegúrese de que haya un registro, un filtro métrico y una alarma para los cambios en la tabla de rutas
CIS v1.2.0	3.14 Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de VPC	[CloudWatch.14] Asegúrese de que haya un registro, un filtro métrico y una alarma para los cambios en la VPC
CIS v1.2.0	3.2 Asegurar que haya un filtro de métricas de registro y alarma de registro para el inicio de sesión en la Consola de administración sin MFA	[CloudWatch.3] Asegúrese de que haya un registro, un filtro métrico y una alarma para iniciar sesión en la consola de administración sin MFA
CIS v1.2.0	3.3 Asegurar que haya un filtro de métricas de registro y alarma de registro para el uso del usuario raíz	[CloudWatch.1] Debe existir un registro, un filtro métrico y una alarma para el uso del usuario «raíz»
CIS v1.2.0	3.4 Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de política de IAM	[CloudWatch.4] Asegúrese de que haya un registro, un filtro métrico y una alarma para los cambios en las políticas de IAM
CIS v1.2.0	3.5 Asegúrese de que haya un registro, un filtro métrico y una alarma para los cambios CloudTrail de configuración	[CloudWatch.5] Asegúrese de que existan un registro, un filtro métrico y una alarma para los cambios CloudTrail de configuración
CIS v1.2.0	3.6 Asegúrese de que existan un filtro métrico de registro y una alarma para los errores de Consola de administración de AWS autenticación	[CloudWatch.6] Asegúrese de que existan un registro métrico, un filtro y una alarma para Consola de administración de AWS errores de autenticación

Standard	Identificador y título del control estándar	Identificador y título del control de seguridad
CIS v1.2.0	3.7 Asegurar que haya un filtro de métricas de registro y alarma de registro para la deshabilitación o eliminación programada de CMK creadas por el cliente	[CloudWatch.7] Asegúrese de que haya un registro, un filtro métrico y una alarma para deshabilitar o programar la eliminación de las claves administradas por el cliente
CIS v1.2.0	3.8 Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de política de bucket de S3	[CloudWatch.8] Asegúrese de que haya un registro, un filtro métrico y una alarma para los cambios en la política de buckets de S3
CIS v1.2.0	3.9 Asegúrese de que existan un filtro métrico de registro y una alarma para los cambios AWS Config de configuración	[CloudWatch.9] Asegúrese de que existan un registro métrico, un filtro y una alarma para AWS Config cambios de configuración
CIS v1.2.0	4.1 Asegúrese de que ningún grupo de seguridad permita la entrada desde la versión 0.0.0. 0/0 al puerto 22	[EC2.13] Los grupos de seguridad no deberían permitir la entrada desde la versión 0.0.0. 0/0 o: :/0 al puerto 22
CIS v1.2.0	4.2 Asegúrese de que ningún grupo de seguridad permita la entrada desde la versión 0.0.0. 0/0 al puerto 3389	[EC2.14] Los grupos de seguridad no deberían permitir la entrada desde la versión 0.0.0. 0/0 o: :/0 al puerto 3389
CIS v1.2.0	4.3 Asegurar que el grupo de seguridad predeterminado de cada VPC limita todo el tráfico	[EC2.2] Los grupos de seguridad predeterminados de VPC no deben permitir el tráfico entrante o saliente
CIS v1.4.0	1.10 Asegurar que la autenticación multifactor (MFA) está habilitada para todos los usuarios de IAM que tienen una contraseña de la consola	[IAM.5] La MFA debe estar habilitad a para todos los usuarios de IAM que tengan una contraseña de consola

Standard	Identificador y título del control estándar	Identificador y título del control de seguridad
CIS v1.4.0	1.14 Asegurar que las claves de acceso se rotan cada 90 días o menos	[IAM.3] Las claves de acceso de los usuarios de IAM deben rotarse cada 90 días o menos
CIS v1.4.0	1.16 Asegurar que no se adjunten políticas de IAM que permitan privilegios administrativos completos “*:*”	[IAM.1] Las políticas de IAM no deberían permitir todos los privilegios administrativos «*»
CIS v1.4.0	1.17 Asegurar que se ha creado un rol de soporte para administrar incidentes con Soporte	[IAM.18] Asegúrese de que se haya creado una función de soporte para gestionar los incidentes conAWS Support
CIS v1.4.0	1.4 Asegurar que no existe una clave de acceso del usuario raíz	[IAM.4] La clave de acceso del usuario raíz de IAM no debería existir
CIS v1.4.0	1.5 Asegurar que la MFA esté activada para el usuario raíz	[IAM.9] La MFA debe estar habilitada para el usuario root
CIS v1.4.0	1.6 Asegurar que la MFA basada en hardware está activada para el usuario raíz	[IAM.6] La MFA de hardware debe estar habilitada para el usuario root
CIS v1.4.0	1.7 Elimine el uso del usuario raíz para las tareas administrativas y diarias	[CloudWatch.1] Debe existir un registro, un filtro métrico y una alarma para el uso del usuario «raíz»
CIS v1.4.0	1.8 Asegurar que la política de contraseñas de IAM requiere una longitud mínima de 14 o más	[IAM.15] Asegúrese de que la política de contraseñas de IAM exija una longitud de contraseña mínima de 14 o más
CIS v1.4.0	1.9 Asegurar que la política de contraseñas de IAM impide la reutilización de contraseñas	[IAM.16] Asegúrese de que la política de contraseñas de IAM impida la reutilización de contraseñas

Standard	Identificador y título del control estándar	Identificador y título del control de seguridad
CIS v1.4.0	2.1.2 Asegúrese de que la política de buckets de S3 esté configurada para denegar las solicitudes HTTP	[S3.5] Los cubos de uso general de S3 deberían requerir que las solicitudes usen TLS
CIS v1.4.0	2.1.5.1 La configuración de S3 Block Public Access debe estar habilitada	[S3.1] Los cubos de uso general de S3 deben tener habilitada la configuración de bloqueo del acceso público
CIS v1.4.0	2.1.5.2 La configuración de acceso público al bloque S3 debe estar habilitada en el nivel de bucket	[S3.8] Los cubos de uso general de S3 deben bloquear el acceso público
CIS v1.4.0	2.2.1 Asegúrese de que el cifrado de volúmenes de EBS esté activado	[EC2.7] El cifrado predeterminado de EBS debe estar habilitado
CIS v1.4.0	2.3.1 Asegúrese de que el cifrado esté habilitado para las instancias RDS	[RDS.3] Las instancias de base de datos de RDS deben tener habilitado el cifrado en reposo
CIS v1.4.0	3.1 Asegúrese de que CloudTrail esté habilitado en todas las regiones	[CloudTrail.1] CloudTrail debe estar habilitado y configurado con al menos un registro multirregional que incluya eventos de administración de lectura y escritura
CIS v1.4.0	3.2 Asegúrese de que la validación del archivo de CloudTrail registro esté habilitada	[CloudTrail.4] La validación del archivo de CloudTrail registro debe estar habilitada
CIS v1.4.0	3.4 Asegúrese de que las CloudTrail rutas estén integradas con CloudWatch los registros	[CloudTrail.5] los CloudTrail senderos deben estar integrados con Amazon CloudWatch Logs

Standard	Identificador y título del control estándar	Identificador y título del control de seguridad
CIS v1.4.0	3.5 Ensure AWS Config está habilitado en todas las regiones	[Config.1] AWS Config deben estar habilitados y usar la función vinculada al servicio para el registro de recursos
CIS v1.4.0	3.6 Asegúrese de que el registro de acceso al bucket S3 esté habilitado en el bucket CloudTrail S3	[CloudTrail.7] Asegúrese de que el registro de acceso al bucket de S3 esté habilitado en el CloudTrail bucket de S3
CIS v1.4.0	3.7 Asegúrese de que CloudTrail los registros estén cifrados en reposo mediante las CMK de KMS	[CloudTrail.2] CloudTrail debe tener activado el cifrado en reposo
CIS v1.4.0	3.8 Asegurar que está habilitada la rotación de las CMK creadas por el cliente	[KMS.4]AWS KMSla rotación de claves debe estar habilitada
CIS v1.4.0	3.9 Asegurar que el registro de flujo de la VPC está habilitado en todas las VPC	[EC2.6] El registro de flujo de VPC debe estar habilitado en todas las VPC
CIS v1.4.0	4.4 Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de política de IAM	[CloudWatch.4] Asegúrese de que haya un registro, un filtro métrico y una alarma para los cambios en las políticas de IAM
CIS v1.4.0	4.5 Asegúrese de que haya un registro, un filtro métrico y una alarma para los cambios CloudTrail de configuración	[CloudWatch.5] Asegúrese de que existan un registro, un filtro métrico y una alarma para los cambios CloudTrail de configuración

Standard	Identificador y título del control estándar	Identificador y título del control de seguridad
CIS v1.4.0	4.6 Asegúrese de que existan un filtro métrico de registro y una alarma para los errores de Consola de administración de AWS autenticación	[CloudWatch.6] Asegúrese de que existan un registro métrico, un filtro y una alarma para Consola de administración de AWS errores de autenticación
CIS v1.4.0	4.7 Asegurar que haya un filtro de métricas de registro y alarma de registro para la deshabilitación o eliminación programada de CMK creadas por el cliente	[CloudWatch.7] Asegúrese de que haya un registro, un filtro métrico y una alarma para deshabilitar o programar la eliminación de las claves administradas por el cliente
CIS v1.4.0	4.8 Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de política de bucket de S3	[CloudWatch.8] Asegúrese de que haya un registro, un filtro métrico y una alarma para los cambios en la política de buckets de S3
CIS v1.4.0	4.9 Asegúrese de que existan un filtro métrico de registro y una alarma para los cambios AWS Config de configuración	[CloudWatch.9] Asegúrese de que existan un registro métrico, un filtro y una alarma para AWS Config cambios de configuración
CIS v1.4.0	4.10 Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de grupos de seguridad	[CloudWatch.10] Asegúrese de que haya un registro, un filtro métrico y una alarma para los cambios en los grupos de seguridad
CIS v1.4.0	4.11 Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios en las listas de control de acceso a la red (NACL)	[CloudWatch.11] Asegúrese de que existan un filtro métrico de registro y una alarma para los cambios en las listas de control de acceso a la red (NACL)

Standard	Identificador y título del control estándar	Identificador y título del control de seguridad
CIS v1.4.0	4.12 Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios a las puertas de enlace de la red	[CloudWatch.12] Asegúrese de que haya un registro, un filtro métrico y una alarma para detectar los cambios en las pasarelas de red
CIS v1.4.0	4.13 Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios ala tabla de enrutamiento	[CloudWatch.13] Asegúrese de que haya un registro, un filtro métrico y una alarma para los cambios en la tabla de rutas
CIS v1.4.0	4.14 Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de VPC	[CloudWatch.14] Asegúrese de que haya un registro, un filtro métrico y una alarma para los cambios en la VPC
CIS v1.4.0	5.1 Asegúrese de que ninguna ACL de red permita la entrada desde la versión 0.0.0. 0/0 a los puertos de administración de servidores remotos	[EC2.21] Las ACL de red no deberían permitir la entrada desde la versión 0.0.0. 0/0 al puerto 22 o al puerto 3389
CIS v1.4.0	5.3 Asegurar que el grupo de seguridad predeterminado de cada VPC limita todo el tráfico	[EC2.2] Los grupos de seguridad predeterminados de VPC no deben permitir el tráfico entrante o saliente
PCI DSS v3.2.1	PCI.AutoScaling.1 Los grupos de escalado automático asociados a un balanceador de cargas deben utilizar las comprobaciones de estado del balanceador de cargas	[AutoScaling.1] Los grupos de Auto Scaling asociados a un balanceador de cargas deben usar comprobaciones de estado del ELB
PCI DSS v3.2.1	PCI.CloudTrail.1 CloudTrail los registros deben cifrarse en reposo mediante CMK AWS KMS	[CloudTrail.2] CloudTrail debe tener activado el cifrado en reposo

Standard	Identificador y título del control estándar	Identificador y título del control de seguridad
PCI DSS v3.2.1	PCI.CloudTrail.2 CloudTrail debe estar habilitada	[CloudTrail.3] Debe estar habilitada al menos una CloudTrail ruta
PCI DSS v3.2.1	PCI.CloudTrail.3 CloudTrail la validación del archivo de registro debe estar habilitada	[CloudTrail.4] La validación del archivo de CloudTrail registro debe estar habilitada
PCI DSS v3.2.1	PCI.CloudTrail.4 CloudTrail las rutas deben estar integradas con Amazon CloudWatch Logs	[CloudTrail.5] los CloudTrail senderos deben estar integrados con Amazon CloudWatch Logs
PCI DSS v3.2.1	PCI.CodeBuild.1 CodeBuild GitHub o las URL del repositorio fuente de Bitbucket deben usar OAuth	[CodeBuild.1] Las URL del repositorio fuente de CodeBuild Bitbucket no deben contener credenciales confidenciales
PCI DSS v3.2.1	PCI.CodeBuild.2 CodeBuild las variables de entorno del proyecto no deben contener credenciales en texto sin cifrar	[CodeBuild.2] las variables de entorno CodeBuild del proyecto no deben contener credenciales de texto claro
PCI DSS v3.2.1	PCI.Config.1 AWS Config debe estar habilitada	[Config.1] AWS Config deben estar habilitados y usar la función vinculada al servicio para el registro de recursos
PCI DSS v3.2.1	PCI.CW.1 Debe existir un registro, un filtro métrico y una alarma para el uso del usuario «raíz»	[CloudWatch.1] Debe existir un registro, un filtro métrico y una alarma para el uso del usuario «raíz»
PCI DSS v3.2.1	PCI.DMS.1 Las instancias de replicación del Servicio de Migración de Bases de Datos no deben ser públicas	[DMS.1] Las instancias de replicación de Database Migration Service no deben ser públicas

Standard	Identificador y título del control estándar	Identificador y título del control de seguridad
PCI DSS v3.2.1	PCI.EC2.1 Las instantáneas de EBS no deben poder restaurarse públicamente	[EC2.1] Las instantáneas de Amazon EBS no deben configurarse para que se puedan restaurar públicamente
PCI DSS v3.2.1	PCI.EC2.2 El grupo de seguridad predeterminado de la VPC debe prohibir el tráfico entrante y saliente	[EC2.2] Los grupos de seguridad predeterminados de VPC no deben permitir el tráfico entrante o saliente
PCI DSS v3.2.1	PCI.EC2.4 Se deben eliminar los EIP de EC2 no utilizados	[EC2.12] Deben eliminarse las EIP de Amazon EC2 no utilizadas
PCI DSS v3.2.1	PCI.EC2.5 Los grupos de seguridad no deben permitir la entrada desde la versión 0.0.0. 0/0 al puerto 22	[EC2.13] Los grupos de seguridad no deberían permitir la entrada desde la versión 0.0.0. 0/0 o: :/0 al puerto 22
PCI DSS v3.2.1	PCI.EC2.6 El registro de flujo de VPC debe estar habilitado en todas las VPC	[EC2.6] El registro de flujo de VPC debe estar habilitado en todas las VPC
PCI DSS v3.2.1	PCI.ELBv2.1 El balanceador de carga de aplicaciones debe configura rse para redirigir todas las solicitudes HTTP a HTTPS	[ELB.1] El balanceador de carga de aplicaciones debe configurarse para redirigir todas las solicitudes HTTP a HTTPS
PCI DSS v3.2.1	PCI.ES.1 Los dominios de Elasticse arch deben estar en una VPC	[ES.2] Los dominios de Elasticsearch no deben ser de acceso público
PCI DSS v3.2.1	PCI.ES.2 Los dominios de Elasticse arch deben tener habilitado el cifrado en reposo	[ES.1] Los dominios de Elasticsearch deben tener habilitado el cifrado en reposo
PCI DSS v3.2.1	PCI.GuardDuty.1 GuardDuty debe estar habilitado	[GuardDuty.1] GuardDuty debería estar activado
PCI DSS v3.2.1	PCI.IAM.1 La clave de acceso del usuario raíz de IAM no debería existir	[IAM.4] La clave de acceso del usuario raíz de IAM no debería existir

Standard	Identificador y título del control estándar	Identificador y título del control de seguridad
PCI DSS v3.2.1	PCI.IAM.2 Los usuarios de IAM no deben tener adjuntas políticas de IAM	[IAM.2] Los usuarios de IAM no deberían tener políticas de IAM adjuntas
PCI DSS v3.2.1	PCI.IAM.3 Las políticas de IAM no deben permitir privilegios administr ativos completos con «*»	[IAM.1] Las políticas de IAM no deberían permitir todos los privilegios administrativos «*»
PCI DSS v3.2.1	PCI.IAM.4 La MFA de hardware debe estar habilitada para el usuario raíz	[IAM.6] La MFA de hardware debe estar habilitada para el usuario root
PCI DSS v3.2.1	PCI.IAM.5 La MFA virtual debe estar habilitada para el usuario raíz	[IAM.9] La MFA debe estar habilitada para el usuario root
PCI DSS v3.2.1	PCI.IAM.6 La MFA debe estar habilitada para todos los usuarios de IAM	[IAM.19] La MFA debe estar habilitad a para todos los usuarios de IAM
PCI DSS v3.2.1	PCI.IAM.7 Las credenciales de usuario de IAM deben deshabilitarse si no se utilizan en un número de días predefinido	[IAM.8] Se deben eliminar las credenciales de usuario de IAM no utilizadas
PCI DSS v3.2.1	PCI.IAM.8 Las políticas de contraseñ as para los usuarios de IAM deben tener configuraciones sólidas	[IAM.10] Las políticas de contraseñas para los usuarios de IAM deben tener configuraciones sólidas
PCI DSS v3.2.1	PCI.KMS.1 La rotación de la clave maestra del cliente (CMK) debe estar habilitada	[KMS.4]AWS KMSla rotación de claves debe estar habilitada
PCI DSS v3.2.1	PCI.Lambda.1 Las funciones de Lambda deberían prohibir el acceso público	[Lambda.1] Las políticas de las funciones de Lambda deberían prohibir el acceso público

Standard	Identificador y título del control estándar	Identificador y título del control de seguridad
PCI DSS v3.2.1	PCI.Lambda.2 Las funciones de Lambda deben estar en una VPC	[Lambda.3] Las funciones de Lambda deben estar en una VPC
PCI DSS v3.2.1	PCI.Opensearch.1 OpenSearch los dominios deben estar en una VPC	[Opensearch.2] OpenSearch los dominios no deben ser de acceso público
PCI DSS v3.2.1	PCI.Opensearch.2 Las instantáneas de EBS no deben poder restaurarse públicamente	[Opensearch.1] OpenSearch los dominios deben tener activado el cifrado en reposo
PCI DSS v3.2.1	PCI.RDS.1 La instantánea de RDS debe ser privada	[RDS.1] La instantánea de RDS debe ser privada
PCI DSS v3.2.1	PCI.RDS.2 Las instancias de base de datos de RDS deben prohibir el acceso público	[RDS.2] Las instancias de base de datos de RDS deben prohibir el acceso público, según lo determine la configuración PubliclyAccessible
PCI DSS v3.2.1	PCI.Redshift.1 Los clústeres de Amazon Redshift deben prohibir el acceso público	[Redshift.1] Los clústeres de Amazon Redshift deberían prohibir el acceso público
PCI DSS v3.2.1	PCI.S3.1 Los buckets S3 deberían prohibir el acceso público de escritura	[S3.3] Los cubos S3 de uso general deberían bloquear el acceso público a la escritura
PCI DSS v3.2.1	PCI.S3.2 Los cubos S3 deberían prohibir el acceso de lectura pública	[S3.2] Los cubos de uso general de S3 deberían bloquear el acceso de lectura pública
PCI DSS v3.2.1	PCI.S3.3 Los buckets S3 deben tener habilitada la replicación entre regiones	[S3.7] Los cubos de uso general de S3 deben utilizar la replicación entre regiones

Standard	Identificador y título del control estándar	Identificador y título del control de seguridad
PCI DSS v3.2.1	PCI.S3.5 Los buckets S3 deben requerir solicitudes para usar Secure Socket Layer	[S3.5] Los cubos de uso general de S3 deberían requerir que las solicitudes usen TLS
PCI DSS v3.2.1	PCI.S3.6 La configuración S3 Block Public Access debe estar habilitada	[S3.1] Los cubos de uso general de S3 deben tener habilitada la configuración de bloqueo del acceso público
PCI DSS v3.2.1	PCI.SageMaker.1 Las instancias de Amazon SageMaker Notebook no deben tener acceso directo a Internet	[SageMaker.1] Las instancias de Amazon SageMaker Notebook no deberían tener acceso directo a Internet
PCI DSS v3.2.1	PCI.SSM.1 Las instancias EC2 administradas por Systems Manager deben tener un estado de cumplimiento de los parches de COMPLIANT después de la instalación de un parche	[SSM.2] Las instancias de Amazon EC2 administradas por Systems Manager deben tener el estado de conformidad con los parches de CONFORMIDAD CON LOS PARCHES tras la instalación de un parche
PCI DSS v3.2.1	PCI.SSM.2 Las instancias EC2 administradas por Systems Manager deben tener un estado de cumplimiento de la asociación de COMPLIANT	[SSM.3] Las instancias de Amazon EC2 administradas por Systems Manager deben tener el estado de conformidad de la asociación de COMPLIANT
PCI DSS v3.2.1	PCI.SSM.3 Las instancias EC2 deben gestionarse mediante AWS Systems Manager	[SSM.1] Las instancias de Amazon EC2 deben administrarse medianteAWS Systems Manager

Actualización de los flujos de trabajo para la consolidación

Si los flujos de trabajo no dependen del formato específico de ninguno de los campos en los resultados de controles, no se requiere ninguna acción.

Si los flujos de trabajo dependen del formato específico de uno o varios campos en los resultados de controles, como se indica en las tablas anteriores, debe actualizar los flujos de trabajo. Por ejemplo, si creó una EventBridge regla de Amazon que activó una acción para un ID de control específico, como invocar una AWS Lambda función si el ID de control es igual al CIS 2.7, actualice la regla para usarla CloudTrail.2, que es el valor del `Compliance.SecurityControlId` campo de ese control.

Si usted creó productos de información personalizados que usan alguno de los campos o valores que cambiaron, debe actualizar esos productos de información de modo que utilicen los nuevos campos o valores.

Atributos de nivel superior necesarios del ASFF

Los siguientes atributos de nivel superior del formato de búsqueda de AWS seguridad (ASFF) son obligatorios para todas las conclusiones del CSPM de Security Hub. Para obtener más información sobre estos atributos, consulte AwsSecurityFinding en la Referencia de la API de AWS Security Hub.

AwsAccountId

El Cuenta de AWS identificador al que se aplica el hallazgo.

Ejemplo

```
"AwsAccountId": "111111111111"
```

CreatedAt

Indica el momento en que se creó el posible problema o evento de seguridad que aparece en el resultado.

Ejemplo

```
"CreatedAt": "2017-03-22T13:22:13.933Z"
```

Description (Descripción)

Una descripción del hallazgo. Este campo puede ser texto reutilizable no específico o información específica de la instancia del hallazgo.

En el caso de los resultados de controles que genera el CSPM de Security Hub, este campo proporciona una descripción del control.

Este campo no hace referencia a un estándar si activa los resultados de control consolidados.

Ejemplo

```
"Description": "This AWS control checks whether AWS Config is enabled in the current
 account and Region."
```

GeneratorId

El identificador para el componente específico de la solución (unidad de lógica discreta) que generó un hallazgo.

En el caso de los resultados de controles que genera el CSPM de Security Hub, este campo no hace referencia a ningún estándar cuando habilita los resultados consolidados de controles.

Ejemplo

```
"GeneratorId": "security-control/Config.1"
```

Id

El identificador específico del producto para un hallazgo. En el caso de los resultados de controles que genera el CSPM de Security Hub, este campo proporciona el nombre de recurso de Amazon (ARN) del resultado.

Este campo no hace referencia a un estándar si activa los resultados de control consolidados.

Ejemplo

```
"Id": "arn:aws:securityhub:eu-central-1:123456789012:security-control/iam.9/finding/
ab6d6a26-a156-48f0-9403-115983e5a956"
```

ProductArn

El nombre de recurso de Amazon (ARN) que genera el CSPM de Security Hub y que identifica de forma única un producto de resultados de un tercero después de que dicho producto se registra en el CSPM de Security Hub.

El formato de este campo es `arn:`*`partition`*`:securityhub:`*`region`*`:`*`account-id`*`:product/`*`company-id`*`/`*`product-id`*.

- Para Servicios de AWS que estén integrados con Security Hub CSPM, `company-id` debe ser `aws` "» y `product-id` debe ser el nombre del servicio AWS público. Como AWS los productos y servicios no están asociados a una cuenta, la `account-id` sección del ARN está vacía. Servicios de AWS los que aún no están integrados con Security Hub CSPM se consideran productos de terceros.
- En el caso de productos públicos, el `company-id` y el `product-id` deben ser los valores de ID especificados en el momento del registro.
- En el caso de productos privados, el `company-id` debe ser el ID de la cuenta. El `product-id` debe ser la palabra reservada de forma predeterminada o el ID que se especificó en el momento del registro.

Ejemplo

```
// Private ARN
    "ProductArn": "arn:aws:securityhub:us-east-1:111111111111:product/111111111111/
default"

// Public ARN
    "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty"
    "ProductArn": "arn:aws:securityhub:us-west-2:222222222222:product/generico/secure-
pro"
```

Recursos

La `Resources` matriz de objetos proporciona un conjunto de tipos de datos de recursos que describen AWS los recursos a los que hace referencia el hallazgo. Para ver los detalles sobre los campos que puede incluir el objeto `Resources`, incluidos los campos obligatorios, consulte Resource en la Referencia de la API de AWS Security Hub. Para ver ejemplos de `Resources` objetos específicos Servicios de AWS, consulteRecursos Objeto ASFF.

Ejemplo

```
"Resources": [
  {
    "ApplicationArn": "arn:aws:resource-groups:us-west-2:123456789012:group/
SampleApp/1234567890abcdef0",
```

```
    "ApplicationName": "SampleApp",
    "DataClassification": {
    "DetailedResultsLocation": "Path_to_Folder_Or_File",
    "Result": {
        "MimeType": "text/plain",
        "SizeClassified": 2966026,
        "AdditionalOccurrences": false,
        "Status": {
            "Code": "COMPLETE",
            "Reason": "Unsupportedfield"
        },
       "SensitiveData": [
            {
                "Category": "PERSONAL_INFORMATION",
                "Detections": [
                    {
                        "Count": 34,
                        "Type": "GE_PERSONAL_ID",
                        "Occurrences": {
                            "LineRanges": [
                                {
                                    "Start": 1,
                                    "End": 10,
                                    "StartColumn": 20
                                }
                            ],
                            "Pages": [],
                            "Records": [],
                            "Cells": []
                        }
                    },
                    {
                        "Count": 59,
                        "Type": "EMAIL_ADDRESS",
                        "Occurrences": {
                            "Pages": [
                                {
                                    "PageNumber": 1,
                                    "OffsetRange": {
                                        "Start": 1,
                                        "End": 100,
                                        "StartColumn": 10
                                     },
                                    "LineRange": {
```

```
                                        "Start": 1,
                                        "End": 100,
                                        "StartColumn": 10
                                    }
                                }
                            ]
                        }
                    },
                    {
                        "Count": 2229,
                        "Type": "URL",
                        "Occurrences": {
                           "LineRanges": [
                               {
                                   "Start": 1,
                                   "End": 13
                               }
                           ]
                        }
                    },
                    {
                        "Count": 13826,
                        "Type": "NameDetection",
                        "Occurrences": {
                             "Records": [
                                 {
                                     "RecordIndex": 1,
                                     "JsonPath": "$.ssn.value"
                                 }
                             ]
                        }
                    },
                    {
                        "Count": 32,
                        "Type": "AddressDetection"
                    }
                ],
                "TotalCount": 32
            }
        ],
        "CustomDataIdentifiers": {
            "Detections": [
                 {
                     "Arn": "1712be25e7c7f53c731fe464f1c869b8",
```

```
                    "Name": "1712be25e7c7f53c731fe464f1c869b8",
                    "Count": 2
                }
            ],
            "TotalCount": 2
        }
    }
},
 "Type": "AwsEc2Instance",
 "Id": "arn:aws:ec2:us-west-2:123456789012:instance/i-abcdef01234567890",
 "Partition": "aws",
 "Region": "us-west-2",
 "ResourceRole": "Target",
 "Tags": {
  "billingCode": "Lotus-1-2-3",
  "needsPatching": true
 },
 "Details": {
  "IamInstanceProfileArn": "arn:aws:iam::123456789012:role/IamInstanceProfileArn",
  "ImageId": "ami-79fd7eee",
  "IpV4Addresses": ["1.1.1.1"],
  "IpV6Addresses": ["2001:db8:1234:1a2b::123"],
  "KeyName": "testkey",
  "LaunchedAt": "2018-09-29T01:25:54Z",
  "MetadataOptions": {
   "HttpEndpoint": "enabled",
   "HttpProtocolIpv6": "enabled",
   "HttpPutResponseHopLimit": 1,
   "HttpTokens": "optional",
   "InstanceMetadataTags": "disabled"
  }
 },
  "NetworkInterfaces": [
  {
   "NetworkInterfaceId": "eni-e5aa89a3"
  }
  ],
  "SubnetId": "PublicSubnet",
  "Type": "i3.xlarge",
  "VirtualizationType": "hvm",
  "VpcId": "TestVPCIpv6"
 }
```

```
]
```

SchemaVersion

La versión del esquema para el que se está formateado un hallazgo. El valor de este campo debe ser una de las versiones publicadas oficialmente identificadas por AWS. En la versión actual, la versión del esquema del formato de búsqueda de AWS seguridad es`2018-10-08`.

Ejemplo

```
"SchemaVersion": "2018-10-08"
```

Gravedad

Define la importancia de un resultado. Para obtener más información sobre este objeto, consulte `Severity` en la referencia de la API de AWS Security Hub .

`Severity` es a la vez un objeto de nivel superior en un resultado y está anidado debajo del objeto `FindingProviderFields`.

El valor del objeto de nivel superior `Severity` para un resultado se debe actualizar solo mediante la API `BatchUpdateFindings`.

Para proporcionar información sobre la gravedad, los proveedores de resultados deben actualizar el objeto `Severity` de `FindingProviderFields` cuando se hace una solicitud a la API `BatchImportFindings`.
Si una solicitud `BatchImportFindings` para un nuevo resultado solo proporciona `Label` o `Normalized` únicamente, el CSPM de Security Hub completa automáticamente el valor del otro campo. Los campos `Product` y `Original` también pueden completarse.

Si el objeto de nivel superior `Finding.Severity` está presente pero `Finding.FindingProviderFields` no está presente, el CSPM de Security Hub crea el objeto `FindingProviderFields.Severity` y copia en este la totalidad de `Finding.Severity object`. Esto garantiza que los detalles originales proporcionados por el proveedor se van a retener en la estructura `FindingProviderFields.Severity`, incluso si se sobrescribe el objeto de nivel superior `Severity`.

La gravedad del hallazgo no tiene en cuenta la importancia crítica de los activos involucrados o del recurso subyacente. El nivel de importancia crítica se define como el nivel de importancia de los

recursos que están asociados con el hallazgo. Por ejemplo, un recurso que está asociado a una aplicación de misión crítica tiene mayor importancia crítica frente a uno asociado a pruebas que no son de producción. Para capturar información sobre la importancia crítica de los recursos, utilice el campo `Criticality`.

Recomendamos utilizar la siguiente guía al traducir las puntuaciones de gravedad nativas de los resultados al valor `Severity.Label` en ASFF.

- `INFORMATIONAL`: Esta categoría puede incluir el resultado de `PASSED`, `WARNING`, `NOT AVAILABLE` o una identificación de datos confidenciales.
- `LOW`: Resultados que podrían resultar en futuros compromisos. Por ejemplo, esta categoría puede incluir vulnerabilidades, puntos débiles de configuración y contraseñas expuestas.
- `MEDIUM` – Resultados que están asociados con problemas que indican una situación de peligro activa, pero ninguna indicación de que un adversario haya completado sus objetivos. Por ejemplo, esta categoría puede incluir actividad de malware, actividad de piratería y detección de comportamientos inusual.
- `HIGH` o `CRITICAL` – Resultados que indican que un adversario ha completado sus objetivos, como, por ejemplo, pérdida de datos activa, situación en peligro o denegación de servicios.

Ejemplo

```
"Severity": {
    "Label": "CRITICAL",
    "Normalized": 90,
    "Original": "CRITICAL"
}
```

Title

El título de un hallazgo. Este campo puede contener texto reutilizable no específico o información específica de esta instancia del hallazgo.

En el caso de los resultados de control, este campo proporciona el título del control. Este campo no hace referencia a un estándar si activa los resultados de control consolidados.

Ejemplo

```
"Title": "AWS Config should be enabled"
```

Tipos

Uno o varios tipos de hallazgos en el formato de *namespace*/*category*/*classifier* que clasifica un hallazgo. Este campo no hace referencia a un estándar si activa los resultados de control consolidados.

`Types` se debe actualizar solo mediante la API `BatchUpdateFindings`.

Los proveedores de resultados que deseen proporcionar un valor para `Types` deben utilizar el atributo `Types` en `FindingProviderFields`.

En la siguiente lista, las viñetas de nivel superior son espacios de nombres, las viñetas de segundo nivel son categorías y las viñetas de tercer nivel son clasificadores. Recomendamos que los proveedores de resultado utilicen espacios de nombres definidos para ayudar a ordenar y agrupar los resultados. Se recomienda el uso de las categorías y clasificadores definidos, pero no son obligatorios. Sólo el espacio de nombres Comprobaciones de software y configuración tiene clasificadores definidos.

Puede definir una ruta parcial para namespace/category /classifier. Por ejemplo, los siguientes tipos de hallazgo son válidos:

- TTP
- TTPs/Defense Evasión
- TTPs/Defense Evasion/CloudTrailStopped

Las categorías de tácticas, técnicas y procedimientos (TTP) en la siguiente lista se alinean con MITRE ATT&CK MatrixTM. Los comportamientos inusuales reflejan un comportamiento general inusual, como anomalías estadísticas generales y no están alineados con un TTP específico. Sin embargo, puede clasificar un hallazgo tanto con tipos de hallazgo de Comportamientos inusuales como TTP.

Lista de espacios de nombres, categorías y clasificadores:

- Comprobaciones de configuración y software
  - Vulnerabilidades
    - CVE
  - AWS Mejores prácticas de seguridad
    - Accesibilidad de red

    - Análisis del comportamiento del tiempo de ejecución
- Estándares del sector y normativos
    - AWS Mejores prácticas fundamentales de seguridad
    - Indicadores de referencia de fortalecimiento de host de CIS
    - Punto de referencia de CIS AWS Foundations
    - PCI-DSS
    - Controles Cloud Security Alliance
    - Controles ISO 90001
    - Controles ISO 27001
    - Controles ISO 27017
    - Controles ISO 27018
    - SOC 1
    - SOC 2
    - Controles HIPAA (EE. UU.)
    - Controles 800-53 de NIST (EE. UU.)
    - Controles de CSF del NIST (EE. UU.)
    - Controles IRAP (Australia)
    - K-ISMS Controls (Corea)
    - Controles MTCS (Singapur)
    - Controles FISC (Japón)
    - Controles My Number Act (Japón)
    - Controles ENS (España)
    - Controles Cyber Essentials Plus (Reino Unido)
    - G-Cloud Controls (Reino Unido)
    - Controles C5 (Alemania)
    - IT-Grundschutz Controls (Alemania)
    - Controles del RGPD (Europa)
    - Controles TISAX (Europa)
- Administración de parches

- TTP

  - Acceso inicial
  - Ejecución
  - Persistencia
  - Escalado de privilegios
  - Evasión de defensa
  - Acceso a credenciales
  - Discovery
  - Movimiento lateral
  - Recopilación
  - Comando y control
- Efectos
  - Exposición de datos
  - Filtración de datos
  - Destrucción de datos
  - Ataques de denegación de servicio
  - Consumo de recursos
- Comportamientos inusuales
  - Aplicación
  - Flujo de red
  - Dirección IP
  - Usuario
  - VM
  - Container
  - Sin servidor
  - Proceso
  - Base de datos
  - Datos
- Identificaciones de información confidencial
  - PII

  - Contraseñas

- Cuestiones legales
- Datos financieros
- Seguridad
- Usuarios

Ejemplo

```
"Types": [
    "Software and Configuration Checks/Vulnerabilities/CVE"
]
```

UpdatedAt

Indica cuándo fue la última vez que el proveedor de resultados actualizó el registro de resultado.

Esta marca de tiempo refleja la hora en que el registro de resultado se actualizó por última vez o por última vez. En consecuencia, puede diferir de la marca de tiempo `LastObservedAt`, que refleja cuándo se observó por última vez o más recientemente el evento o la vulnerabilidad.

Al actualizar el registro del hallazgo, debe actualizar esta marca temporal con la marca temporal actual. Tras la creación de un registro del resultado, las marcas temporales `CreatedAt` y `UpdatedAt` deben actualizarse a la misma marca temporal. Después de una actualización del registro del resultado, el valor de este campo debe ser el más reciente frente a todos los valores anteriores que contenía.

Tenga en cuenta que `UpdatedAt` no se puede actualizar mediante la operación `BatchUpdateFindings`. Usted solo puede actualizarlo mediante la operación `BatchImportFindings`.

Ejemplo

```
"UpdatedAt": "2017-04-22T13:22:13.933Z"
```

Atributos de nivel superior opcionales del ASFF

Los siguientes atributos de nivel superior del formato de búsqueda de AWS seguridad (ASFF) son opcionales para las conclusiones del CSPM de Security Hub. Para obtener más información sobre estos atributos, consulte AwsSecurityFinding en la Referencia de la API de AWS Security Hub.

Action

El objeto `Action` proporciona detalles sobre una acción que afecta a un recurso o que se realizó respecto a este.

Ejemplo

```
"Action": {
    "ActionType": "PORT_PROBE",
    "PortProbeAction": {
        "PortProbeDetails": [
            {
                "LocalPortDetails": {
                    "Port": 80,
                    "PortName": "HTTP"
                  },
                "LocalIpDetails": {
                     "IpAddressV4": "192.0.2.0"
                 },
                "RemoteIpDetails": {
                    "Country": {
                        "CountryName": "Example Country"
                    },
                    "City": {
                        "CityName": "Example City"
                    },
                   "GeoLocation": {
                       "Lon": 0,
                       "Lat": 0
                   },
                   "Organization": {
                       "AsnOrg": "ExampleASO",
                       "Org": "ExampleOrg",
                       "Isp": "ExampleISP",
                       "Asn": 64496
                   }
                }
            }
        ],
        "Blocked": false
    }
}
```

AwsAccountName

El Cuenta de AWS nombre al que se aplica el hallazgo.

Ejemplo

```
"AwsAccountName": "jane-doe-testaccount"
```

CompanyName

El nombre de la empresa del producto que generó el resultado. Para los hallazgos basados en el control, la empresa es AWS.

El CSPM de Security Hub completa este atributo de forma automática para cada resultado. No puede actualizarlo mediante `BatchImportFindings` o `BatchUpdateFindings`. La excepción a esto es cuando se utiliza una integración personalizada. Consulte the section called “Integraciones de productos personalizados”.

Cuando usa la consola del CSPM de Security Hub para filtrar resultados por nombre de empresa, se utiliza este atributo. Cuando usa la API del CSPM de Security Hub para filtrar resultados por nombre de empresa, utiliza el atributo `aws/securityhub/CompanyName` dentro de `ProductFields`. El CSPM de Security Hub no sincroniza esos dos atributos.

Ejemplo

```
"CompanyName": "AWS"
```

Conformidad

El objeto `Compliance` normalmente proporciona detalles sobre un resultado de control, como los estándares aplicables y el estado de la comprobación de control.

Ejemplo

```
"Compliance": {
    "AssociatedStandards": [
        {"StandardsId": "standards/aws-foundational-security-best-practices/v/1.0.0"},
        {"StandardsId": "standards/service-managed-aws-control-tower/v/1.0.0"},
        {"StandardsId": "standards/nist-800-53/v/5.0.0"}
```

```
    ],
    "RelatedRequirements": [
        "NIST.800-53.r5 AC-4",
        "NIST.800-53.r5 AC-4(21)",
        "NIST.800-53.r5 SC-7",
        "NIST.800-53.r5 SC-7(11)",
        "NIST.800-53.r5 SC-7(16)",
        "NIST.800-53.r5 SC-7(21)",
        "NIST.800-53.r5 SC-7(4)",
        "NIST.800-53.r5 SC-7(5)"
    ],
    "SecurityControlId": "EC2.18",
    "SecurityControlParameters":[
        {
            "Name": "authorizedTcpPorts",
            "Value": ["80", "443"]
        },
        {
            "Name": "authorizedUdpPorts",
            "Value": ["427"]
        }
    ],
    "Status": "NOT_AVAILABLE",
    "StatusReasons": [
        {
            "ReasonCode": "CONFIG_RETURNS_NOT_APPLICABLE",
            "Description": "This finding has a compliance status of NOT AVAILABLE
 because AWS Config sent Security Hub CSPM a finding with a compliance state of Not
 Applicable. The potential reasons for a Not Applicable finding from Config are that
 (1) a resource has been moved out of scope of the Config rule; (2) the Config rule has
 been deleted; (3) the resource has been deleted; or (4) the logic of the Config rule
 itself includes scenarios where Not Applicable is returned. The specific reason why
 Not Applicable is returned is not available in the Config rule evaluation."
        }
    ]
}
```

Confianza

La probabilidad de que un resultado identifique de forma precisa el comportamiento o problema que se pretendía identificar.

`Confidence` solo debe actualizarse mediante `BatchUpdateFindings`.

Los proveedores de resultados que deseen proporcionar un valor para `Confidence` deben utilizar el atributo `Confidence` en `FindingProviderFields`. Consulte the section called “Actualización de los hallazgos con FindingProviderFields”.

`Confidence` recibe una puntuación de 0-100 en base a una escala de proporción, donde 0 significa 0 por cien de confianza y 100 significa 100 por cien de confianza. Por ejemplo, una detección de filtración de datos en base a una desviación estadística del tráfico de red tiene una confianza mucho más baja porque no se ha verificado una filtración real.

Ejemplo

```
"Confidence": 42
```

Criticidad

El nivel de importancia que se asigna a los recursos asociados con el resultado.

`Criticality` solo debe actualizarse llamando a la operación de la API `BatchUpdateFindings`. No actualice este objeto con `BatchImportFindings`.

Los proveedores de resultados que deseen proporcionar un valor para `Criticality` deben utilizar el atributo `Criticality` en `FindingProviderFields`. Consulte the section called “Actualización de los hallazgos con FindingProviderFields”.

`Criticality` se puntúa de 0-100, mediante una escala de proporción que solo admite números enteros. Una puntuación de 0 significa que los recursos subyacentes no tienen mucha importancia y una puntuación de 100 está reservada para los recursos de importancia vital.

Para cada recurso, tenga en cuenta lo siguiente al asignar `Criticality`:

- ¿Contiene el recurso afectado información confidencial (por ejemplo, un bucket de S3 con PII)?
- ¿Permite el recurso afectado que un adversario profundice su acceso o amplíe sus capacidades de llevar a cabo actividades malintencionadas adicionales (por ejemplo, cuenta sysadmin en peligro)?
- ¿Es el recurso un activo vital de la empresa (por ejemplo, un sistema empresarial clave que si estuviera en peligro podría afectar a los ingresos significativamente)?

Puede utilizar las siguientes directrices:

- Un recurso que habilita sistemas esenciales o que contiene un alto nivel de información confidencial puede puntuar en el intervalo de 75-100.
- Un recurso que habilita sistemas importantes (pero no esenciales) o que contiene datos moderadamente importantes puede puntuar en el intervalo de 25-75.
- Un recurso que habilita sistemas no importantes o que no contienen información confidencial debe puntuar en el intervalo de 0-24.

Ejemplo

```
"Criticality": 99
```

Detección

El `Detection` objeto proporciona detalles sobre una secuencia de ataque detectada por Amazon GuardDuty Extended Threat Detection. GuardDuty genera una secuencia de ataque que detecta cuando varios eventos coinciden con una actividad potencialmente sospechosa. Para recibir los resultados de la secuencia de GuardDuty ataque en AWS Security Hub CSPM, debes tener GuardDuty habilitada esta opción en tu cuenta. Para obtener más información, consulte Amazon GuardDuty Extended Threat Detection en la Guía del GuardDuty usuario de Amazon.

Ejemplo

```
"Detection": {
    "Sequence": {
     "Uid": "1111111111111-184ec3b9-cf8d-452d-9aad-f5bdb7afb010",
     "Actors": [{
      "Id": "USER:AROA987654321EXAMPLE:i-b188560f:1234567891",
      "Session": {
       "Uid": "1234567891",
       "MfAStatus": "DISABLED",
       "CreatedTime": "1716916944000",
       "Issuer": "arn:aws:s3:::amzn-s3-demo-destination-bucket"
      },
      "User": {
       "CredentialUid": "ASIAIOSFODNN7EXAMPLE",
       "Name": "ec2_instance_role_production",
       "Type": "AssumedRole",
       "Uid": "AROA987654321EXAMPLE:i-b188560f",
       "Account": {
        "Uid": "AccountId",
```

```
        "Name": "AccountName"
       }
      }
     }],
     "Endpoints": [{
      "Id": "EndpointId",
      "Ip": "203.0.113.1",
      "Domain": "example.com",
      "Port": 4040,
      "Location": {
       "City": "New York",
       "Country": "US",
       "Lat": 40.7123,
       "Lon": -74.0068
      },
      "AutonomousSystem": {
       "Name": "AnyCompany",
       "Number": 64496
      },
      "Connection": {
       "Direction": "INBOUND"
      }
     }],
     "Signals": [{
      "Id": "arn:aws:guardduty:us-east-1:123456789012:detector/
d0bfe135ab8b4dd8c3eaae7df9900073/finding/535a382b1bcc44d6b219517a29058fb7",
      "Title": "Someone ran a penetration test tool on your account.",
      "ActorIds": ["USER:AROA987654321EXAMPLE:i-b188560f:1234567891"],
      "Count": 19,
      "FirstSeenAt": 1716916943000,
      "SignalIndicators": [
       {
        "Key": "ATTACK_TACTIC",
        "Title": "Attack Tactic",
        "Values": [
         "Impact"
        ]
       },
       {
        "Key": "HIGH_RISK_API",
        "Title": "High Risk Api",
        "Values": [
         "s3:DeleteObject"
        ]
```

```
        },
        {
         "Key": "ATTACK_TECHNIQUE",
         "Title": "Attack Technique",
         "Values": [
          "Data Destruction"
         ]
        },
       ],
       "LastSeenAt": 1716916944000,
       "Name": "Test:IAMUser/KaliLinux",
       "ResourceIds": [
        "arn:aws:s3:::amzn-s3-demo-destination-bucket"
       ],
       "Type": "FINDING"
      }],
      "SequenceIndicators": [
       {
        "Key": "ATTACK_TACTIC",
        "Title": "Attack Tactic",
        "Values": [
         "Discovery",
         "Exfiltration",
         "Impact"
        ]
       },
       {
        "Key": "HIGH_RISK_API",
        "Title": "High Risk Api",
        "Values": [
         "s3:DeleteObject",
         "s3:GetObject",
         "s3:ListBuckets"
         "s3:ListObjects"
        ]
       },
       {
        "Key": "ATTACK_TECHNIQUE",
        "Title": "Attack Technique",
        "Values": [
         "Cloud Service Discovery",
         "Data Destruction"
        ]
       }
```

```
     ]
    }
}
```

FindingProviderFields

`FindingProviderFields` incluye los siguientes atributos:

- `Confidence`
- `Criticality`
- `RelatedFindings`
- `Severity`
- `Types`

Los campos anteriores están anidados debajo del objeto `FindingProviderFields`, pero tienen análogos del mismo nombre que los campos del ASFF de nivel superior. Cuando un proveedor envía un nuevo resultado al CSPM de Security Hub, el CSPM de Security Hub completa automáticamente el objeto `FindingProviderFields` si está vacío, según los campos de nivel superior correspondientes.

Los proveedores de resultados pueden actualizar `FindingProviderFields` mediante la operación `BatchImportFindings` de la API del CSPM de Security Hub. Los proveedores de resultados no pueden actualizar este objeto mediante `BatchUpdateFindings`.

Para obtener detalles sobre cómo el CSPM de Security Hub maneja las actualizaciones desde `BatchImportFindings` hacia `FindingProviderFields` y hacia los atributos de nivel superior correspondientes, consulte the section called “Actualización de los hallazgos con FindingProviderFields”.

Los clientes pueden actualizar los campos de nivel superior mediante la operación `BatchUpdateFindings`. Los clientes no pueden actualizar `FindingProviderFields`.

Ejemplo

```
"FindingProviderFields": {
    "Confidence": 42,
    "Criticality": 99,
    "RelatedFindings":[
      {
```

```
        "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
        "Id": "123e4567-e89b-12d3-a456-426655440000"
      }
    ],
    "Severity": {
        "Label": "MEDIUM",
        "Original": "MEDIUM"
    },
    "Types": [ "Software and Configuration Checks/Vulnerabilities/CVE" ]
}
```

FirstObservedAt

Indica el momento en que se observó por primera vez el posible problema o evento de seguridad que aparece en el resultado.

Esta marca de tiempo indica cuándo se observó por primera vez el evento o la vulnerabilidad. Por lo tanto, puede diferir de la marca de tiempo `CreatedAt`, la cual refleja cuándo se creó este registro del resultado.

En el caso de los resultados de controles que genera y actualiza el CSPM de Security Hub, esta marca de tiempo también puede indicar cuándo cambió por última vez el estado de cumplimiento de un recurso. Para otros tipos de resultados, esta marca de tiempo debe permanecer inmutable entre las actualizaciones del registro del resultado, pero puede actualizarse si se determina una marca de tiempo más precisa.

Ejemplo

```
"FirstObservedAt": "2017-03-22T13:22:13.933Z"
```

LastObservedAt

Indica el momento en que el producto de resultados de seguridad observó por última vez el posible problema o evento capturado por un resultado.

Esta marca de tiempo indica cuándo se observó por última vez el evento o la vulnerabilidad. Por lo tanto, puede diferir de la marca de tiempo `UpdatedAt`, que refleja cuándo se actualizó este registro de resultados por última vez.

Puede proporcionar esta marca temporal, pero no es necesaria tras la primera observación. Si completa este campo en la primera observación, la marca de tiempo debe coincidir con la marca de

tiempo `FirstObservedAt`. Debe actualizar este campo para reflejar la marca temporal observada más recientemente o por última vez cada vez se observa un resultado.

Ejemplo

```
"LastObservedAt": "2017-03-23T13:22:13.933Z"
```

Malware

El objeto `Malware` proporciona una lista de malware relacionada con un resultado.

Ejemplo

```
"Malware": [
    {
        "Name": "Stringler",
        "Type": "COIN_MINER",
        "Path": "/usr/sbin/stringler",
        "State": "OBSERVED"
    }
]
```

Network (Retired)

El objeto `Network` brinda información relacionada con la red de un resultado.

Este objeto se ha retirado. Para proporcionar estos datos, puede asignar los datos a un recurso en `Resources` o utilizar el objeto `Action`.

Ejemplo

```
"Network": {
    "Direction": "IN",
    "OpenPortRange": {
        "Begin": 443,
        "End": 443
    },
    "Protocol": "TCP",
    "SourceIpV4": "1.2.3.4",
    "SourceIpV6": "FE80:CD00:0000:0CDE:1257:0000:211E:729C",
    "SourcePort": "42",
    "SourceDomain": "example1.com",
```

```
    "SourceMac": "00:0d:83:b1:c0:8e",
    "DestinationIpV4": "2.3.4.5",
    "DestinationIpV6": "FE80:CD00:0000:0CDE:1257:0000:211E:729C",
    "DestinationPort": "80",
    "DestinationDomain": "example2.com"
}
```

NetworkPath

El objeto `NetworkPath` proporciona información sobre una ruta de red relacionada con un resultado. Cada entrada en `NetworkPath` representa un componente de la ruta.

Ejemplo

```
"NetworkPath" : [
    {
        "ComponentId": "abc-01a234bc56d8901ee",
        "ComponentType": "AWS::EC2::InternetGateway",
        "Egress": {
            "Destination": {
                "Address": [ "192.0.2.0/24" ],
                "PortRanges": [
                    {
                        "Begin": 443,
                        "End": 443
                    }
                ]
            },
            "Protocol": "TCP",
            "Source": {
                "Address": ["203.0.113.0/24"]
            }
        },
        "Ingress": {
            "Destination": {
                "Address": [ "198.51.100.0/24" ],
                "PortRanges": [
                    {
                        "Begin": 443,
                        "End": 443
                    }
                 ]
            },
```

```
            "Protocol": "TCP",
            "Source": {
                "Address": [ "203.0.113.0/24" ]
            }
        }
    }
]
```

Nota

El objeto `Note` especifica una nota definida por el usuario que se puede añadir a un resultado.

Un proveedor de hallazgos puede proporcionar una nota inicial para un hallazgo, pero después no puede agregar más notas. Solo puede actualizar una nota con `BatchUpdateFindings`.

Ejemplo

```
"Note": {
    "Text": "Don't forget to check under the mat.",
    "UpdatedBy": "jsmith",
    "UpdatedAt": "2018-08-31T00:15:09Z"
}
```

PatchSummary

El objeto `PatchSummary` proporciona un resumen del estado de conformidad del parche de una instancia con respecto a un estándar de cumplimiento seleccionado.

Ejemplo

```
"PatchSummary" : {
    "FailedCount" : 0,
    "Id" : "pb-123456789098",
    "InstalledCount" : 100,
    "InstalledOtherCount" : 1023,
    "InstalledPendingReboot" : 0,
    "InstalledRejectedCount" : 0,
    "MissingCount" : 100,
    "Operation" : "Install",
    "OperationEndTime" : "2018-09-27T23:39:31Z",
    "OperationStartTime" : "2018-09-27T23:37:31Z",
    "RebootOption" : "RebootIfNeeded"
```

```
}
```

Proceso

El objeto `Process` proporciona detalles relacionados con el proceso acerca del resultado.

Ejemplo:

```
"Process": {
    "LaunchedAt": "2018-09-27T22:37:31Z",
    "Name": "syslogd",
    "ParentPid": 56789,
    "Path": "/usr/sbin/syslogd",
    "Pid": 12345,
    "TerminatedAt": "2018-09-27T23:37:31Z"
}
```

ProcessedAt

Indica el momento en que el CSPM de Security Hub recibió un resultado y comenzó a procesarlo.

Esto difiere de `CreatedAt` y `UpdatedAt`, que son marcas de tiempo obligatorias relacionadas con la interacción del proveedor del resultado con el problema de seguridad y con el propio resultado. La marca de tiempo `ProcessedAt` señala cuándo el CSPM de Security Hub inicia el procesamiento de un resultado. Un resultado aparece en la cuenta del usuario después de que el procesamiento finaliza.

```
"ProcessedAt": "2023-03-23T13:22:13.933Z"
```

ProductFields

Tipo de datos en el que los productos de búsqueda de seguridad pueden incluir detalles adicionales específicos de la solución que no forman parte del formato de búsqueda de AWS seguridad definido.

En el caso de los resultados generados por los controles del CSPM de Security Hub, `ProductFields` incluye información sobre el control. Consulte the section called “Generación y actualización de los resultados de control”.

Este campo no debe contener datos redundantes ni debe contener datos que entren en conflicto con los campos del formato de búsqueda AWS de seguridad.

El prefijo `aws/` "» representa un espacio de nombres reservado únicamente para AWS productos y servicios y no debe enviarse junto con los resultados de integraciones de terceros.

Aunque no es necesario, los productos deben formatear los nombres de los campos como `company-id/product-id/field-name`, donde el `company-id` y el `product-id` coinciden con los suministrados en el `ProductArn` del hallazgo.

Los campos que hacen referencia a `Archival` se usan cuando el CSPM de Security Hub archiva un resultado existente. Por ejemplo, el CSPM de Security Hub archiva los resultados existentes cuando desactiva un control o un estándar y cuando activa o desactiva los resultados consolidados de controles.

Este campo también puede incluir información sobre el estándar que incluye el control que produjo el resultado.

Ejemplo

```
"ProductFields": {
    "API", "DeleteTrail",
    "ArchivalReasons:0/Description": "The finding is in an ARCHIVED state because
 consolidated control findings has been turned on or off. This causes findings in the
 previous state to be archived when new findings are being generated.",
    "ArchivalReasons:0/ReasonCode": "CONSOLIDATED_CONTROL_FINDINGS_UPDATE",
    "aws/inspector/AssessmentTargetName": "My prod env",
    "aws/inspector/AssessmentTemplateName": "My daily CVE assessment",
    "aws/inspector/RulesPackageName": "Common Vulnerabilities and Exposures",
    "generico/secure-pro/Action.Type", "AWS_API_CALL",
    "generico/secure-pro/Count": "6",
    "Service_Name": "cloudtrail.amazonaws.com"
}
```

ProductName

Proporciona el nombre del producto que generó el resultado. En el caso de los resultados basados en controles, el nombre del producto es CSPM de Security Hub.

El CSPM de Security Hub completa este atributo de forma automática para cada resultado. No puede actualizarlo mediante `BatchImportFindings` o `BatchUpdateFindings`. La excepción a esto es cuando se utiliza una integración personalizada. Consulte the section called “Integraciones de productos personalizados”.

Cuando usa la consola del CSPM de Security Hub para filtrar resultados por nombre de producto, utiliza este atributo.

Cuando usa la API del CSPM de Security Hub para filtrar resultados por nombre de producto, utiliza el atributo `aws/securityhub/ProductName` dentro de `ProductFields`.

El CSPM de Security Hub no sincroniza esos dos atributos.

RecordState

El estado de registro de un a resultado.

De forma predeterminada, los hallazgos generados inicialmente por un servicio se consideran `ACTIVE`.

El estado `ARCHIVED` indica que un hallazgo estará oculto a la vista. Los resultados archivados no se eliminan de inmediato. Puede buscar, examinar e informar sobre ellos. El CSPM de Security Hub archiva automáticamente los resultados basados en controles cuando el recurso asociado se elimina, el recurso no existe o el control está desactivado.

`RecordState` está destinado a los proveedores de resultados y solo se puede actualizar mediante la operación `BatchImportFindings`. No puede actualizarlo mediante la operación `BatchUpdateFindings`.

Para hacer un seguimiento del estado de la investigación sobre un resultado, utilice `Workflow` en lugar de `RecordState`.

Si el estado del registro cambia de `ARCHIVED` a `ACTIVE` y el estado del flujo de trabajo del resultado es `NOTIFIED` o `RESOLVED`, el CSPM de Security Hub cambia automáticamente el estado del flujo de trabajo a `NEW`.

Ejemplo

```
"RecordState": "ACTIVE"
```

Region

Especifica a Región de AWS partir del cual se generó la búsqueda.

El CSPM de Security Hub completa este atributo de forma automática para cada resultado. No puede actualizarlo mediante `BatchImportFindings` o `BatchUpdateFindings`.

Ejemplo

```
"Region": "us-west-2"
```

RelatedFindings

Proporciona una lista de resultados relacionados con el resultado actual.

`RelatedFindings` solo debe actualizarse con la operación de la API `BatchUpdateFindings`. No debe actualizar este objeto con `BatchImportFindings`.

Para las solicitudes `BatchImportFindings`, los proveedores de resultados deben utilizar el objeto `RelatedFindings` en `FindingProviderFields`.

Para ver las descripciones de los atributos `RelatedFindings`, consulte `RelatedFinding` en la referencia de la API de AWS Security Hub .

Ejemplo

```
"RelatedFindings": [
    { "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
      "Id": "123e4567-e89b-12d3-a456-426655440000" },
    { "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
      "Id": "AcmeNerfHerder-111111111111-x189dx7824" }
]
```

RiskAssessment

Ejemplo

```
"RiskAssessment": {
    "Posture": {
        "FindingTotal": 4,
        "Indicators": [
            {
                "Type": "Reachability",
                "Findings": [
                    {
                        "Id": "arn:aws:inspector2:us-
east-2:123456789012:finding/1234567890abcdef0",
                        "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/
inspector",
```

```
                        "Title": "Finding title"
                    },
                    {
                        "Id": "arn:aws:inspector2:us-east-2:123456789012:finding/
abcdef01234567890",
                        "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/
inspector",
                        "Title": "Finding title"
                    }
                ]
            },
            {
                "Type": "Vulnerability",
                "Findings": [
                    {
                        "Id": "arn:aws:inspector2:us-
east-2:123456789012:finding/021345abcdef6789",
                        "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/
inspector",
                        "Title": "Finding title"
                    },
                    {
                        "Id": "arn:aws:inspector2:us-
east-2:123456789012:finding/021345ghijkl6789",
                        "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/
inspector",
                        "Title": "Finding title"
                    }
                ]
            }
        ]
    }
}
```

Corrección

El objeto `Remediation` proporciona información sobre los pasos de remediación recomendados para abordar el resultado.

Ejemplo

```
"Remediation": {
    "Recommendation": {
```

```
        "Text": "For instructions on how to fix this issue, see the AWS Security Hub
 CSPM documentation for EC2.2.",
        "Url": "https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation"
    }
}
```

Muestra

Especifica si el resultado es un resultado de muestra.

```
"Sample": true
```

SourceUrl

El objeto `SourceUrl` brinda una URL que enlaza a una página sobre el resultado actual en el producto de resultados.

```
"SourceUrl": "http://sourceurl.com"
```

ThreatIntelIndicators

El objeto `ThreatIntelIndicator` brinda detalles de información de amenazas que están relacionados con un resultado.

Ejemplo

```
"ThreatIntelIndicators": [
  {
    "Category": "BACKDOOR",
    "LastObservedAt": "2018-09-27T23:37:31Z",
    "Source": "Threat Intel Weekly",
    "SourceUrl": "http://threatintelweekly.org/backdoors/8888",
    "Type": "IPV4_ADDRESS",
    "Value": "8.8.8.8",
  }
]
```

Amenazas

El objeto Threats proporciona detalles sobre la amenaza detectada por un resultado.

Ejemplo

```
"Threats": [{
    "FilePaths": [{
        "FileName": "b.txt",
        "FilePath": "/tmp/b.txt",
        "Hash": "sha256",
        "ResourceId": "arn:aws:ec2:us-west-2:123456789012:volume/vol-032f3bdd89aee112f"
    }],
    "ItemCount": 3,
    "Name": "Iot.linux.mirai.vwisi",
    "Severity": "HIGH"
}]
```

UserDefinedFields

Una lista de pares de cadenas de nombre/valor que están asociados con el resultado. Son campos definidos por el usuario y personalizados que se añaden a un hallazgo. Estos campos se pueden generar de forma automática a través de su configuración específica.

Los proveedores de resultados no deben utilizar este campo para los datos que genera el producto. En su lugar, los proveedores de búsqueda pueden usar el `ProductFields` campo para los datos que no corresponden a ningún campo del formato AWS de búsqueda de seguridad estándar.

Estos campos solo se pueden actualizar con `BatchUpdateFindings`.

Ejemplo

```
"UserDefinedFields": {
    "reviewedByCio": "true",
    "comeBackToLater": "Check this again on Monday"
}
```

VerificationState

Brinda la veracidad de un resultado. Los productos de resultados pueden proporcionar el valor `UNKNOWN` para este campo. Un producto de resultados puede proporcionar este valor para este campo si hay un valor analógico significativo en el sistema del producto de resultados. Este campo suele ser rellenado por una determinación o acción del usuario después de que haya investigado un resultado.

Un proveedor de hallazgos puede proporcionar un valor inicial para este atributo, pero después no puede actualizarlo. Solo puede actualizar este atributo mediante `BatchUpdateFindings`.

```
"VerificationState": "Confirmed"
```

Vulnerabilidades

El objeto Vulnerabilities proporciona una lista de vulnerabilidades asociadas a un resultado.

Ejemplo

```
"Vulnerabilities" : [
    {
        "CodeVulnerabilities": [{
            "Cwes": [
                "CWE-798",
                "CWE-799"
            ],
            "FilePath": {
                "EndLine": 421,
                "FileName": "package-lock.json",
                "FilePath": "package-lock.json",
                "StartLine": 420
            },
                "SourceArn":"arn:aws:lambda:us-east-1:123456789012:layer:AWS-AppConfig-
Extension:114"
        }],
        "Cvss": [
            {
                "BaseScore": 4.7,
                "BaseVector": "AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N",
                "Version": "V3"
            },
            {
                "BaseScore": 4.7,
                "BaseVector": "AV:L/AC:M/Au:N/C:C/I:N/A:N",
                "Version": "V2"
            }
        ],
        "EpssScore": 0.015,
        "ExploitAvailable": "YES",
        "FixAvailable": "YES",
        "Id": "CVE-2020-12345",
        "LastKnownExploitAt": "2020-01-16T00:01:35Z",
        "ReferenceUrls":[
           "http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12418",
```

```
            "http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17563"
        ],
        "RelatedVulnerabilities": ["CVE-2020-12345"],
        "Vendor": {
            "Name": "Alas",
            "Url":"https://alas.aws.amazon.com/ALAS-2020-1337.html",
            "VendorCreatedAt":"2020-01-16T00:01:43Z",
            "VendorSeverity":"Medium",
            "VendorUpdatedAt":"2020-01-16T00:01:43Z"
        },
        "VulnerablePackages": [
            {
                "Architecture": "x86_64",
                "Epoch": "1",
                "FilePath": "/tmp",
                "FixedInVersion": "0.14.0",
                "Name": "openssl",
                "PackageManager": "OS",
                "Release": "16.amzn2.0.3",
                "Remediation": "Update aws-crt to 0.14.0",
                "SourceLayerArn": "arn:aws:lambda:us-west-2:123456789012:layer:id",
                "SourceLayerHash":
 "sha256:c1962c35b63a6ff6ce7df6e042ee82371a605ca9515569edec46ff14f926f001",
                "Version": "1.0.2k"
            }
        ]
    }
]
```

Flujo de trabajo

El objeto `Workflow` proporciona información sobre el estado de la investigación de un resultado.

Este campo está pensado para que los clientes lo utilicen con herramientas de corrección, orquestación y emisión de tickets. No está destinado a proveedores de hallazgos.

Solo puede actualizar el campo `Workflow` con `BatchUpdateFindings`. Los clientes también pueden actualizarlo desde la consola. Consulte the section called “Configuración del estado de flujo de trabajo de los resultados”.

Ejemplo

```
"Workflow": {
```

```
    "Status": "NEW"
}
```

WorkflowState (Retirado)

Este objeto está retirado y se ha sustituido por el campo `Status` del objeto `Workflow`.

Este campo proporciona el estado del flujo de trabajo de un resultado. Los productos de hallazgos puede proporcionar el valor `NEW` para este campo. Un producto de hallazgos puede proporcionar este valor si hay un valor analógico significativo en el sistema del producto de hallazgos.

Ejemplo

```
"WorkflowState": "NEW"
```

Recursos Objeto ASFF

En el formato AWS de búsqueda de seguridad (ASFF), el `Resources` objeto proporciona información sobre los recursos involucrados en una búsqueda. Contiene una matriz de hasta 32 objetos de recursos. Para determinar el formato de los nombres de los recursos, consulte AWS Formato de búsqueda de seguridad (ASFF). Para ver ejemplos de cada objeto de recurso, seleccione un recurso en la siguiente lista.

Temas

- Atributos de recursos en el formato ASFF
- AwsAmazonMQ recursos en ASFF
- AwsApiGateway recursos en ASFF
- AwsAppSync recursos en ASFF
- AwsAthena recursos en ASFF
- AwsAutoScaling recursos en ASFF
- AwsBackup recursos en ASFF
- AwsCertificateManager recursos en ASFF
- AwsCloudFormation recursos en ASFF
- AwsCloudFront recursos en ASFF
- AwsCloudTrail recursos en ASFF

- AwsCloudWatch recursos en ASFF
- AwsCodeBuild recursos en ASFF
- AwsDms recursos en ASFF
- AwsDynamoDB recursos en ASFF
- AwsEc2. recursos en ASFF
- AwsEcr recursos en ASFF
- AwsEcs recursos en ASFF
- AwsEfs recursos en ASFF
- AwsEks recursos en ASFF
- AwsElasticBeanstalk recursos en ASFF
- AwsElasticSearch recursos en ASFF
- AwsElb recursos en ASFF
- AwsEventBridge recursos en ASFF
- AwsGuardDuty recursos en ASFF
- AwsIam recursos en ASFF
- AwsKinesis recursos en ASFF
- AwsKms recursos en ASFF
- AwsLambda
- AwsMsk recursos en ASFF
- AwsNetworkFirewall recursos en ASFF
- AwsOpenSearchService recursos en ASFF
- AwsRds recursos en ASFF
- AwsRedshift recursos en ASFF
- AwsRoute53 recursos en ASFF
- Ass3 recursos en ASFF
- AwsSageMaker recursos en ASFF
- AwsSecretsManager recursos en ASFF
- AwsSns recursos en ASFF

- AwsSqs recursos en ASFF
- AwsSsm recursos en ASFF
- AwsStepFunctions recursos en ASFF
- AwsWaf recursos en ASFF
- AwsXray recursos en ASFF
- CodeRepository objeto en ASFF
- Container objeto en ASFF
- Otro objeto en ASFF

Atributos de recursos en el formato ASFF

A continuación se muestran descripciones y ejemplos del `Resources` objeto en el formato de búsqueda AWS de seguridad (ASFF). Para obtener más información acerca de estos campos, consulte Recursos.

ApplicationArn

Identifica el nombre de recurso de Amazon (ARN) de la aplicación implicada en el resultado.

Ejemplo

```
"ApplicationArn": "arn:aws:resource-groups:us-west-2:123456789012:group/
SampleApp/1234567890abcdef0"
```

ApplicationName

Identifica el nombre de la aplicación implicada en el resultado.

Ejemplo

```
"ApplicationName": "SampleApp"
```

DataClassification

El campo DataClassification proporciona información sobre los datos confidenciales que se detectaron en el recurso.

Ejemplo

```
"DataClassification": {
    "DetailedResultsLocation": "Path_to_Folder_Or_File",
    "Result": {
        "MimeType": "text/plain",
        "SizeClassified": 2966026,
        "AdditionalOccurrences": false,
        "Status": {
            "Code": "COMPLETE",
            "Reason": "Unsupportedfield"
        },
       "SensitiveData": [
            {
                "Category": "PERSONAL_INFORMATION",
                "Detections": [
                    {
                        "Count": 34,
                        "Type": "GE_PERSONAL_ID",
                        "Occurrences": {
                            "LineRanges": [
                                {
                                    "Start": 1,
                                    "End": 10,
                                    "StartColumn": 20
                                }
                            ],
                            "Pages": [],
                            "Records": [],
                            "Cells": []
                        }
                    },
                    {
                        "Count": 59,
                        "Type": "EMAIL_ADDRESS",
                        "Occurrences": {
                            "Pages": [
                                {
                                    "PageNumber": 1,
                                    "OffsetRange": {
                                        "Start": 1,
                                        "End": 100,
                                        "StartColumn": 10
                                     },
```

```
                                "LineRange": {
                                    "Start": 1,
                                    "End": 100,
                                    "StartColumn": 10
                                }
                            }
                        ]
                    }
                },
                {
                    "Count": 2229,
                    "Type": "URL",
                    "Occurrences": {
                       "LineRanges": [
                           {
                               "Start": 1,
                               "End": 13
                           }
                       ]
                    }
                },
                {
                    "Count": 13826,
                    "Type": "NameDetection",
                    "Occurrences": {
                         "Records": [
                             {
                                 "RecordIndex": 1,
                                 "JsonPath": "$.ssn.value"
                             }
                         ]
                    }
                },
                {
                    "Count": 32,
                    "Type": "AddressDetection"
                }
            ],
            "TotalCount": 32
        }
    ],
    "CustomDataIdentifiers": {
        "Detections": [
             {
```

```
                    "Arn": "1712be25e7c7f53c731fe464f1c869b8",
                    "Name": "1712be25e7c7f53c731fe464f1c869b8",
                    "Count": 2,
                }
            ],
            "TotalCount": 2
        }
    }
}
```

Details

El campo Details proporciona información adicional sobre un único recurso que utiliza los objetos adecuados. Cada recurso debe facilitarse en un objeto de recurso independiente en el objeto `Resources`.

Tenga en cuenta que si el tamaño del resultado supera el máximo de 240 KB, el objeto `Details` se elimina del resultado. Para ver los resultados de los controles que utilizan AWS Config reglas, puede ver los detalles del recurso en la AWS Config consola.

Security Hub CSPM proporciona un conjunto de detalles de los recursos disponibles para los tipos de recursos compatibles. Estos detalles corresponden a los valores del objeto `Type`. Siempre que sea posible, utilice los tipos proporcionados.

Por ejemplo, si el recurso es un bucket de S3, entonces establezca el recurso `Type` en `AwsS3Bucket` y proporcione los detalles del recurso en el objeto `AwsS3Bucket`.

El objeto `Other` le permite proporcionar campos y valores personalizados. Utilice el objeto `Other` en los siguientes casos:

- El tipo de recurso (el valor del recurso `Type`) no tiene un objeto con detalles correspondiente. Para proporcionar detalles sobre el recurso, utilice el objeto `Other`.
- El objeto del tipo de recurso no incluye todos los campos que desea rellenar. En este caso, utilice el objeto de detalles del tipo de recurso para rellenar los campos disponibles. Utilice el objeto `Other` para rellenar los campos que no están en el subcampo específico de ese objeto.
- El tipo de recurso no es uno de los tipos proporcionados. En este caso, establezca `Resource.Type` en `Other` y utilice el objeto `Other` para rellenar los detalles.

Ejemplo

```
"Details": {
  "AwsEc2Instance": {
    "IamInstanceProfileArn": "arn:aws:iam::123456789012:role/IamInstanceProfileArn",
    "ImageId": "ami-79fd7eee",
    "IpV4Addresses": ["1.1.1.1"],
    "IpV6Addresses": ["2001:db8:1234:1a2b::123"],
    "KeyName": "testkey",
    "LaunchedAt": "2018-09-29T01:25:54Z",
    "MetadataOptions": {
      "HttpEndpoint": "enabled",
      "HttpProtocolIpv6": "enabled",
      "HttpPutResponseHopLimit": 1,
      "HttpTokens": "optional",
      "InstanceMetadataTags": "disabled"
    },
    "NetworkInterfaces": [
    {
      "NetworkInterfaceId": "eni-e5aa89a3"
    }
    ],
    "SubnetId": "PublicSubnet",
    "Type": "i3.xlarge",
    "VirtualizationType": "hvm",
    "VpcId": "TestVPCIpv6"
  },
  "AwsS3Bucket": {
    "OwnerId": "da4d66eac431652a4d44d490a00500bded52c97d235b7b4752f9f688566fe6de",
    "OwnerName": "acmes3bucketowner"
  },
  "Other": { "LightPen": "blinky", "SerialNo": "1234abcd"}
}
```

Id

El identificador para el tipo de recurso determinado.

Para AWS los recursos que se identifican mediante los nombres de recursos de Amazon (ARN), este es el ARN.

En el AWS caso de los recursos que carecen de ARN, este es el identificador definido por el AWS servicio que creó el recurso.

En el caso de AWS los recursos no relacionados con los recursos, se trata de un identificador único que está asociado al recurso.

Ejemplo

```
"Id": "arn:aws:s3:::amzn-s3-demo-bucket"
```

Partición

La partición en la que se encuentra el recurso. Una partición es un grupo de Regiones de AWS. Cada una Cuenta de AWS tiene como ámbito una partición.

Se admiten las siguientes particiones:

- `aws` – Regiones de AWS
- `aws-cn`: regiones de China
- `aws-us-gov` – AWS GovCloud (US) Region

Ejemplo

```
"Partition": "aws"
```

Region

El código Región de AWS donde se encuentra este recurso. Para ver una lista de códigos de regiones, consulte Puntos de conexión regionales.

Ejemplo

```
"Region": "us-west-2"
```

ResourceRole

Identifica la característica del recurso en el resultado. Un recurso es el objetivo de la actividad de resultado o el actor que realizó la actividad.

Ejemplo

```
"ResourceRole": "target"
```

Tags

Este campo proporciona información sobre la clave y el valor de la etiqueta del recurso implicado en un resultado. Puede etiquetar los recursos compatibles con el `GetResources` funcionamiento de la API de Grupos de recursos de AWS etiquetado. El CSPM de Security Hub llama a esta operación a través del rol vinculado al servicio y recupera las etiquetas de los recursos si el `Resource.Id` campo del formato de búsqueda de AWS seguridad (ASFF) se rellena con el ARN del recurso. AWS Los identificadores de recursos no válidos se omiten.

Puede agregar etiquetas de recursos a los hallazgos que recopila el CSPM de Security Hub, incluidos los hallazgos de productos integrados y de terceros. Servicios de AWS

Cuando agrega etiquetas, se indican las etiquetas que estaban asociadas con un recurso en el momento en que se procesó el resultado. Puede incluir el atributo `Tags` solamente para los recursos que tienen una etiqueta asociada. Si un recurso no tiene etiqueta asociada, no incluya un atributo `Tags` en el hallazgo.

La inclusión de etiquetas de recursos en los resultados elimina la necesidad de crear canalizaciones de enriquecimiento de datos o enriquecer manualmente los metadatos de los resultados de seguridad. También puede usar etiquetas para buscar o filtrar los resultados e información y crear reglas de automatización.

Para obtener información sobre las restricciones que se aplican a las etiquetas, consulte Tag naming limits and requirements.

En este campo, solo puede incluir las etiquetas que existan en un AWS recurso. Para proporcionar datos que no estén definidos en el formato de búsqueda AWS de seguridad, usa el subcampo de `Other` detalles.

Ejemplo

```
"Tags": {
    "billingCode": "Lotus-1-2-3",
    "needsPatching": "true"
}
```

Tipo

Tipo de recurso del que se proporcionan detalles.

Siempre que sea posible, utilice uno de los tipos de recursos proporcionados, como `AwsEc2Instance` o `AwsS3Bucket`.

Si el tipo de recurso no coincide con ninguno de los tipos de recursos proporcionados, establezca el recurso `Type` en `Other` y utilice el subcampo de detalles `Other` para rellenar los detalles.

Los valores admitidos se muestran en Recursos.

Ejemplo

```
"Type": "AwsS3Bucket"
```

AwsAmazonMQ recursos en ASFF

Los siguientes son ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para los `AwsAmazonMQ` recursos.

AWS Security Hub CSPM normaliza los hallazgos de varias fuentes en el ASFF. Para obtener información general sobre el ASFF, consulte AWS Formato de búsqueda de seguridad (ASFF).

AwsAmazonMQBroker

`AwsAmazonMQBroker` proporciona información acerca de un agente de Amazon MQ, que es un entorno de agente de mensajes que se ejecuta en Amazon MQ.

En el ejemplo siguiente se muestra el ASFF para el objeto `AwsAmazonMQBroker`. Para ver las descripciones de los atributos `AwsAmazonMQBroker`, consulte AwsAmazonMQBroker en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsAmazonMQBroker": {
    "AutoMinorVersionUpgrade": true,
    "BrokerArn": "arn:aws:mq:us-east-1:123456789012:broker:TestBroker:b-
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "BrokerId": "b-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "BrokerName": "TestBroker",
    "Configuration": {
        "Id": "c-a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
        "Revision": 1
    },
```

```
    "DeploymentMode": "ACTIVE_STANDBY_MULTI_AZ",
    "EncryptionOptions": {
        "UseAwsOwnedKey": true
    },
    "EngineType": "ActiveMQ",
    "EngineVersion": "5.17.2",
    "HostInstanceType": "mq.t2.micro",
    "Logs": {
        "Audit": false,
        "AuditLogGroup": "/aws/amazonmq/broker/b-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111/
audit",
        "General": false,
        "GeneralLogGroup": "/aws/amazonmq/broker/b-a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111/general"
    },
    "MaintenanceWindowStartTime": {
        "DayOfWeek": "MONDAY",
        "TimeOfDay": "22:00",
        "TimeZone": "UTC"
    },
    "PubliclyAccessible": true,
    "SecurityGroups": [
        "sg-021345abcdef6789"
    ],
    "StorageType": "efs",
    "SubnetIds": [
        "subnet-1234567890abcdef0",
        "subnet-abcdef01234567890"
    ],
    "Users": [
        {
            "Username": "admin"
        }
    ]
}
```

AwsApiGateway recursos en ASFF

Los siguientes son ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para `AwsApiGateway` los recursos.

AWS Security Hub CSPM normaliza los hallazgos de varias fuentes en el ASFF. Para obtener información general sobre el ASFF, consulte AWS Formato de búsqueda de seguridad (ASFF).

AwsApiGatewayRestApi

El objeto `AwsApiGatewayRestApi` contiene información sobre una API de REST de la versión 1 de Amazon API Gateway.

A continuación, se muestra un ejemplo de resultado de `AwsApiGatewayRestApi` en Formato de resultados de seguridad de AWS (ASFF). Para ver las descripciones de los atributos `AwsApiGatewayRestApi`, consulte AwsApiGatewayRestApiDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
AwsApiGatewayRestApi: {
    "Id": "exampleapi",
    "Name": "Security Hub",
    "Description": "AWS Security Hub",
    "CreatedDate": "2018-11-18T10:20:05-08:00",
    "Version": "2018-10-26",
    "BinaryMediaTypes" : ["-'*~1*'"],
    "MinimumCompressionSize": 1024,
    "ApiKeySource": "AWS_ACCOUNT_ID",
    "EndpointConfiguration": {
        "Types": [
            "REGIONAL"
        ]
    }
}
```

AwsApiGatewayStage

El objeto `AwsApiGatewayStage` proporciona información sobre una etapa de Amazon API Gateway de la versión 1.

A continuación, se muestra un ejemplo de resultado de `AwsApiGatewayStage` en Formato de resultados de seguridad de AWS (ASFF). Para ver las descripciones de los atributos `AwsApiGatewayStage`, consulte AwsApiGatewayStageDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsApiGatewayStage": {
    "DeploymentId": "n7hlmf",
```

```
    "ClientCertificateId": "a1b2c3",
    "StageName": "Prod",
    "Description" : "Stage Description",
    "CacheClusterEnabled": false,
    "CacheClusterSize" : "1.6",
    "CacheClusterStatus": "NOT_AVAILABLE",
    "MethodSettings": [
        {
            "MetricsEnabled": true,
            "LoggingLevel": "INFO",
            "DataTraceEnabled": false,
            "ThrottlingBurstLimit": 100,
            "ThrottlingRateLimit": 5.0,
            "CachingEnabled": false,
            "CacheTtlInSeconds": 300,
            "CacheDataEncrypted": false,
            "RequireAuthorizationForCacheControl": true,
            "UnauthorizedCacheControlHeaderStrategy": "SUCCEED_WITH_RESPONSE_HEADER",
            "HttpMethod": "POST",
            "ResourcePath": "/echo"
        }
    ],
    "Variables": {"test": "value"},
    "DocumentationVersion": "2.0",
    "AccessLogSettings": {
        "Format": "{\"requestId\": \"$context.requestId\", \"extendedRequestId
\": \"$context.extendedRequestId\", \"ownerAccountId\": \"$context.accountId\",
 \"requestAccountId\": \"$context.identity.accountId\", \"callerPrincipal\":
 \"$context.identity.caller\", \"httpMethod\": \"$context.httpMethod\", \"resourcePath
\": \"$context.resourcePath\", \"status\": \"$context.status\", \"requestTime
\": \"$context.requestTime\", \"responseLatencyMs\": \"$context.responseLatency
\", \"errorMessage\": \"$context.error.message\", \"errorResponseType\":
 \"$context.error.responseType\", \"apiId\": \"$context.apiId\", \"awsEndpointRequestId
\": \"$context.awsEndpointRequestId\", \"domainName\": \"$context.domainName\", \"stage
\": \"$context.stage\", \"xrayTraceId\": \"$context.xrayTraceId\", \"sourceIp\":
 \"$context.identity.sourceIp\", \"user\": \"$context.identity.user\", \"userAgent
\": \"$context.identity.userAgent\", \"userArn\": \"$context.identity.userArn\",
 \"integrationLatency\": \"$context.integrationLatency\", \"integrationStatus
\": \"$context.integrationStatus\", \"authorizerIntegrationLatency\":
 \"$context.authorizer.integrationLatency\" }",
        "DestinationArn": "arn:aws:logs:us-west-2:111122223333:log-
group:SecurityHubAPIAccessLog/Prod"
    },
    "CanarySettings": {
```

```
        "PercentTraffic": 0.0,
        "DeploymentId": "ul73s8",
        "StageVariableOverrides" : [
            "String" : "String"
        ],
        "UseStageCache": false
    },
    "TracingEnabled": false,
    "CreatedDate": "2018-07-11T10:55:18-07:00",
    "LastUpdatedDate": "2020-08-26T11:51:04-07:00",
    "WebAclArn" : "arn:aws:waf-regional:us-west-2:111122223333:webacl/
cb606bd8-5b0b-4f0b-830a-dd304e48a822"
}
```

AwsApiGatewayV2Api

El objeto `AwsApiGatewayV2Api` contiene información acerca de una API de versión 2 en Amazon API Gateway.

A continuación, se muestra un ejemplo de resultado de `AwsApiGatewayV2Api` en Formato de resultados de seguridad de AWS (ASFF). Para ver las descripciones de los atributos `AwsApiGatewayV2Api`, consulte AwsApiGatewayV2ApiDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsApiGatewayV2Api": {
    "ApiEndpoint": "https://example.us-west-2.amazonaws.com",
    "ApiId": "a1b2c3d4",
    "ApiKeySelectionExpression": "$request.header.x-api-key",
    "CreatedDate": "2020-03-28T00:32:37Z",
   "Description": "ApiGatewayV2 Api",
   "Version": "string",
    "Name": "my-api",
    "ProtocolType": "HTTP",
    "RouteSelectionExpression": "$request.method $request.path",
   "CorsConfiguration": {
        "AllowOrigins": [ "*" ],
        "AllowCredentials": true,
        "ExposeHeaders": [ "string" ],
        "MaxAge": 3000,
        "AllowMethods": [
```

```
            "GET",
            "PUT",
            "POST",
            "DELETE",
            "HEAD"
        ],
        "AllowHeaders": [ "*" ]
    }
}
```

AwsApiGatewayV2Stage

`AwsApiGatewayV2Stage` contiene información sobre una etapa de la versión 2 de Amazon API Gateway.

A continuación, se muestra un ejemplo de resultado de `AwsApiGatewayV2Stage` en Formato de resultados de seguridad de AWS (ASFF). Para ver las descripciones de los atributos `AwsApiGatewayV2Stage`, consulte AwsApiGatewayV2StageDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsApiGatewayV2Stage": {
    "CreatedDate": "2020-04-08T00:36:05Z",
    "Description" : "ApiGatewayV2",
    "DefaultRouteSettings": {
        "DetailedMetricsEnabled": false,
        "LoggingLevel": "INFO",
        "DataTraceEnabled": true,
        "ThrottlingBurstLimit": 100,
        "ThrottlingRateLimit": 50
    },
    "DeploymentId": "x1zwyv",
    "LastUpdatedDate": "2020-04-08T00:36:13Z",
    "RouteSettings": {
        "DetailedMetricsEnabled": false,
        "LoggingLevel": "INFO",
        "DataTraceEnabled": true,
        "ThrottlingBurstLimit": 100,
        "ThrottlingRateLimit": 50
    },
    "StageName": "prod",
    "StageVariables": [
```

```
        "function": "my-prod-function"
    ],
    "AccessLogSettings": {
        "Format": "{\"requestId\": \"$context.requestId\", \"extendedRequestId
\": \"$context.extendedRequestId\", \"ownerAccountId\": \"$context.accountId\",
 \"requestAccountId\": \"$context.identity.accountId\", \"callerPrincipal\":
 \"$context.identity.caller\", \"httpMethod\": \"$context.httpMethod\", \"resourcePath
\": \"$context.resourcePath\", \"status\": \"$context.status\", \"requestTime
\": \"$context.requestTime\", \"responseLatencyMs\": \"$context.responseLatency
\", \"errorMessage\": \"$context.error.message\", \"errorResponseType\":
 \"$context.error.responseType\", \"apiId\": \"$context.apiId\", \"awsEndpointRequestId
\": \"$context.awsEndpointRequestId\", \"domainName\": \"$context.domainName\", \"stage
\": \"$context.stage\", \"xrayTraceId\": \"$context.xrayTraceId\", \"sourceIp\":
 \"$context.identity.sourceIp\", \"user\": \"$context.identity.user\", \"userAgent
\": \"$context.identity.userAgent\", \"userArn\": \"$context.identity.userArn\",
 \"integrationLatency\": \"$context.integrationLatency\", \"integrationStatus
\": \"$context.integrationStatus\", \"authorizerIntegrationLatency\":
 \"$context.authorizer.integrationLatency\" }",
        "DestinationArn": "arn:aws:logs:us-west-2:111122223333:log-
group:SecurityHubAPIAccessLog/Prod"
    },
    "AutoDeploy": false,
    "LastDeploymentStatusMessage": "Message",
    "ApiGatewayManaged": true,
}
```

AwsAppSync recursos en ASFF

Los siguientes son ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para `AwsAppSync` los recursos.

AWS Security Hub CSPM normaliza los hallazgos de varias fuentes en el ASFF. Para obtener información general sobre el ASFF, consulte AWS Formato de búsqueda de seguridad (ASFF).

AwsAppSyncGraphQLApi

`AwsAppSyncGraphQLApi`proporciona información sobre una API de AWS AppSync GraphQL, que es una construcción de nivel superior para tu aplicación.

En el ejemplo siguiente se muestra el ASFF para el objeto `AwsAppSyncGraphQLApi`. Para ver las descripciones de los atributos `AwsAppSyncGraphQLApi`, consulte AwsAppSyncGraphQLApi en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsAppSyncGraphQLApi": {
    "AdditionalAuthenticationProviders": [
    {
     "AuthenticationType": "AWS_LAMBDA",
     "LambdaAuthorizerConfig": {
      "AuthorizerResultTtlInSeconds": 300,
      "AuthorizerUri": "arn:aws:lambda:us-east-1:123456789012:function:mylambdafunc"
     }
    },
    {
     "AuthenticationType": "AWS_IAM"
    }
    ],
    "ApiId": "021345abcdef6789",
    "Arn": "arn:aws:appsync:eu-central-1:123456789012:apis/021345abcdef6789",
    "AuthenticationType": "API_KEY",
    "Id": "021345abcdef6789",
    "LogConfig": {
     "CloudWatchLogsRoleArn": "arn:aws:iam::123456789012:role/service-role/appsync-
graphqlapi-logs-eu-central-1",
     "ExcludeVerboseContent": true,
     "FieldLogLevel": "ALL"
    },
    "Name": "My AppSync App",
    "XrayEnabled": true,
}
```

AwsAthena recursos en ASFF

Los siguientes son ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para los `AwsAthena` recursos.

AWS Security Hub CSPM normaliza los hallazgos de varias fuentes en el ASFF. Para obtener información general sobre el ASFF, consulte AWS Formato de búsqueda de seguridad (ASFF).

AwsAthenaWorkGroup

`AwsAthenaWorkGroup` proporciona información sobre un grupo de trabajo de Amazon Athena. Un grupo de trabajo le ayuda a separar los usuarios, los equipos, las aplicaciones o las cargas de trabajo. También le ayuda a establecer límites en el procesamiento de datos y a realizar un seguimiento de los costos.

En el ejemplo siguiente se muestra el ASFF para el objeto `AwsAthenaWorkGroup`. Para ver las descripciones de los atributos `AwsAthenaWorkGroup`, consulte AwsAthenaWorkGroup en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsAthenaWorkGroup": {
    "Description": "My workgroup for prod workloads",
    "Name": "MyWorkgroup",
    "WorkgroupConfiguration" {
        "ResultConfiguration": {
            "EncryptionConfiguration": {
                "EncryptionOption": "SSE_KMS",
                "KmsKey": "arn:aws:kms:us-east-1:123456789012:key/a1b2c3d4-5678-90ab-
cdef-EXAMPLE11111"
            }
        }
    },
        "State": "ENABLED"
}
```

AwsAutoScaling recursos en ASFF

Los siguientes son ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para `AwsAutoScaling` los recursos.

AWS Security Hub CSPM normaliza los hallazgos de varias fuentes en el ASFF. Para obtener información general sobre el ASFF, consulte AWS Formato de búsqueda de seguridad (ASFF).

AwsAutoScalingAutoScalingGroup

El objeto `AwsAutoScalingAutoScalingGroup` proporciona detalles sobre un grupo de escalado automático.

A continuación, se muestra un ejemplo de resultado de `AwsAutoScalingAutoScalingGroup` en Formato de resultados de seguridad de AWS (ASFF). Para ver las descripciones de los atributos `AwsAutoScalingAutoScalingGroup`, consulte AwsAutoScalingAutoScalingGroupDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsAutoScalingAutoScalingGroup": {
        "CreatedTime": "2017-10-17T14:47:11Z",
        "HealthCheckGracePeriod": 300,
        "HealthCheckType": "EC2",
        "LaunchConfigurationName": "mylaunchconf",
        "LoadBalancerNames": [],
        "LaunchTemplate": {
            "LaunchTemplateId": "string",
            "LaunchTemplateName": "string",
            "Version": "string"
        },
        "MixedInstancesPolicy": {
            "InstancesDistribution": {
                "OnDemandAllocationStrategy": "prioritized",
                "OnDemandBaseCapacity": number,
                "OnDemandPercentageAboveBaseCapacity": number,
                "SpotAllocationStrategy": "lowest-price",
                "SpotInstancePools": number,
                "SpotMaxPrice": "string"
            },
            "LaunchTemplate": {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateId": "string",
                    "LaunchTemplateName": "string",
                    "Version": "string"
                 },
                "CapacityRebalance": true,
                "Overrides": [
                    {
                       "InstanceType": "string",
                       "WeightedCapacity": "string"
                    }
                ]
            }
        }
    }
}
```

AwsAutoScalingLaunchConfiguration

El objeto `AwsAutoScalingLaunchConfiguration` proporciona detalles sobre la configuración de una característica de .

El siguiente es un ejemplo de `AwsAutoScalingLaunchConfiguration` búsqueda en el formato de búsqueda AWS de seguridad (ASFF).

Para ver las descripciones de los atributos `AwsAutoScalingLaunchConfiguration`, consulte AwsAutoScalingLaunchConfigurationDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
AwsAutoScalingLaunchConfiguration: {
    "LaunchConfigurationName": "newtest",
    "ImageId": "ami-058a3739b02263842",
    "KeyName": "55hundredinstance",
    "SecurityGroups": [ "sg-01fce87ad6e019725" ],
    "ClassicLinkVpcSecurityGroups": [],
    "UserData": "...Base64-Encoded user data..."
    "InstanceType": "a1.metal",
    "KernelId": "",
    "RamdiskId": "ari-a51cf9cc",
    "BlockDeviceMappings": [
        {
            "DeviceName": "/dev/sdh",
            "Ebs": {
                "VolumeSize": 30,
                "VolumeType": "gp2",
                "DeleteOnTermination": false,
                "Encrypted": true,
                "SnapshotId": "snap-ffaa1e69",
                "VirtualName": "ephemeral1"
            }
        },
        {
            "DeviceName": "/dev/sdb",
            "NoDevice": true
        },
        {
            "DeviceName": "/dev/sda1",
            "Ebs": {
                "SnapshotId": "snap-02420cd3d2dea1bc0",
                "VolumeSize": 8,
                "VolumeType": "gp2",
                "DeleteOnTermination": true,
                "Encrypted": false
            }
```

```
        },
        {
            "DeviceName": "/dev/sdi",
            "Ebs": {
                "VolumeSize": 20,
                "VolumeType": "gp2",
                "DeleteOnTermination": false,
                "Encrypted": true
            }
        },
        {
            "DeviceName": "/dev/sdc",
            "NoDevice": true
        }
    ],
    "InstanceMonitoring": {
        "Enabled": false
    },
    "CreatedTime": 1620842933453,
    "EbsOptimized": false,
    "AssociatePublicIpAddress": true,
    "SpotPrice": "0.045"
}
```

AwsBackup recursos en ASFF

Los siguientes son ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para `AwsBackup` los recursos.

AWS Security Hub CSPM normaliza los hallazgos de varias fuentes en el ASFF. Para obtener información general sobre el ASFF, consulte AWS Formato de búsqueda de seguridad (ASFF).

AwsBackupBackupPlan

El objeto `AwsBackupBackupPlan` proporciona información sobre un proyecto de plan de copia de seguridad de AWS Backup . Un plan AWS Backup de respaldo es una expresión de política que define cuándo y cómo desea realizar una copia de seguridad de sus AWS recursos.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsBackupBackupPlan` objeto. Para ver las descripciones de los atributos `AwsBackupBackupPlan`, consulte AwsBackupBackupPlan en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsBackupBackupPlan": {
    "BackupPlan": {
     "AdvancedBackupSettings": [{
      "BackupOptions": {
       "WindowsVSS":"enabled"
      },
      "ResourceType":"EC2"
     }],
     "BackupPlanName": "test",
     "BackupPlanRule": [{
      "CompletionWindowMinutes": 10080,
      "CopyActions": [{
       "DestinationBackupVaultArn": "arn:aws:backup:us-east-1:858726136373:backup-
vault:aws/efs/automatic-backup-vault",
       "Lifecycle": {
        "DeleteAfterDays": 365,
        "MoveToColdStorageAfterDays": 30
       }
      }],
      "Lifecycle": {
       "DeleteAfterDays": 35
      },
      "RuleName": "DailyBackups",
      "ScheduleExpression": "cron(0 5 ? * * *)",
      "StartWindowMinutes": 480,
      "TargetBackupVault": "Default"
      },
      {
      "CompletionWindowMinutes": 10080,
      "CopyActions": [{
       "DestinationBackupVaultArn": "arn:aws:backup:us-east-1:858726136373:backup-
vault:aws/efs/automatic-backup-vault",
       "Lifecycle": {
        "DeleteAfterDays": 365,
        "MoveToColdStorageAfterDays": 30
       }
      }],
      "Lifecycle": {
       "DeleteAfterDays": 35
      },
      "RuleName": "Monthly",
      "ScheduleExpression": "cron(0 5 1 * ? *)",
```

```
      "StartWindowMinutes": 480,
      "TargetBackupVault": "Default"
     }]
    },
    "BackupPlanArn": "arn:aws:backup:us-east-1:858726136373:backup-
plan:b6d6b896-590d-4ee1-bf29-c5ccae63f4e7",
    "BackupPlanId": "b6d6b896-590d-4ee1-bf29-c5ccae63f4e7",
    "VersionId": "ZDVjNDIzMjItYTZiNS00NzczLTg4YzctNmExMWM2NjZhY2E1"
}
```

AwsBackupBackupVault

El objeto `AwsBackupBackupVault` proporciona información sobre un almacén de copias de seguridad de AWS Backup . Un almacén AWS Backup de copias de seguridad es un contenedor que almacena y organiza las copias de seguridad.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsBackupBackupVault` objeto. Para ver las descripciones de los atributos `AwsBackupBackupVault`, consulte AwsBackupBackupVault en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsBackupBackupVault": {
    "AccessPolicy": {
     "Statement": [{
      "Action": [
       "backup:DeleteBackupVault",
       "backup:DeleteBackupVaultAccessPolicy",
       "backup:DeleteRecoveryPoint",
       "backup:StartCopyJob",
       "backup:StartRestoreJob",
       "backup:UpdateRecoveryPointLifecycle"
      ],
      "Effect": "Deny",
      "Principal": {
       "AWS": "*"
      },
      "Resource": "*"
     }],
     "Version": "2012-10-17"
    },
```

```
    "BackupVaultArn": "arn:aws:backup:us-east-1:123456789012:backup-vault:aws/efs/
automatic-backup-vault",
    "BackupVaultName": "aws/efs/automatic-backup-vault",
    "EncrytionKeyArn": "arn:aws:kms:us-east-1:444455556666:key/72ba68d4-5e43-40b0-
ba38-838bf8d06ca0",
    "Notifications": {
     "BackupVaultEvents": ["BACKUP_JOB_STARTED", "BACKUP_JOB_COMPLETED",
 "COPY_JOB_STARTED"],
     "SNSTopicArn": "arn:aws:sns:us-west-2:111122223333:MyVaultTopic"
    }
}
```

AwsBackupRecoveryPoint

El objeto `AwsBackupRecoveryPoint` proporciona información sobre una copia de seguridad de AWS Backup , también denominada punto de recuperación. Un punto AWS Backup de recuperación representa el contenido de un recurso en un momento específico.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsBackupRecoveryPoint` objeto. Para ver las descripciones de los atributos `AwsBackupBackupVault`, consulte AwsBackupRecoveryPoint en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsBackupRecoveryPoint": {
    "BackupSizeInBytes": 0,
    "BackupVaultName": "aws/efs/automatic-backup-vault",
    "BackupVaultArn": "arn:aws:backup:us-east-1:111122223333:backup-vault:aws/efs/
automatic-backup-vault",
    "CalculatedLifecycle": {
     "DeleteAt": "2021-08-30T06:51:58.271Z",
     "MoveToColdStorageAt": "2020-08-10T06:51:58.271Z"
    },
    "CompletionDate": "2021-07-26T07:21:40.361Z",
    "CreatedBy": {
     "BackupPlanArn": "arn:aws:backup:us-east-1:111122223333:backup-plan:aws/
efs/73d922fb-9312-3a70-99c3-e69367f9fdad",
     "BackupPlanId": "aws/efs/73d922fb-9312-3a70-99c3-e69367f9fdad",
     "BackupPlanVersion": "ZGM4YzY5YjktMWYxNC00ZTBmLWE5MjYtZmU5OWNiZmM5ZjIz",
     "BackupRuleId": "2a600c2-42ad-4196-808e-084923ebfd25"
    },
    "CreationDate": "2021-07-26T06:51:58.271Z",
```

```
    "EncryptionKeyArn": "arn:aws:kms:us-east-1:111122223333:key/72ba68d4-5e43-40b0-
ba38-838bf8d06ca0",
    "IamRoleArn": "arn:aws:iam::111122223333:role/aws-service-role/
backup.amazonaws.com/AWSServiceRoleForBackup",
    "IsEncrypted": true,
    "LastRestoreTime": "2021-07-26T06:51:58.271Z",
    "Lifecycle": {
     "DeleteAfterDays": 35,
     "MoveToColdStorageAfterDays": 15
    },
    "RecoveryPointArn": "arn:aws:backup:us-east-1:111122223333:recovery-point:151a59e4-
f1d5-4587-a7fd-0774c6e91268",
    "ResourceArn": "arn:aws:elasticfilesystem:us-east-1:858726136373:file-system/
fs-15bd31a1",
    "ResourceType": "EFS",
    "SourceBackupVaultArn": "arn:aws:backup:us-east-1:111122223333:backup-vault:aws/
efs/automatic-backup-vault",
    "Status": "COMPLETED",
    "StatusMessage": "Failure message",
    "StorageClass": "WARM"
}
```

AwsCertificateManager recursos en ASFF

Los siguientes son ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para los `AwsCertificateManager` recursos.

AWS Security Hub CSPM normaliza los hallazgos de varias fuentes en el ASFF. Para obtener información general sobre el ASFF, consulte AWS Formato de búsqueda de seguridad (ASFF).

AwsCertificateManagerCertificate

El objeto `AwsCertificateManagerCertificate` proporciona detalles sobre un certificado de AWS Gestor de certificados (ACM).

El siguiente es un ejemplo de `AwsCertificateManagerCertificate` búsqueda en el formato de búsqueda AWS de seguridad (ASFF). Para ver las descripciones de los atributos `AwsCertificateManagerCertificate`, consulte AwsCertificateManagerCertificateDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsCertificateManagerCertificate": {
```

```
    "CertificateAuthorityArn": "arn:aws:acm:us-west-2:444455556666:certificate-
authority/example",
    "CreatedAt": "2019-05-24T18:12:02.000Z",
    "DomainName": "example.amazondomains.com",
    "DomainValidationOptions": [
        {
            "DomainName": "example.amazondomains.com",
            "ResourceRecord": {
                "Name": "_1bacb61828d3a1020c40a560ceed08f7.example.amazondomains.com",
                "Type": "CNAME",
                "Value": "_example.acm-validations.aws."
             },
             "ValidationDomain": "example.amazondomains.com",
             "ValidationEmails": [sample_email@sample.com],
             "ValidationMethod": "DNS",
             "ValidationStatus": "SUCCESS"
        }
    ],
    "ExtendedKeyUsages": [
        {
            "Name": "TLS_WEB_SERVER_AUTHENTICATION",
            "OId": "1.3.6.1.5.5.7.3.1"
        },
        {
            "Name": "TLS_WEB_CLIENT_AUTHENTICATION",
            "OId": "1.3.6.1.5.5.7.3.2"
        }
    ],
    "FailureReason": "",
    "ImportedAt": "2018-08-17T00:13:00.000Z",
    "InUseBy": ["arn:aws:amazondomains:us-west-2:444455556666:loadbalancer/example"],
    "IssuedAt": "2020-04-26T00:41:17.000Z",
    "Issuer": "Amazon",
    "KeyAlgorithm": "RSA-1024",
    "KeyUsages": [
        {
            "Name": "DIGITAL_SIGNATURE",
        },
        {
            "Name": "KEY_ENCIPHERMENT",
        }
    ],
    "NotAfter": "2021-05-26T12:00:00.000Z",
    "NotBefore": "2020-04-26T00:00:00.000Z",
```

```
    "Options": {
        "CertificateTransparencyLoggingPreference": "ENABLED",
    }
    "RenewalEligibility": "ELIGIBLE",
    "RenewalSummary": {
        "DomainValidationOptions": [
            {
                "DomainName": "example.amazondomains.com",
                "ResourceRecord": {
                    "Name":
 "_1bacb61828d3a1020c40a560ceed08f7.example.amazondomains.com",
                    "Type": "CNAME",
                    "Value": "_example.acm-validations.aws.com",
                },
                "ValidationDomain": "example.amazondomains.com",
                "ValidationEmails": ["sample_email@sample.com"],
                "ValidationMethod": "DNS",
                "ValidationStatus": "SUCCESS"
            }
        ],
        "RenewalStatus": "SUCCESS",
        "RenewalStatusReason": "",
        "UpdatedAt": "2020-04-26T00:41:35.000Z",
    },
    "Serial": "02:ac:86:b6:07:2f:0a:61:0e:3a:ac:fd:d9:ab:17:1a",
    "SignatureAlgorithm": "SHA256WITHRSA",
    "Status": "ISSUED",
    "Subject": "CN=example.amazondomains.com",
    "SubjectAlternativeNames": ["example.amazondomains.com"],
    "Type": "AMAZON_ISSUED"
}
```

AwsCloudFormation recursos en ASFF

Los siguientes son ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para `AwsCloudFormation` los recursos.

AWS Security Hub CSPM normaliza los hallazgos de varias fuentes en el ASFF. Para obtener información general sobre el ASFF, consulte AWS Formato de búsqueda de seguridad (ASFF).

AwsCloudFormationStack

El objeto `AwsCloudFormationStack` proporciona detalles acerca de una pila de AWS CloudFormation que está anidada como un recurso en una plantilla de nivel superior.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsCloudFormationStack` objeto. Para ver las descripciones de los atributos `AwsCloudFormationStack`, consulte AwsCloudFormationStackDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsCloudFormationStack": {
 "Capabilities": [
  "CAPABILITY_IAM",
  "CAPABILITY_NAMED_IAM"
 ],
 "CreationTime": "2022-02-18T15:31:53.161Z",
 "Description": "AWS CloudFormation Sample",
 "DisableRollback": true,
 "DriftInformation": {
  "StackDriftStatus": "DRIFTED"
 },
 "EnableTerminationProtection": false,
 "LastUpdatedTime": "2022-02-18T15:31:53.161Z",
 "NotificationArns": [
  "arn:aws:sns:us-east-1:978084797471:sample-sns-cfn"
 ],
 "Outputs": [{
  "Description": "URL for newly created LAMP stack",
  "OutputKey": "WebsiteUrl",
  "OutputValue": "http://ec2-44-193-18-241.compute-1.amazonaws.com"
 }],
 "RoleArn": "arn:aws:iam::012345678910:role/exampleRole",
 "StackId": "arn:aws:cloudformation:us-east-1:978084797471:stack/sample-stack/
e5d9f7e0-90cf-11ec-88c6-12ac1f91724b",
 "StackName": "sample-stack",
 "StackStatus": "CREATE_COMPLETE",
 "StackStatusReason": "Success",
 "TimeoutInMinutes": 1
}
```

AwsCloudFront recursos en ASFF

Los siguientes son ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para `AwsCloudFront` los recursos.

AWS Security Hub CSPM normaliza los hallazgos de varias fuentes en el ASFF. Para obtener información general sobre el ASFF, consulte AWS Formato de búsqueda de seguridad (ASFF).

AwsCloudFrontDistribution

El `AwsCloudFrontDistribution` objeto proporciona detalles sobre la configuración de una CloudFront distribución de Amazon.

A continuación, se muestra un ejemplo de resultado de `AwsCloudFrontDistribution` en Formato de resultados de seguridad de AWS (ASFF). Para ver las descripciones de los atributos `AwsCloudFrontDistribution`, consulte AwsCloudFrontDistributionDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsCloudFrontDistribution": {
    "CacheBehaviors": {
        "Items": [
            {
               "ViewerProtocolPolicy": "https-only"
            }
         ]
    },
    "DefaultCacheBehavior": {
         "ViewerProtocolPolicy": "https-only"
    },
    "DefaultRootObject": "index.html",
    "DomainName": "d2wkuj2w9l34gt.cloudfront.net",
    "Etag": "E37HOT42DHPVYH",
    "LastModifiedTime": "2015-08-31T21:11:29.093Z",
    "Logging": {
         "Bucket": "myawslogbucket.s3.amazonaws.com",
         "Enabled": false,
         "IncludeCookies": false,
         "Prefix": "myawslog/"
     },
     "OriginGroups": {
          "Items": [
```

```
              {
                 "FailoverCriteria": {
                     "StatusCodes": {
                          "Items": [
                              200,
                              301,
                              404
                          ]
                          "Quantity": 3
                      }
                 }
              }
           ]
     },
     "Origins": {
           "Items": [
               {
                  "CustomOriginConfig": {
                      "HttpPort": 80,
                      "HttpsPort": 443,
                      "OriginKeepaliveTimeout": 60,
                      "OriginProtocolPolicy": "match-viewer",
                      "OriginReadTimeout": 30,
                      "OriginSslProtocols": {
                        "Items": ["SSLv3", "TLSv1"],
                        "Quantity": 2
                      }
                  }
               },
           ]
     },
                  "DomainName": "amzn-s3-demo-bucket.s3.amazonaws.com",
                  "Id": "my-origin",
                  "OriginPath": "/production",
                  "S3OriginConfig": {
                      "OriginAccessIdentity": "origin-access-identity/cloudfront/
E2YFS67H6VB6E4"
                  }
           ]
     },
     "Status": "Deployed",
     "ViewerCertificate": {
            "AcmCertificateArn": "arn:aws:acm::123456789012:AcmCertificateArn",
            "Certificate": "ASCAJRRE5XYF52TKRY5M4",
```

```
            "CertificateSource": "iam",
            "CloudFrontDefaultCertificate": true,
            "IamCertificateId": "ASCAJRRE5XYF52TKRY5M4",
            "MinimumProtocolVersion": "TLSv1.2_2021",
            "SslSupportMethod": "sni-only"
      },
      "WebAclId": "waf-1234567890"
}
```

AwsCloudTrail recursos en ASFF

Los siguientes son ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para `AwsCloudTrail` los recursos.

AWS Security Hub CSPM normaliza los hallazgos de varias fuentes en el ASFF. Para obtener información general sobre el ASFF, consulte AWS Formato de búsqueda de seguridad (ASFF).

AwsCloudTrailTrail

El objeto `AwsCloudTrailTrail` proporciona detalles sobre un seguimiento de AWS CloudTrail .

A continuación, se muestra un ejemplo de resultado de `AwsCloudTrailTrail` en Formato de resultados de seguridad de AWS (ASFF). Para ver las descripciones de los atributos `AwsCloudTrailTrail`, consulte AwsCloudTrailTrailDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsCloudTrailTrail": {
    "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-west-2:123456789012:log-
group:CloudTrail/regression:*",
    "CloudWatchLogsRoleArn": "arn:aws:iam::866482105055:role/
CloudTrail_CloudWatchLogs",
    "HasCustomEventSelectors": true,
    "HomeRegion": "us-west-2",
    "IncludeGlobalServiceEvents": true,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": false,
    "KmsKeyId": "kmsKeyId",
    "LogFileValidationEnabled": true,
    "Name": "regression-trail",
    "S3BucketName": "cloudtrail-bucket",
    "S3KeyPrefix": "s3KeyPrefix",
```

```
    "SnsTopicArn": "arn:aws:sns:us-east-2:123456789012:MyTopic",
    "SnsTopicName": "snsTopicName",
    "TrailArn": "arn:aws:cloudtrail:us-west-2:123456789012:trail"
}
```

AwsCloudWatch recursos en ASFF

Los siguientes son ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para `AwsCloudWatch` los recursos.

AWS Security Hub CSPM normaliza los hallazgos de varias fuentes en el ASFF. Para obtener información general sobre el ASFF, consulte AWS Formato de búsqueda de seguridad (ASFF).

AwsCloudWatchAlarm

El `AwsCloudWatchAlarm` objeto proporciona detalles sobre CloudWatch las alarmas de Amazon que vigilan una métrica o realizan una acción cuando una alarma cambia de estado.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsCloudWatchAlarm` objeto. Para ver las descripciones de los atributos `AwsCloudWatchAlarm`, consulte AwsCloudWatchAlarmDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsCloudWatchAlarm": {
 "ActionsEnabled": true,
 "AlarmActions": [
  "arn:aws:automate:region:ec2:stop",
  "arn:aws:automate:region:ec2:terminate"
 ],
 "AlarmArn": "arn:aws:cloudwatch:us-west-2:012345678910:alarm:sampleAlarm",
 "AlarmConfigurationUpdatedTimestamp": "2022-02-18T15:31:53.161Z",
 "AlarmDescription": "Alarm Example",
 "AlarmName": "Example",
 "ComparisonOperator": "GreaterThanOrEqualToThreshold",
 "DatapointsToAlarm": 1,
 "Dimensions": [{
  "Name": "InstanceId",
  "Value": "i-1234567890abcdef0"
 }],
 "EvaluateLowSampleCountPercentile": "evaluate",
 "EvaluationPeriods": 1,
 "ExtendedStatistic": "p99.9",
```

```
 "InsufficientDataActions": [
  "arn:aws:automate:region:ec2:stop"
 ],
 "MetricName": "Sample Metric",
 "Namespace": "YourNamespace",
 "OkActions": [
  "arn:aws:swf:region:account-id:action/actions/AWS_EC2.InstanceId.Stop/1.0"
 ],
 "Period": 1,
 "Statistic": "SampleCount",
 "Threshold": 12.3,
 "ThresholdMetricId": "t1",
 "TreatMissingData": "notBreaching",
 "Unit": "Kilobytes/Second"
}
```

AwsCodeBuild recursos en ASFF

Los siguientes son ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para `AwsCodeBuild` los recursos.

AWS Security Hub CSPM normaliza los hallazgos de varias fuentes en el ASFF. Para obtener información general sobre el ASFF, consulte AWS Formato de búsqueda de seguridad (ASFF).

AwsCodeBuildProject

El objeto `AwsCodeBuildProject` proporciona información sobre un proyecto de AWS CodeBuild .

A continuación, se muestra un ejemplo de resultado de `AwsCodeBuildProject` en Formato de resultados de seguridad de AWS (ASFF). Para ver las descripciones de los atributos `AwsCodeBuildProject`, consulte AwsCodeBuildProjectDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsCodeBuildProject": {
   "Artifacts": [
      {
          "ArtifactIdentifier": "string",
          "EncryptionDisabled": boolean,
          "Location": "string",
          "Name": "string",
          "NamespaceType": "string",
```

```
            "OverrideArtifactName": boolean,
            "Packaging": "string",
            "Path": "string",
            "Type": "string"
        }
    ],
    "SecondaryArtifacts": [
       {
            "ArtifactIdentifier": "string",
            "EncryptionDisabled": boolean,
            "Location": "string",
            "Name": "string",
            "NamespaceType": "string",
            "OverrideArtifactName": boolean,
            "Packaging": "string",
            "Path": "string",
            "Type": "string"
        }
    ],
    "EncryptionKey": "string",
    "Certificate": "string",
    "Environment": {
       "Certificate": "string",
       "EnvironmentVariables": [
            {
                 "Name": "string",
                 "Type": "string",
                 "Value": "string"
            }
       ],
    "ImagePullCredentialsType": "string",
    "PrivilegedMode": boolean,
    "RegistryCredential": {
        "Credential": "string",
        "CredentialProvider": "string"
    },
    "Type": "string"
    },
    "LogsConfig": {
         "CloudWatchLogs": {
              "GroupName": "string",
              "Status": "string",
              "StreamName": "string"
         },
```

```
        "S3Logs": {
             "EncryptionDisabled": boolean,
             "Location": "string",
             "Status": "string"
        }
    },
    "Name": "string",
    "ServiceRole": "string",
    "Source": {
        "Type": "string",
        "Location": "string",
        "GitCloneDepth": integer
    },
    "VpcConfig": {
        "VpcId": "string",
        "Subnets": ["string"],
        "SecurityGroupIds": ["string"]
    }
}
```

AwsDms recursos en ASFF

Los siguientes son ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para `AwsDms` los recursos.

AWS Security Hub CSPM normaliza los hallazgos de varias fuentes en el ASFF. Para obtener información general sobre el ASFF, consulte AWS Formato de búsqueda de seguridad (ASFF).

AwsDmsEndpoint

El `AwsDmsEndpoint` objeto proporciona información sobre un punto final AWS Database Migration Service (AWS DMS). Un punto de conexión proporciona información de conexión, tipo de almacén de datos y ubicación acerca de su almacén de datos.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsDmsEndpoint` objeto. Para ver las descripciones de los atributos `AwsDmsEndpoint`, consulte AwsDmsEndpointDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsDmsEndpoint": {
    "CertificateArn": "arn:aws:dms:us-
east-1:123456789012:cert:EXAMPLEIGDURVZGVJQZDPWJ5A7F2YDJVSMTBWFI",
```

```
    "DatabaseName": "Test",
    "EndpointArn": "arn:aws:dms:us-
east-1:123456789012:endpoint:EXAMPLEQB3CZY33F7XV253NAJVBNPK6MJQVFVQA",
    "EndpointIdentifier": "target-db",
    "EndpointType": "TARGET",
    "EngineName": "mariadb",
    "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",
    "Port": 3306,
    "ServerName": "target-db.exampletafyu.us-east-1.rds.amazonaws.com",
    "SslMode": "verify-ca",
    "Username": "admin"
}
```

AwsDmsReplicationInstance

El `AwsDmsReplicationInstance` objeto proporciona información sobre una instancia de replicación AWS Database Migration Service (AWS DMS). DMS utiliza una instancia de replicación para conectarse con su almacén de datos de origen, leer los datos de origen y formatear los datos para que el almacén de datos de destino pueda consumirlos.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsDmsReplicationInstance` objeto. Para ver las descripciones de los atributos `AwsDmsReplicationInstance`, consulte AwsDmsReplicationInstanceDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsDmsReplicationInstance": {
    "AllocatedStorage": 50,
    "AutoMinorVersionUpgrade": true,
    "AvailabilityZone": "us-east-1b",
    "EngineVersion": "3.5.1",
    "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",
    "MultiAZ": false,
    "PreferredMaintenanceWindow": "wed:08:08-wed:08:38",
    "PubliclyAccessible": true,
    "ReplicationInstanceClass": "dms.c5.xlarge",
    "ReplicationInstanceIdentifier": "second-replication-instance",
    "ReplicationSubnetGroup": {
        "ReplicationSubnetGroupIdentifier": "default-vpc-2344f44f"
    },
```

```
    "VpcSecurityGroups": [
        {
            "VpcSecurityGroupId": "sg-003a34e205138138b"
        }
    ]
}
```

AwsDmsReplicationTask

El `AwsDmsReplicationTask` objeto proporciona información sobre una tarea de replicación AWS Database Migration Service (AWS DMS). Una tarea de replicación mueve un conjunto de datos desde el punto de conexión de origen al punto de conexión de destino.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsDmsReplicationInstance` objeto. Para ver las descripciones de los atributos `AwsDmsReplicationInstance`, consulte AwsDmsReplicationInstance en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsDmsReplicationTask": {
    "CdcStartPosition": "2023-08-28T14:26:22",
    "Id": "arn:aws:dms:us-
east-1:123456789012:task:YDYUOHZIXWKQSUCBMUCQCNY44SJW74VJNB5DFWQ",
    "MigrationType": "cdc",
    "ReplicationInstanceArn": "arn:aws:dms:us-
east-1:123456789012:rep:T7V6RFDP23PYQWUL26N3PF5REKML4YOUGIMYJUI",
    "ReplicationTaskIdentifier": "test-task",
    "ReplicationTaskSettings": "{\"Logging\":{\"EnableLogging\":false,
\"EnableLogContext\":false,\"LogComponents\":[{\"Severity\":\"LOGGER_SEVERITY_DEFAULT
\",\"Id\":\"TRANSFORMATION\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",
\"Id\":\"SOURCE_UNLOAD\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":
\"IO\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"TARGET_LOAD\"},
{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"PERFORMANCE\"},{\"Severity
\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"SOURCE_CAPTURE\"},{\"Severity\":
\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"SORTER\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT
\",\"Id\":\"REST_SERVER\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id
\":\"VALIDATOR_EXT\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":
\"TARGET_APPLY\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"TASK_MANAGER
\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"TABLES_MANAGER\"},
{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"METADATA_MANAGER\"},
{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"FILE_FACTORY\"},{\"Severity\":
\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"COMMON\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT
```

\",\"Id\":\"ADDONS\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"DATA_STRUCTURE
\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"COMMUNICATION\"},{\"Severity
\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"FILE_TRANSFER\"}],\"CloudWatchLogGroup
\":null,\"CloudWatchLogStream\":null},\"StreamBufferSettings\":{\"StreamBufferCount
\":3,\"CtrlStreamBufferSizeInMB\":5,\"StreamBufferSizeInMB\":8},\"ErrorBehavior
\":{\"FailOnNoTablesCaptured\":true,\"ApplyErrorUpdatePolicy\":\"LOG_ERROR\",
\"FailOnTransactionConsistencyBreached\":false,\"RecoverableErrorThrottlingMax\":1800,
\"DataErrorEscalationPolicy\":\"SUSPEND_TABLE\",\"ApplyErrorEscalationCount\":0,
\"RecoverableErrorStopRetryAfterThrottlingMax\":true,\"RecoverableErrorThrottling
\":true,\"ApplyErrorFailOnTruncationDdl\":false,\"DataTruncationErrorPolicy\":
\"LOG_ERROR\",\"ApplyErrorInsertPolicy\":\"LOG_ERROR\",\"EventErrorPolicy\":
\"IGNORE\",\"ApplyErrorEscalationPolicy\":\"LOG_ERROR\",\"RecoverableErrorCount
\":-1,\"DataErrorEscalationCount\":0,\"TableErrorEscalationPolicy\":\"STOP_TASK
\",\"RecoverableErrorInterval\":5,\"ApplyErrorDeletePolicy\":\"IGNORE_RECORD\",
\"TableErrorEscalationCount\":0,\"FullLoadIgnoreConflicts\":true,\"DataErrorPolicy
\":\"LOG_ERROR\",\"TableErrorPolicy\":\"SUSPEND_TABLE\"},\"TTSettings
\":{\"TTS3Settings\":null,\"TTRecordSettings\":null,\"EnableTT\":false},
\"FullLoadSettings\":{\"CommitRate\":10000,\"StopTaskCachedChangesApplied
\":false,\"StopTaskCachedChangesNotApplied\":false,\"MaxFullLoadSubTasks
\":8,\"TransactionConsistencyTimeout\":600,\"CreatePkAfterFullLoad\":false,
\"TargetTablePrepMode\":\"DO_NOTHING\"},\"TargetMetadata\":{\"ParallelApplyBufferSize
\":0,\"ParallelApplyQueuesPerThread\":0,\"ParallelApplyThreads\":0,\"TargetSchema
\":\"\",\"InlineLobMaxSize\":0,\"ParallelLoadQueuesPerThread\":0,\"SupportLobs
\":true,\"LobChunkSize\":64,\"TaskRecoveryTableEnabled\":false,\"ParallelLoadThreads
\":0,\"LobMaxSize\":0,\"BatchApplyEnabled\":false,\"FullLobMode\":true,
\"LimitedSizeLobMode\":false,\"LoadMaxFileSize\":0,\"ParallelLoadBufferSize\":0},
\"BeforeImageSettings\":null,\"ControlTablesSettings\":{\"historyTimeslotInMinutes
\":5,\"HistoryTimeslotInMinutes\":5,\"StatusTableEnabled\":false,
\"SuspendedTablesTableEnabled\":false,\"HistoryTableEnabled\":false,\"ControlSchema
\":\"\",\"FullLoadExceptionTableEnabled\":false},\"LoopbackPreventionSettings
\":null,\"CharacterSetSettings\":null,\"FailTaskWhenCleanTaskResourceFailed
\":false,\"ChangeProcessingTuning\":{\"StatementCacheSize\":50,\"CommitTimeout
\":1,\"BatchApplyPreserveTransaction\":true,\"BatchApplyTimeoutMin\":1,
\"BatchSplitSize\":0,\"BatchApplyTimeoutMax\":30,\"MinTransactionSize\":1000,
\"MemoryKeepTime\":60,\"BatchApplyMemoryLimit\":500,\"MemoryLimitTotal\":1024},
\"ChangeProcessingDdlHandlingPolicy\":{\"HandleSourceTableDropped\":true,
\"HandleSourceTableTruncated\":true,\"HandleSourceTableAltered\":true},
\"PostProcessingRules\":null}",
    "SourceEndpointArn": "arn:aws:dms:us-
east-1:123456789012:endpoint:TZPWV2VCXEGHYOKVKRNHAKJ4Q3RUXACNGFGYWRI",
    "TableMappings": "{\"rules\":[{\"rule-type\":\"selection\",\"rule-id\":
\"969761702\",\"rule-name\":\"969761702\",\"object-locator\":{\"schema-name\":\"%table
\",\"table-name\":\"%example\"},\"rule-action\":\"exclude\",\"filters\":[]}]}",

```
    "TargetEndpointArn": "arn:aws:dms:us-
east-1:123456789012:endpoint:ABR8LBOQB3CZY33F7XV253NAJVBNPK6MJQVFVQA"
}
```

AwsDynamoDB recursos en ASFF

Los siguientes son ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para los recursos. `AwsDynamoDB`

AWS Security Hub CSPM normaliza los hallazgos de varias fuentes en el ASFF. Para obtener información general sobre el ASFF, consulte AWS Formato de búsqueda de seguridad (ASFF).

AwsDynamoDbTable

El objeto `AwsDynamoDbTable` proporciona detalles sobre una tabla de Amazon DynamoDB.

A continuación, se muestra un ejemplo de resultado de `AwsDynamoDbTable` en Formato de resultados de seguridad de AWS (ASFF). Para ver las descripciones de los atributos `AwsDynamoDbTable`, consulte AwsDynamoDbTableDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsDynamoDbTable": {
    "AttributeDefinitions": [
        {
            "AttributeName": "attribute1",
            "AttributeType": "value 1"
        },
        {
            "AttributeName": "attribute2",
            "AttributeType": "value 2"
        },
        {
            "AttributeName": "attribute3",
            "AttributeType": "value 3"
        }
    ],
    "BillingModeSummary": {
        "BillingMode": "PAY_PER_REQUEST",
        "LastUpdateToPayPerRequestDateTime": "2019-12-03T15:23:10.323Z"
    },
    "CreationDateTime": "2019-12-03T15:23:10.248Z",
```

```
    "DeletionProtectionEnabled": true,
    "GlobalSecondaryIndexes": [
        {
            "Backfilling": false,
            "IndexArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable/
index/exampleIndex",
            "IndexName": "standardsControlArnIndex",
            "IndexSizeBytes": 1862513,
            "IndexStatus": "ACTIVE",
            "ItemCount": 20,
            "KeySchema": [
                {
                    "AttributeName": "City",
                    "KeyType": "HASH"
                },
                {
                    "AttributeName": "Date",
                    "KeyType": "RANGE"
                }
            ],
            "Projection": {
                "NonKeyAttributes": ["predictorName"],
                "ProjectionType": "ALL"
            },
            "ProvisionedThroughput": {
                "LastIncreaseDateTime": "2019-03-14T13:21:00.399Z",
                "LastDecreaseDateTime": "2019-03-14T12:47:35.193Z",
                "NumberOfDecreasesToday": 0,
                "ReadCapacityUnits": 100,
                "WriteCapacityUnits": 50
            },
        }
   ],
   "GlobalTableVersion": "V1",
   "ItemCount": 2705,
   "KeySchema": [
        {
            "AttributeName": "zipcode",
            "KeyType": "HASH"
        }
    ],
    "LatestStreamArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable/
stream/2019-12-03T23:23:10.248",
    "LatestStreamLabel": "2019-12-03T23:23:10.248",
```

```
    "LocalSecondaryIndexes": [
        {
            "IndexArn": "arn:aws:dynamodb:us-east-1:111122223333:table/exampleGroup/
index/exampleId",
            "IndexName": "CITY_DATE_INDEX_NAME",
            "KeySchema": [
                {
                    "AttributeName": "zipcode",
                    "KeyType": "HASH"
                }
            ],
            "Projection": {
                "NonKeyAttributes": ["predictorName"],
                "ProjectionType": "ALL"
            },
        }
    ],
    "ProvisionedThroughput": {
        "LastIncreaseDateTime": "2019-03-14T13:21:00.399Z",
        "LastDecreaseDateTime": "2019-03-14T12:47:35.193Z",
        "NumberOfDecreasesToday": 0,
        "ReadCapacityUnits": 100,
        "WriteCapacityUnits": 50
    },
    "Replicas": [
        {
            "GlobalSecondaryIndexes":[
                {
                    "IndexName": "CITY_DATE_INDEX_NAME",
                    "ProvisionedThroughputOverride": {
                        "ReadCapacityUnits": 10
                    }
                }
            ],
            "KmsMasterKeyId" : "KmsKeyId"
            "ProvisionedThroughputOverride": {
                "ReadCapacityUnits": 10
            },
            "RegionName": "regionName",
            "ReplicaStatus": "CREATING",
            "ReplicaStatusDescription": "replicaStatusDescription"
        }
    ],
    "RestoreSummary" : {
```

```
        "SourceBackupArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable/
backup/backup1",
        "SourceTableArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable",
        "RestoreDateTime": "2020-06-22T17:40:12.322Z",
        "RestoreInProgress": true
    },
    "SseDescription": {
        "InaccessibleEncryptionDateTime": "2018-01-26T23:50:05.000Z",
        "Status": "ENABLED",
        "SseType": "KMS",
        "KmsMasterKeyArn": "arn:aws:kms:us-east-1:111122223333:key/key1"
    },
    "StreamSpecification" : {
        "StreamEnabled": true,
        "StreamViewType": "NEW_IMAGE"
    },
    "TableId": "example-table-id-1",
    "TableName": "example-table",
    "TableSizeBytes": 1862513,
    "TableStatus": "ACTIVE"
}
```

AwsEc2. recursos en ASFF

Los siguientes son ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para los `AwsEc2` recursos.

AWS Security Hub CSPM normaliza los hallazgos de varias fuentes en el ASFF. Para obtener información general sobre el ASFF, consulte AWS Formato de búsqueda de seguridad (ASFF).

AwsEc2ClientVpnEndpoint

El `AwsEc2ClientVpnEndpoint` objeto proporciona información sobre un AWS Client VPN punto final. El punto de conexión de Client VPN es el recurso que crea y configura para habilitar y administrar sesiones de Client VPN. Es el punto de terminación de todas las sesiones de Client VPN.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsEc2ClientVpnEndpoint` objeto. Para ver las descripciones de los atributos `AwsEc2ClientVpnEndpoint`, consulte AwsEc2ClientVpnEndpointDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsEc2ClientVpnEndpoint": {
    "AuthenticationOptions": [
        {
            "MutualAuthentication": {
                "ClientRootCertificateChainArn": "arn:aws:acm:us-
east-1:123456789012:certificate/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
            },
            "Type": "certificate-authentication"
        }
    ],
    "ClientCidrBlock": "10.0.0.0/22",
    "ClientConnectOptions": {
        "Enabled": false
    },
    "ClientLoginBannerOptions": {
        "Enabled": false
    },
    "ClientVpnEndpointId": "cvpn-endpoint-00c5d11fc4729f2a5",
    "ConnectionLogOptions": {
        "Enabled": false
    },
    "Description": "test",
    "DnsServer": ["10.0.0.0"],
    "ServerCertificateArn": "arn:aws:acm:us-east-1:123456789012:certificate/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "SecurityGroupIdSet": [
        "sg-0f7a177b82b443691"
    ],
    "SelfServicePortalUrl": "https://self-service.clientvpn.amazonaws.com/endpoints/
cvpn-endpoint-00c5d11fc4729f2a5",
    "SessionTimeoutHours": 24,
    "SplitTunnel": false,
    "TransportProtocol": "udp",
    "VpcId": "vpc-1a2b3c4d5e6f1a2b3",
    "VpnPort": 443
}
```

AwsEc2Eip

El objeto `AwsEc2Eip` proporciona información sobre una dirección IP elástica.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsEc2Eip` objeto. Para ver las descripciones de los atributos `AwsEc2Eip`, consulte AwsEc2EipDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsEc2Eip": {
    "InstanceId": "instance1",
    "PublicIp": "192.0.2.04",
    "AllocationId": "eipalloc-example-id-1",
    "AssociationId": "eipassoc-example-id-1",
    "Domain": "vpc",
    "PublicIpv4Pool": "anycompany",
    "NetworkBorderGroup": "eu-central-1",
    "NetworkInterfaceId": "eni-example-id-1",
    "NetworkInterfaceOwnerId": "777788889999",
    "PrivateIpAddress": "192.0.2.03"
}
```

AwsEc2Instance

El objeto `AwsEc2Instance` proporciona detalles sobre una instancia de base de datos de Amazon EC2.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsEc2Instance` objeto. Para ver las descripciones de los atributos `AwsEc2Instance`, consulte AwsEc2InstanceDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsEc2Instance": {
    "IamInstanceProfileArn": "arn:aws:iam::123456789012:instance-profile/AdminRole",
    "ImageId": "ami-1234",
    "IpV4Addresses": [ "1.1.1.1" ],
    "IpV6Addresses": [ "2001:db8:1234:1a2b::123" ],
    "KeyName": "my_keypair",
    "LaunchedAt": "2018-05-08T16:46:19.000Z",
    "MetadataOptions": {
     "HttpEndpoint": "enabled",
     "HttpProtocolIpv6": "enabled",
     "HttpPutResponseHopLimit": 1,
     "HttpTokens": "optional",
```

```
     "InstanceMetadataTags": "disabled",
    },
    "Monitoring": {
     "State": "disabled"
    },
    "NetworkInterfaces": [
      {
         "NetworkInterfaceId": "eni-e5aa89a3"
      }
    ],
    "SubnetId": "subnet-123",
    "Type": "i3.xlarge",
    "VpcId": "vpc-123"
}
```

AwsEc2LaunchTemplate

El objeto `AwsEc2LaunchTemplate` contiene detalles sobre una plantilla de lanzamiento de Amazon Elastic Compute Cloud que especifica la información de configuración de la instancia.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsEc2LaunchTemplate` objeto. Para ver las descripciones de los atributos `AwsEc2LaunchTemplate`, consulte AwsEc2LaunchTemplateDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsEc2LaunchTemplate": {
    "DefaultVersionNumber": "1",
    "ElasticGpuSpecifications": ["string"],
    "ElasticInferenceAccelerators": ["string"],
    "Id": "lt-0a16e9802800bdd85",
    "ImageId": "ami-0d5eff06f840b45e9",
    "LatestVersionNumber": "1",
    "LaunchTemplateData": {
     "BlockDeviceMappings": [{
      "DeviceName": "/dev/xvda",
      "Ebs": {
       "DeleteonTermination": true,
       "Encrypted": true,
       "SnapshotId": "snap-01047646ec075f543",
       "VolumeSize": 8,
```

```
        "VolumeType:" "gp2"
       }
      }],
      "MetadataOptions": {
       "HttpTokens": "enabled",
       "HttpPutResponseHopLimit" : 1
      },
      "Monitoring": {
       "Enabled": true,
      "NetworkInterfaces": [{
       "AssociatePublicIpAddress" : true,
      }],
     "LaunchTemplateName": "string",
     "LicenseSpecifications": ["string"],
     "SecurityGroupIds": ["sg-01fce87ad6e019725"],
     "SecurityGroups": ["string"],
     "TagSpecifications": ["string"]
}
```

AwsEc2NetworkAcl

El objeto `AwsEc2NetworkAcl` contiene detalles sobre una lista de control de acceso (ACL) a la red de Amazon EC2.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsEc2NetworkAcl` objeto. Para ver las descripciones de los atributos `AwsEc2NetworkAcl`, consulte AwsEc2NetworkAclDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsEc2NetworkAcl": {
    "IsDefault": false,
    "NetworkAclId": "acl-1234567890abcdef0",
    "OwnerId": "123456789012",
    "VpcId": "vpc-1234abcd",
    "Associations": [{
        "NetworkAclAssociationId": "aclassoc-abcd1234",
        "NetworkAclId": "acl-021345abcdef6789",
        "SubnetId": "subnet-abcd1234"
   }],
   "Entries": [{
        "CidrBlock": "10.24.34.0/23",
        "Egress": true,
```

```
        "IcmpTypeCode": {
            "Code": 10,
            "Type": 30
        },
        "Ipv6CidrBlock": "2001:DB8::/32",
        "PortRange": {
            "From": 20,
            "To": 40
        },
        "Protocol": "tcp",
        "RuleAction": "allow",
        "RuleNumber": 100
    }]
}
```

AwsEc2NetworkInterface

El objeto `AwsEc2NetworkInterface` proporciona información acerca de una interfaz de red de Amazon EC2.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsEc2NetworkInterface` objeto. Para ver las descripciones de los atributos `AwsEc2NetworkInterface`, consulte AwsEc2NetworkInterfaceDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsEc2NetworkInterface": {
    "Attachment": {
        "AttachTime": "2019-01-01T03:03:21Z",
        "AttachmentId": "eni-attach-43348162",
        "DeleteOnTermination": true,
        "DeviceIndex": 123,
        "InstanceId": "i-1234567890abcdef0",
        "InstanceOwnerId": "123456789012",
        "Status": 'ATTACHED'
    },
    "SecurityGroups": [
        {
            "GroupName": "my-security-group",
            "GroupId": "sg-903004f8"
        },
    ],
```

```
    "NetworkInterfaceId": 'eni-686ea200',
    "SourceDestCheck": false
}
```

AwsEc2RouteTable

El objeto `AwsEc2RouteTable` proporciona información sobre una tabla de enrutamiento de Amazon EC2.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsEc2RouteTable` objeto. Para ver las descripciones de los atributos `AwsEc2RouteTable`, consulte AwsEc2RouteTableDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsEc2RouteTable": {
    "AssociationSet": [{
     "AssociationSet": {
      "State": "associated"
        },
     "Main": true,
     "RouteTableAssociationId": "rtbassoc-08e706c45de9f7512",
     "RouteTableId": "rtb-0a59bde9cf2548e34",
    }],
    "PropogatingVgwSet": [],
    "RouteTableId": "rtb-0a59bde9cf2548e34",
    "RouteSet": [
     {
      "DestinationCidrBlock": "10.24.34.0/23",
      "GatewayId": "local",
      "Origin": "CreateRouteTable",
      "State": "active"
     },
     {
      "DestinationCidrBlock": "10.24.34.0/24",
      "GatewayId": "igw-0242c2d7d513fc5d3",
      "Origin": "CreateRoute",
      "State": "active"
     }
    ],
    "VpcId": "vpc-0c250a5c33f51d456"
}
```

AwsEc2SecurityGroup

El objeto `AwsEc2SecurityGroup` describe un grupo de seguridad de Amazon EC2.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsEc2SecurityGroup` objeto. Para ver las descripciones de los atributos `AwsEc2SecurityGroup`, consulte AwsEc2SecurityGroupDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsEc2SecurityGroup": {
    "GroupName": "MySecurityGroup",
    "GroupId": "sg-903004f8",
    "OwnerId": "123456789012",
    "VpcId": "vpc-1a2b3c4d",
    "IpPermissions": [
        {
            "IpProtocol": "-1",
            "IpRanges": [],
            "UserIdGroupPairs": [
                {
                    "UserId": "123456789012",
                    "GroupId": "sg-903004f8"
                }
            ],
            "PrefixListIds": [
                {"PrefixListId": "pl-63a5400a"}
            ]
        },
        {
            "PrefixListIds": [],
            "FromPort": 22,
            "IpRanges": [
                {
                    "CidrIp": "203.0.113.0/24"
                }
            ],
            "ToPort": 22,
            "IpProtocol": "tcp",
            "UserIdGroupPairs": []
        }
    ]
```

```
}
```

AwsEc2Subnet

El objeto `AwsEc2Subnet` proporciona información sobre una subred de Amazon EC2.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsEc2Subnet` objeto. Para ver las descripciones de los atributos `AwsEc2Subnet`, consulte AwsEc2SubnetDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
AwsEc2Subnet: {
    "AssignIpv6AddressOnCreation": false,
    "AvailabilityZone": "us-west-2c",
    "AvailabilityZoneId": "usw2-az3",
    "AvailableIpAddressCount": 8185,
    "CidrBlock": "10.0.0.0/24",
    "DefaultForAz": false,
    "MapPublicIpOnLaunch": false,
    "OwnerId": "123456789012",
    "State": "available",
    "SubnetArn": "arn:aws:ec2:us-west-2:123456789012:subnet/subnet-d5436c93",
    "SubnetId": "subnet-d5436c93",
    "VpcId": "vpc-153ade70",
    "Ipv6CidrBlockAssociationSet": [{
        "AssociationId": "subnet-cidr-assoc-EXAMPLE",
        "Ipv6CidrBlock": "2001:DB8::/32",
        "CidrBlockState": "associated"
   }]
}
```

AwsEc2TransitGateway

El objeto `AwsEc2TransitGateway` proporciona detalles acerca de una puerta de enlace de tránsito de Amazon EC2 que interconecta las nubes privadas virtuales (VPC) y las redes en las instalaciones.

El siguiente es un ejemplo de `AwsEc2TransitGateway` búsqueda en el formato de búsqueda AWS de seguridad (ASFF). Para ver las descripciones de los atributos `AwsEc2TransitGateway`, consulte AwsEc2TransitGatewayDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsEc2TransitGateway": {
 "AmazonSideAsn": 65000,
 "AssociationDefaultRouteTableId": "tgw-rtb-099ba47cbbea837cc",
 "AutoAcceptSharedAttachments": "disable",
 "DefaultRouteTableAssociation": "enable",
 "DefaultRouteTablePropagation": "enable",
 "Description": "sample transit gateway",
 "DnsSupport": "enable",
 "Id": "tgw-042ae6bf7a5c126c3",
 "MulticastSupport": "disable",
 "PropagationDefaultRouteTableId": "tgw-rtb-099ba47cbbea837cc",
 "TransitGatewayCidrBlocks": ["10.0.0.0/16"],
 "VpnEcmpSupport": "enable"
}
```

AwsEc2Volume

El objeto `AwsEc2Volume` proporciona información detallada sobre un volumen de Amazon EC2.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsEc2Volume` objeto. Para ver las descripciones de los atributos `AwsEc2Volume`, consulte AwsEc2VolumeDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsEc2Volume": {
    "Attachments": [
      {
        "AttachTime": "2017-10-17T14:47:11Z",
        "DeleteOnTermination": true,
        "InstanceId": "i-123abc456def789g",
        "Status": "attached"
      }
     ],
    "CreateTime": "2020-02-24T15:54:30Z",
    "Encrypted": true,
    "KmsKeyId": "arn:aws:kms:us-east-1:111122223333:key/wJalrXUtnFEMI/K7MDENG/
bPxRfiCYEXAMPLEKEY",
    "Size": 80,
    "SnapshotId": "",
    "Status": "available"
}
```

AwsEc2Vpc

El objeto `AwsEc2Vpc` proporciona información detallada sobre una VPC de Amazon EC2.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsEc2Vpc` objeto. Para ver las descripciones de los atributos `AwsEc2Vpc`, consulte AwsEc2VpcDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsEc2Vpc": {
    "CidrBlockAssociationSet": [
        {
            "AssociationId": "vpc-cidr-assoc-0dc4c852f52abda97",
            "CidrBlock": "192.0.2.0/24",
            "CidrBlockState": "associated"
        }
    ],
    "DhcpOptionsId": "dopt-4e42ce28",
    "Ipv6CidrBlockAssociationSet": [
        {
            "AssociationId": "vpc-cidr-assoc-0dc4c852f52abda97",
            "CidrBlockState": "associated",
            "Ipv6CidrBlock": "192.0.2.0/24"
       }

    ],
    "State": "available"
}
```

AwsEc2VpcEndpointService

El objeto `AwsEc2VpcEndpointService` contiene detalles sobre la configuración del servicio para un servicio de punto de conexión de VPC.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsEc2VpcEndpointService` objeto. Para ver las descripciones de los atributos `AwsEc2VpcEndpointService`, consulte AwsEc2VpcEndpointServiceDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsEc2VpcEndpointService": {
```

```
    "ServiceType": [
      {
        "ServiceType": "Interface"
      }
    ],
    "ServiceId": "vpce-svc-example1",
    "ServiceName": "com.amazonaws.vpce.us-east-1.vpce-svc-example1",
    "ServiceState": "Available",
    "AvailabilityZones": [
      "us-east-1"
    ],
    "AcceptanceRequired": true,
    "ManagesVpcEndpoints": false,
    "NetworkLoadBalancerArns": [
      "arn:aws:elasticloadbalancing:us-east-1:444455556666:loadbalancer/net/my-network-
load-balancer/example1"
    ],
    "GatewayLoadBalancerArns": [],
    "BaseEndpointDnsNames": [
      "vpce-svc-04eec859668b51c34.us-east-1.vpce.amazonaws.com"
    ],
    "PrivateDnsName": "my-private-dns"
}
```

AwsEc2VpcPeeringConnection

El objeto `AwsEc2VpcPeeringConnection` proporciona detalles acerca de la conexión de red entre dos VPC.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsEc2VpcPeeringConnection` objeto. Para ver las descripciones de los atributos `AwsEc2VpcPeeringConnection`, consulte AwsEc2VpcPeeringConnectionDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsEc2VpcPeeringConnection": {
 "AccepterVpcInfo": {
  "CidrBlock": "10.0.0.0/28",
  "CidrBlockSet": [{
   "CidrBlock": "10.0.0.0/28"
  }],
  "Ipv6CidrBlockSet": [{
```

```
    "Ipv6CidrBlock": "2002::1234:abcd:ffff:c0a8:101/64"
   }],
   "OwnerId": "012345678910",
   "PeeringOptions": {
    "AllowDnsResolutionFromRemoteVpc": true,
    "AllowEgressFromLocalClassicLinkToRemoteVpc": false,
    "AllowEgressFromLocalVpcToRemoteClassicLink": true
   },
   "Region": "us-west-2",
   "VpcId": "vpc-i123456"
  },
  "ExpirationTime": "2022-02-18T15:31:53.161Z",
  "RequesterVpcInfo": {
   "CidrBlock": "192.168.0.0/28",
   "CidrBlockSet": [{
    "CidrBlock": "192.168.0.0/28"
   }],
   "Ipv6CidrBlockSet": [{
    "Ipv6CidrBlock": "2002::1234:abcd:ffff:c0a8:101/64"
   }],
   "OwnerId": "012345678910",
   "PeeringOptions": {
    "AllowDnsResolutionFromRemoteVpc": true,
    "AllowEgressFromLocalClassicLinkToRemoteVpc": false,
    "AllowEgressFromLocalVpcToRemoteClassicLink": true
   },
   "Region": "us-west-2",
   "VpcId": "vpc-i123456"
  },
  "Status": {
   "Code": "initiating-request",
   "Message": "Active"
  },
  "VpcPeeringConnectionId": "pcx-1a2b3c4d"
 }
```

AwsEcr recursos en ASFF

Los siguientes son ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para los `AwsEcr` recursos.

AWS Security Hub CSPM normaliza los hallazgos de varias fuentes en el ASFF. Para obtener información general sobre el ASFF, consulte AWS Formato de búsqueda de seguridad (ASFF).

AwsEcrContainerImage

El objeto `AwsEcrContainerImage` proporciona información sobre una imagen de Amazon ECR.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsEcrContainerImage` objeto. Para ver las descripciones de los atributos `AwsEcrContainerImage`, consulte AwsEcrContainerImageDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsEcrContainerImage": {
    "RegistryId": "123456789012",
    "RepositoryName": "repository-name",
    "Architecture": "amd64"
    "ImageDigest":
 "sha256:a568e5c7a953fbeaa2904ac83401f93e4a076972dc1bae527832f5349cd2fb10",
    "ImageTags": ["00000000-0000-0000-0000-000000000000"],
    "ImagePublishedAt": "2019-10-01T20:06:12Z"
}
```

AwsEcrRepository

El objeto `AwsEcrRepository` proporciona información sobre un repositorio de Amazon Elastic Container Registry.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsEcrRepository` objeto. Para ver las descripciones de los atributos `AwsEcrRepository`, consulte AwsEcrRepositoryDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsEcrRepository": {
    "LifecyclePolicy": {
        "RegistryId": "123456789012",
    },
    "RepositoryName": "sample-repo",
    "Arn": "arn:aws:ecr:us-west-2:111122223333:repository/sample-repo",
    "ImageScanningConfiguration": {
        "ScanOnPush": true
    },
    "ImageTagMutability": "IMMUTABLE"
```

```
}
```

AwsEcs recursos en ASFF

Los siguientes son ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para `AwsEcs` los recursos.

AWS Security Hub CSPM normaliza los hallazgos de varias fuentes en el ASFF. Para obtener información general sobre el ASFF, consulte AWS Formato de búsqueda de seguridad (ASFF).

AwsEcsCluster

El objeto `AwsEcsCluster` proporciona detalles sobre un clúster de Amazon Elastic Container Service.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsEcsCluster` objeto. Para ver las descripciones de los atributos `AwsEcsCluster`, consulte AwsEcsClusterDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
    "AwsEcsCluster": {
        "CapacityProviders": [],
        "ClusterSettings": [
            {
                "Name": "containerInsights",
                "Value": "enabled"
            }
        ],
        "Configuration": {
            "ExecuteCommandConfiguration": {
                "KmsKeyId": "kmsKeyId",
                "LogConfiguration": {
                    "CloudWatchEncryptionEnabled": true,
                    "CloudWatchLogGroupName": "cloudWatchLogGroupName",
                    "S3BucketName": "s3BucketName",
                    "S3EncryptionEnabled": true,
                    "S3KeyPrefix": "s3KeyPrefix"
                },
                "Logging": "DEFAULT"
            }
        }
        "DefaultCapacityProviderStrategy": [
```

```
            {
                "Base": 0,
                "CapacityProvider": "capacityProvider",
                "Weight": 1
            }
        ]
    }
```

AwsEcsContainer

El objeto de `AwsEcsContainer` contiene detalles sobre un contenedor Amazon ECS.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsEcsContainer` objeto. Para ver las descripciones de los atributos `AwsEcsContainer`, consulte AwsEcsContainerDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsEcsContainer": {
    "Image": "1111111/
knotejs@sha256:356131c9fef111111111111115f4ed8de5f9dce4dc3bd34bg21846588a3",
    "MountPoints": [{
        "ContainerPath": "/mnt/etc",
        "SourceVolume": "vol-03909e9"
    }],
    "Name": "knote",
    "Privileged": true
}
```

AwsEcsService

El objeto `AwsEcsService` proporciona detalles acerca de un servicio dentro de un clúster de Amazon ECS.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsEcsService` objeto. Para ver las descripciones de los atributos `AwsEcsService`, consulte AwsEcsServiceDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsEcsService": {
    "CapacityProviderStrategy": [
        {
```

```
            "Base": 12,
            "CapacityProvider": "",
            "Weight": ""
        }
    ],
    "Cluster": "arn:aws:ecs:us-east-1:111122223333:cluster/example-ecs-cluster",
    "DeploymentConfiguration": {
        "DeploymentCircuitBreaker": {
            "Enable": false,
            "Rollback": false
        },
        "MaximumPercent": 200,
        "MinimumHealthyPercent": 100
    },
    "DeploymentController": "",
    "DesiredCount": 1,
    "EnableEcsManagedTags": false,
    "EnableExecuteCommand": false,
    "HealthCheckGracePeriodSeconds": 1,
    "LaunchType": "FARGATE",
    "LoadBalancers": [
        {
            "ContainerName": "",
            "ContainerPort": 23,
            "LoadBalancerName": "",
            "TargetGroupArn": ""
        }
    ],
    "Name": "sample-app-service",
    "NetworkConfiguration": {
        "AwsVpcConfiguration": {
            "Subnets": [
                "Subnet-example1",
                "Subnet-example2"
            ],
        "SecurityGroups": [
                "Sg-0ce48e9a6e5b457f5"
        ],
        "AssignPublicIp": "ENABLED"
        }
    },
    "PlacementConstraints": [
        {
            "Expression": "",
```

```
            "Type": ""
        }
    ],
    "PlacementStrategies": [
        {
            "Field": "",
            "Type": ""
        }
    ],
    "PlatformVersion": "LATEST",
    "PropagateTags": "",
    "Role": "arn:aws:iam::111122223333:role/aws-servicerole/ecs.amazonaws.com/
ServiceRoleForECS",
    "SchedulingStrategy": "REPLICA",
    "ServiceName": "sample-app-service",
    "ServiceArn": "arn:aws:ecs:us-east-1:111122223333:service/example-ecs-cluster/
sample-app-service",
    "ServiceRegistries": [
        {
            "ContainerName": "",
            "ContainerPort": 1212,
            "Port": 1221,
            "RegistryArn": ""
        }
    ],
    "TaskDefinition": "arn:aws:ecs:us-east-1:111122223333:task-definition/example-
taskdef:1"
}
```

AwsEcsTask

El objeto `AwsEcsTask` proporciona detalles sobre una tarea de Amazon ECS.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsEcsTask` objeto. Para ver las descripciones de los atributos `AwsEcsTask`, consulte AwsEcsTask en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsEcsTask": {
 "ClusterArn": "arn:aws:ecs:us-west-2:123456789012:task/MyCluster/1234567890123456789",
 "CreatedAt": "1557134011644",
 "Group": "service:fargate-service",
```

```
 "StartedAt": "1557134011644",
 "StartedBy": "ecs-svc/1234567890123456789",
 "TaskDefinitionArn": "arn:aws:ecs:us-west-2:123456789012:task-definition/sample-
fargate:2",
 "Version": 3,
 "Volumes": [{
  "Name": "string",
  "Host": {
   "SourcePath": "string"
  }
 }],
 "Containers": {
  "Image": "1111111/
knotejs@sha256:356131c9fef111111111111115f4ed8de5f9dce4dc3bd34bg21846588a3",
  "MountPoints": [{
   "ContainerPath": "/mnt/etc",
   "SourceVolume": "vol-03909e9"
  }],
  "Name": "knote",
  "Privileged": true
 }
}
```

AwsEcsTaskDefinition

El objeto `AwsEcsTaskDefinition` contiene detalles sobre la definición de una tarea. Una definición de tarea describe las definiciones de contenedor y volumen de una tarea de Amazon Elastic Container Service.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsEcsTaskDefinition` objeto. Para ver las descripciones de los atributos `AwsEcsTaskDefinition`, consulte AwsEcsTaskDefinitionDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
    "AwsEcsTaskDefinition": {
        "ContainerDefinitions": [
            {
                "Command": ['ruby', 'hi.rb'],
                "Cpu":128,
                "Essential": true,
                "HealthCheck": {
```

```
                "Command": ["CMD-SHELL", "curl -f http://localhost/ || exit 1"],
                "Interval": 10,
                "Retries": 3,
                "StartPeriod": 5,
                "Timeout": 20
            },
            "Image": "tongueroo/sinatra:latest",
            "Interactive": true,
            "Links": [],
            "LogConfiguration": {
                "LogDriver": "awslogs",
                "Options": {
                    "awslogs-group": "/ecs/sinatra-hi",
                    "awslogs-region": "ap-southeast-1",
                    "awslogs-stream-prefix": "ecs"
                },
                "SecretOptions": []

            },
            "MemoryReservation": 128,
            "Name": "web",
            "PortMappings": [
                {
                    "ContainerPort": 4567,
                    "HostPort":4567,
                    "Protocol": "tcp"
                }
            ],
            "Privileged": true,
            "StartTimeout": 10,
            "StopTimeout": 100,
        }
    ],
    "Family": "sinatra-hi",
    "NetworkMode": "host",
    "RequiresCompatibilities": ["EC2"],
    "Status": "ACTIVE",
    "TaskRoleArn": "arn:aws:iam::111122223333:role/ecsTaskExecutionRole",
}
```

AwsEfs recursos en ASFF

Los siguientes son ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para `AwsEfs` los recursos.

AWS Security Hub CSPM normaliza los hallazgos de varias fuentes en el ASFF. Para obtener información general sobre el ASFF, consulte AWS Formato de búsqueda de seguridad (ASFF).

AwsEfsAccessPoint

El objeto `AwsEfsAccessPoint` proporciona detalles sobre los archivos almacenados en Amazon Elastic File System.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsEfsAccessPoint` objeto. Para ver las descripciones de los atributos `AwsEfsAccessPoint`, consulte AwsEfsAccessPointDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsEfsAccessPoint": {
 "AccessPointId": "fsap-05c4c0e79ba0b118a",
 "Arn": "arn:aws:elasticfilesystem:us-east-1:863155670886:access-point/
fsap-05c4c0e79ba0b118a",
 "ClientToken": "AccessPointCompliant-ASk06ZZSXsEp",
 "FileSystemId": "fs-0f8137f731cb32146",
 "PosixUser": {
  "Gid": "1000",
  "SecondaryGids": ["0", "4294967295"],
  "Uid": "1234"
 },
 "RootDirectory": {
  "CreationInfo": {
   "OwnerGid": "1000",
   "OwnerUid": "1234",
   "Permissions": "777"
  },
  "Path": "/tmp/example"
 }
}
```

AwsEks recursos en ASFF

Los siguientes son ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para `AwsEks` los recursos.

AWS Security Hub CSPM normaliza los hallazgos de varias fuentes en el ASFF. Para obtener información general sobre el ASFF, consulte AWS Formato de búsqueda de seguridad (ASFF).

AwsEksCluster

El objeto `AwsEksCluster` proporciona detalles sobre un clúster de Amazon EKS.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsEksCluster` objeto. Para ver las descripciones de los atributos `AwsEksCluster`, consulte AwsEksClusterDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
{
  "AwsEksCluster": {
    "Name": "example",
    "Arn": "arn:aws:eks:us-west-2:222222222222:cluster/example",
    "CreatedAt": 1565804921.901,
    "Version": "1.12",
    "RoleArn": "arn:aws:iam::222222222222:role/example-cluster-
ServiceRole-1XWBQWYSFRE2Q",
    "ResourcesVpcConfig": {
      "EndpointPublicAccess": false,
      "SubnetIds": [
        "subnet-021345abcdef6789",
        "subnet-abcdef01234567890",
        "subnet-1234567890abcdef0"
      ],
      "SecurityGroupIds": [
        "sg-abcdef01234567890"
      ]
    },
    "Logging": {
      "ClusterLogging": [
        {
          "Types": [
            "api",
            "audit",
            "authenticator",
```

```
            "controllerManager",
            "scheduler"
          ],
          "Enabled": true
        }
      ]
    },
    "Status": "CREATING",
    "CertificateAuthorityData": {},
  }
}
```

AwsElasticBeanstalk recursos en ASFF

Los siguientes son ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para los recursos. `AwsElasticBeanstalk`

AWS Security Hub CSPM normaliza los hallazgos de varias fuentes en el ASFF. Para obtener información general sobre el ASFF, consulte AWS Formato de búsqueda de seguridad (ASFF).

AwsElasticBeanstalkEnvironment

El objeto `AwsElasticBeanstalkEnvironment` contiene detalles sobre un entorno de AWS Elastic Beanstalk .

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsElasticBeanstalkEnvironment` objeto. Para ver las descripciones de los atributos `AwsElasticBeanstalkEnvironment`, consulte AwsElasticBeanstalkEnvironmentDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsElasticBeanstalkEnvironment": {
    "ApplicationName": "MyApplication",
    "Cname": "myexampleapp-env.devo-2.elasticbeanstalk-internal.com",
    "DateCreated": "2021-04-30T01:38:01.090Z",
    "DateUpdated": "2021-04-30T01:38:01.090Z",
    "Description": "Example description of my awesome application",
    "EndpointUrl": "eb-dv-e-p-AWSEBLoa-abcdef01234567890-021345abcdef6789.us-
east-1.elb.amazonaws.com",
    "EnvironmentArn": "arn:aws:elasticbeanstalk:us-east-1:123456789012:environment/
MyApplication/myapplication-env",
    "EnvironmentId": "e-abcd1234",
```

```
    "EnvironmentLinks": [
        {
            "EnvironmentName": "myexampleapp-env",
            "LinkName": "myapplicationLink"
        }
    ],
    "EnvironmentName": "myapplication-env",
    "OptionSettings": [
        {
            "Namespace": "aws:elasticbeanstalk:command",
            "OptionName": "BatchSize",
            "Value": "100"
        },
        {
            "Namespace": "aws:elasticbeanstalk:command",
            "OptionName": "Timeout",
            "Value": "600"
        },
        {
            "Namespace": "aws:elasticbeanstalk:command",
            "OptionName": "BatchSizeType",
            "Value": "Percentage"
        },
        {
            "Namespace": "aws:elasticbeanstalk:command",
            "OptionName": "IgnoreHealthCheck",
            "Value": "false"
        },
        {
            "Namespace": "aws:elasticbeanstalk:application",
            "OptionName": "Application Healthcheck URL",
            "Value": "TCP:80"
        }
    ],
    "PlatformArn": "arn:aws:elasticbeanstalk:us-east-1::platform/Tomcat 8 with Java 8
 running on 64bit Amazon Linux/2.7.7",
    "SolutionStackName": "64bit Amazon Linux 2017.09 v2.7.7 running Tomcat 8 Java 8",
    "Status": "Ready",
    "Tier": {
        "Name": "WebServer"
       "Type": "Standard"
       "Version": "1.0"
    },
    "VersionLabel": "Sample Application"
```

```
}
```

AwsElasticSearch recursos en ASFF

Los siguientes son ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para `AwsElasticSearch` los recursos.

AWS Security Hub CSPM normaliza los hallazgos de varias fuentes en el ASFF. Para obtener información general sobre el ASFF, consulte AWS Formato de búsqueda de seguridad (ASFF).

AwsElasticSearchDomain

El `AwsElasticSearchDomain` objeto proporciona detalles sobre un dominio de Amazon OpenSearch Service.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsElasticSearchDomain` objeto. Para ver las descripciones de los atributos `AwsElasticSearchDomain`, consulte AwsElasticSearchDomainDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsElasticSearchDomain": {
    "AccessPolicies": "string",
    "DomainStatus": {
           "DomainId": "string",
           "DomainName": "string",
           "Endpoint": "string",
           "Endpoints": {
                  "string": "string"
           }
    },
    "DomainEndpointOptions": {
           "EnforceHTTPS": boolean,
           "TLSSecurityPolicy": "string"
    },
    "ElasticsearchClusterConfig": {
           "DedicatedMasterCount": number,
           "DedicatedMasterEnabled": boolean,
           "DedicatedMasterType": "string",
           "InstanceCount": number,
           "InstanceType": "string",
           "ZoneAwarenessConfig": {
```

```
                "AvailabilityZoneCount": number
        },
        "ZoneAwarenessEnabled": boolean
    },
    "ElasticsearchVersion": "string",
    "EncryptionAtRestOptions": {
        "Enabled": boolean,
        "KmsKeyId": "string"
    },
    "LogPublishingOptions": {
        "AuditLogs": {
                "CloudWatchLogsLogGroupArn": "string",
                "Enabled": boolean
        },
        "IndexSlowLogs": {
                "CloudWatchLogsLogGroupArn": "string",
                "Enabled": boolean
        },
        "SearchSlowLogs": {
                "CloudWatchLogsLogGroupArn": "string",
                "Enabled": boolean
        }
    },
    "NodeToNodeEncryptionOptions": {
        "Enabled": boolean
    },
    "ServiceSoftwareOptions": {
        "AutomatedUpdateDate": "string",
        "Cancellable": boolean,
        "CurrentVersion": "string",
        "Description": "string",
        "NewVersion": "string",
        "UpdateAvailable": boolean,
        "UpdateStatus": "string"
    },
    "VPCOptions": {
        "AvailabilityZones": [
            "string"
        ],
        "SecurityGroupIds": [
            "string"
        ],
        "SubnetIds": [
            "string"
```

```
            ],
           "VPCId": "string"
    }
}
```

AwsElb recursos en ASFF

Los siguientes son ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para `AwsElb` los recursos.

AWS Security Hub CSPM normaliza los hallazgos de varias fuentes en el ASFF. Para obtener información general sobre el ASFF, consulte AWS Formato de búsqueda de seguridad (ASFF).

AwsElbLoadBalancer

El objeto `AwsElbLoadBalancer` contiene detalles sobre un Equilibrador de carga clásico.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsElbLoadBalancer` objeto. Para ver las descripciones de los atributos `AwsElbLoadBalancer`, consulte AwsElbLoadBalancerDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsElbLoadBalancer": {
    "AvailabilityZones": ["us-west-2a"],
    "BackendServerDescriptions": [
         {
            "InstancePort": 80,
            "PolicyNames": ["doc-example-policy"]
        }
    ],
    "CanonicalHostedZoneName": "Z3DZXE0EXAMPLE",
    "CanonicalHostedZoneNameID": "my-load-balancer-444455556666.us-
west-2.elb.amazonaws.com",
    "CreatedTime": "2020-08-03T19:22:44.637Z",
    "DnsName": "my-load-balancer-444455556666.us-west-2.elb.amazonaws.com",
    "HealthCheck": {
        "HealthyThreshold": 2,
        "Interval": 30,
        "Target": "HTTP:80/png",
        "Timeout": 3,
        "UnhealthyThreshold": 2
    },
    "Instances": [
```

```
        {
            "InstanceId": "i-example"
        }
    ],
    "ListenerDescriptions": [
        {
            "Listener": {
                "InstancePort": 443,
                "InstanceProtocol": "HTTPS",
                "LoadBalancerPort": 443,
                "Protocol": "HTTPS",
                "SslCertificateId": "arn:aws:iam::444455556666:server-certificate/my-
server-cert"
            },
            "PolicyNames": ["ELBSecurityPolicy-TLS-1-2-2017-01"]
        }
    ],
    "LoadBalancerAttributes": {
        "AccessLog": {
            "EmitInterval": 60,
            "Enabled": true,
            "S3BucketName": "amzn-s3-demo-bucket",
            "S3BucketPrefix": "doc-example-prefix"
        },
        "ConnectionDraining": {
            "Enabled": false,
            "Timeout": 300
        },
        "ConnectionSettings": {
            "IdleTimeout": 30
        },
        "CrossZoneLoadBalancing": {
            "Enabled": true
        },
        "AdditionalAttributes": [{
            "Key": "elb.http.desyncmitigationmode",
            "Value": "strictest"
        }]

    },
    "LoadBalancerName": "example-load-balancer",
    "Policies": {
        "AppCookieStickinessPolicies": [
            {
```

```
                "CookieName": "",
                "PolicyName": ""
            }
        ],
        "LbCookieStickinessPolicies": [
            {
                "CookieExpirationPeriod": 60,
                "PolicyName": "my-example-cookie-policy"
            }
        ],
        "OtherPolicies": [
            "my-PublicKey-policy",
            "my-authentication-policy",
            "my-SSLNegotiation-policy",
            "my-ProxyProtocol-policy",
            "ELBSecurityPolicy-2015-03"
        ]
    },
    "Scheme": "internet-facing",
    "SecurityGroups": ["sg-example"],
    "SourceSecurityGroup": {
        "GroupName": "my-elb-example-group",
        "OwnerAlias": "444455556666"
    },
    "Subnets": ["subnet-example"],
    "VpcId": "vpc-a01106c2"
}
```

AwsElbv2LoadBalancer

El objeto `AwsElbv2LoadBalancer` proporciona información sobre un balanceador de carga.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsElbv2LoadBalancer` objeto. Para ver las descripciones de los atributos `AwsElbv2LoadBalancer`, consulte AwsElbv2LoadBalancerDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsElbv2LoadBalancer": {
                        "AvailabilityZones": {
                            "SubnetId": "string",
                            "ZoneName": "string"
```

```
                    },
                    "CanonicalHostedZoneId": "string",
                    "CreatedTime": "string",
                    "DNSName": "string",
                    "IpAddressType": "string",
                    "LoadBalancerAttributes": [
                        {
                            "Key": "string",
                            "Value": "string"
                        }
                    ],
                    "Scheme": "string",
                    "SecurityGroups": [ "string" ],
                    "State": {
                        "Code": "string",
                        "Reason": "string"
                    },
                    "Type": "string",
                    "VpcId": "string"
                }
```

AwsEventBridge recursos en ASFF

Los siguientes son ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para `AwsEventBridge` los recursos.

AWS Security Hub CSPM normaliza los hallazgos de varias fuentes en el ASFF. Para obtener información general sobre el ASFF, consulte AWS Formato de búsqueda de seguridad (ASFF).

AwsEventSchemasRegistry

El `AwsEventSchemasRegistry` objeto proporciona información sobre un registro de EventBridge esquemas de Amazon. Un esquema define la estructura de los eventos a los que se envían EventBridge. Los registros de esquemas son contenedores que recopilan y agrupan lógicamente sus esquemas.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsEventSchemasRegistry` objeto. Para ver las descripciones de los atributos `AwsEventSchemasRegistry`, consulte AwsEventSchemasRegistry en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsEventSchemasRegistry": {
    "Description": "This is an example event schema registry.",
    "RegistryArn": "arn:aws:schemas:us-east-1:123456789012:registry/schema-registry",
    "RegistryName": "schema-registry"
}
```

AwsEventsEndpoint

El `AwsEventsEndpoint` objeto proporciona información sobre un punto final EventBridge global de Amazon. El punto final puede mejorar la disponibilidad de la aplicación al hacerla Regional-fault tolerante.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsEventsEndpoint` objeto. Para ver las descripciones de los atributos `AwsEventsEndpoint`, consulte AwsEventsEndpointDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsEventsEndpoint": {
    "Arn": "arn:aws:events:us-east-1:123456789012:endpoint/my-endpoint",
    "Description": "This is a sample endpoint.",
    "EndpointId": "04k1exajoy.veo",
    "EndpointUrl": "https://04k1exajoy.veo.endpoint.events.amazonaws.com",
    "EventBuses": [
        {
            "EventBusArn": "arn:aws:events:us-east-1:123456789012:event-bus/default"
        },
        {
            "EventBusArn": "arn:aws:events:us-east-2:123456789012:event-bus/default"
        }
    ],
    "Name": "my-endpoint",
    "ReplicationConfig": {
        "State": "ENABLED"
    },
    "RoleArn": "arn:aws:iam::123456789012:role/service-role/
Amazon_EventBridge_Invoke_Event_Bus_1258925394",
    "RoutingConfig": {
        "FailoverConfig": {
            "Primary": {
                "HealthCheck": "arn:aws:route53:::healthcheck/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
```

```
            },
            "Secondary": {
                "Route": "us-east-2"
            }
        }
    },
    "State": "ACTIVE"
}
```

AwsEventsEventbus

El `AwsEventsEventbus` objeto proporciona información sobre un punto final EventBridge global de Amazon. El punto final puede mejorar la disponibilidad de la aplicación al hacerla Regional-fault tolerante.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsEventsEventbus` objeto. Para ver las descripciones de los atributos `AwsEventsEventbus`, consulte AwsEventsEventbusDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsEventsEventbus":
    "Arn": "arn:aws:events:us-east-1:123456789012:event-bus/my-event-bus",
    "Name": "my-event-bus",
    "Policy": "{\"Version\":\"2012-10-17\",       \"Statement\":[{\"Sid
\":\"AllowAllAccountsFromOrganizationToPutEvents\",\"Effect\":\"Allow
\",\"Principal\":\"*\",\"Action\":\"events:PutEvents\",\"Resource\":
\"arn:aws:events:us-east-1:123456789012:event-bus/my-event-bus\",\"Condition
\":{\"StringEquals\":{\"aws:PrincipalOrgID\":\"o-ki7yjtkjv5\"}}},{\"Sid\":
\"AllowAccountToManageRulesTheyCreated\",\"Effect\":\"Allow\",\"Principal\":{\"AWS\":
\"arn:aws:iam::123456789012:root\"},\"Action\":[\"events:PutRule\",\"events:PutTargets
\",\"events:DeleteRule\",\"events:RemoveTargets\",\"events:DisableRule\",
\"events:EnableRule\",\"events:TagResource\",\"events:UntagResource\",
\"events:DescribeRule\",\"events:ListTargetsByRule\",\"events:ListTagsForResource\"],
\"Resource\":\"arn:aws:events:us-east-1:123456789012:rule/my-event-bus\",\"Condition\":
{\"StringEqualsIfExists\":{\"events:creatorAccount\":\"123456789012\"}}}]}"
```

AwsGuardDuty recursos en ASFF

Los siguientes son ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para `AwsGuardDuty` los recursos.

AWS Security Hub CSPM normaliza los hallazgos de varias fuentes en el ASFF. Para obtener información general sobre el ASFF, consulte AWS Formato de búsqueda de seguridad (ASFF).

AwsGuardDutyDetector

El `AwsGuardDutyDetector` objeto proporciona información sobre un GuardDuty detector de Amazon. Un detector es un objeto que representa el GuardDuty servicio. Se requiere un detector GuardDuty para que esté en funcionamiento.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsGuardDutyDetector` objeto. Para ver las descripciones de los atributos `AwsGuardDutyDetector`, consulte AwsGuardDutyDetector en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsGuardDutyDetector": {
    "FindingPublishingFrequency": "SIX_HOURS",
    "ServiceRole": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty",
    "Status": "ENABLED",
    "DataSources": {
        "CloudTrail": {
            "Status": "ENABLED"
        },
        "DnsLogs": {
            "Status": "ENABLED"
        },
        "FlowLogs": {
            "Status": "ENABLED"
        },
        "S3Logs": {
             "Status": "ENABLED"
         },
         "Kubernetes": {
             "AuditLogs": {
                "Status": "ENABLED"
             }
         },
         "MalwareProtection": {
             "ScanEc2InstanceWithFindings": {
                "EbsVolumes": {
                    "Status": "ENABLED"
```

```
                }
            },
            "ServiceRole": "arn:aws:iam::123456789012:role/aws-service-role/malware-
protection.guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDutyMalwareProtection"
        }
    }
}
```

AwsIam recursos en ASFF

Los siguientes son ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para los `AwsIam` recursos.

AWS Security Hub CSPM normaliza los hallazgos de varias fuentes en el ASFF. Para obtener información general sobre el ASFF, consulte AWS Formato de búsqueda de seguridad (ASFF).

AwsIamAccessKey

El objeto `AwsIamAccessKey` contiene detalles sobre una clave de acceso de IAM relacionada con un resultado.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsIamAccessKey` objeto. Para ver las descripciones de los atributos `AwsIamAccessKey`, consulte AwsIamAccessKeyDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsIamAccessKey": {
                        "AccessKeyId": "string",
                        "AccountId": "string",
                        "CreatedAt": "string",
                        "PrincipalId": "string",
                        "PrincipalName": "string",
                        "PrincipalType": "string",
                        "SessionContext": {
                            "Attributes": {
                                "CreationDate": "string",
                                "MfaAuthenticated": boolean
                            },
                            "SessionIssuer": {
                                "AccountId": "string",
                                "Arn": "string",
                                "PrincipalId": "string",
```

```
                                "Type": "string",
                                "UserName": "string"
                            }
                        },
                        "Status": "string"
                    }
```

AwsIamGroup

El objeto `AwsIamGroup` contiene detalles acerca de un grupo de IAM.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsIamGroup` objeto. Para ver las descripciones de los atributos `AwsIamGroup`, consulte AwsIamGroupDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsIamGroup": {
    "AttachedManagedPolicies": [
        {
            "PolicyArn": "arn:aws:iam::aws:policy/ExampleManagedAccess",
            "PolicyName": "ExampleManagedAccess",
        }
    ],
    "CreateDate": "2020-04-28T14:08:37.000Z",
    "GroupId": "AGPA4TPS3VLP7QEXAMPLE",
    "GroupName": "Example_User_Group",
    "GroupPolicyList": [
        {
            "PolicyName": "ExampleGroupPolicy"
        }
    ],
    "Path": "/"
}
```

AwsIamPolicy

El objeto `AwsIamPolicy` representa una política de permisos de IAM.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsIamPolicy` objeto. Para ver las descripciones de los atributos `AwsIamPolicy`, consulte AwsIamPolicyDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsIamPolicy": {
    "AttachmentCount": 1,
    "CreateDate": "2017-09-14T08:17:29.000Z",
    "DefaultVersionId": "v1",
    "Description": "Example IAM policy",
    "IsAttachable": true,
    "Path": "/",
    "PermissionsBoundaryUsageCount": 5,
    "PolicyId": "ANPAJ2UCCR6DPCEXAMPLE",
    "PolicyName": "EXAMPLE-MANAGED-POLICY",
    "PolicyVersionList": [
        {
            "VersionId": "v1",
            "IsDefaultVersion": true,
            "CreateDate": "2017-09-14T08:17:29.000Z"
        }
    ],
    "UpdateDate": "2017-09-14T08:17:29.000Z"
}
```

AwsIamRole

El objeto `AwsIamRole` contiene información sobre un rol de IAM, incluidas todas las políticas del rol.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsIamRole` objeto. Para ver las descripciones de los atributos `AwsIamRole`, consulte AwsIamRoleDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsIamRole": {
    "AssumeRolePolicyDocument": "{'Version': '2012-10-17',       'Statement':
 [{'Effect': 'Allow','Action': 'sts:AssumeRole'}]}",
    "AttachedManagedPolicies": [
        {
            "PolicyArn": "arn:aws:iam::aws:policy/ExamplePolicy1",
            "PolicyName": "Example policy 1"
        },
        {
            "PolicyArn": "arn:aws:iam::444455556666:policy/ExamplePolicy2",
```

```
            "PolicyName": "Example policy 2"
        }
        ],
        "CreateDate": "2020-03-14T07:19:14.000Z",
        "InstanceProfileList": [
            {
                "Arn": "arn:aws:iam::333333333333:ExampleProfile",
                "CreateDate": "2020-03-11T00:02:27Z",
                "InstanceProfileId": "AIPAIXEU4NUHUPEXAMPLE",
                "InstanceProfileName": "ExampleInstanceProfile",
                "Path": "/",
                "Roles": [
                    {
                       "Arn": "arn:aws:iam::444455556666:role/example-role",
                        "AssumeRolePolicyDocument": "",
                        "CreateDate": "2020-03-11T00:02:27Z",
                        "Path": "/",
                        "RoleId": "AROAJ52OTH4H7LEXAMPLE",
                        "RoleName": "example-role",
                    }
                ]
            }
        ],
        "MaxSessionDuration": 3600,
        "Path": "/",
        "PermissionsBoundary": {
            "PermissionsBoundaryArn": "arn:aws:iam::aws:policy/AdministratorAccess",
            "PermissionsBoundaryType": "PermissionsBoundaryPolicy"
        },
        "RoleId": "AROA4TPS3VLEXAMPLE",
        "RoleName": "BONESBootstrapHydra-OverbridgeOpsFunctionsLambda",
        "RolePolicyList": [
            {
                "PolicyName": "Example role policy"
            }
        ]
    }
```

AwsIamUser

El objeto `AwsIamUser` proporciona información sobre un usuario.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsIamUser` objeto. Para ver las descripciones de los atributos `AwsIamUser`, consulte AwsIamUserDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsIamUser": {
    "AttachedManagedPolicies": [
        {
            "PolicyName": "ExamplePolicy",
            "PolicyArn": "arn:aws:iam::aws:policy/ExampleAccess"
        }
    ],
    "CreateDate": "2018-01-26T23:50:05.000Z",
    "GroupList": [],
    "Path": "/",
    "PermissionsBoundary" : {
        "PermissionsBoundaryArn" : "arn:aws:iam::aws:policy/AdministratorAccess",
        "PermissionsBoundaryType" : "PermissionsBoundaryPolicy"
    },
    "UserId": "AIDACKCEVSQ6C2EXAMPLE",
    "UserName": "ExampleUser",
    "UserPolicyList": [
        {
            "PolicyName": "InstancePolicy"
        }
    ]
}
```

AwsKinesis recursos en ASFF

Los siguientes son ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para los `AwsKinesis` recursos.

AWS Security Hub CSPM normaliza los hallazgos de varias fuentes en el ASFF. Para obtener información general sobre el ASFF, consulte AWS Formato de búsqueda de seguridad (ASFF).

AwsKinesisStream

El objeto `AwsKinesisStream` proporciona detalles sobre Amazon Kinesis Data Streams.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsKinesisStream` objeto. Para ver las descripciones de los atributos `AwsKinesisStream`, consulte AwsKinesisStreamDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsKinesisStream": {
 "Name": "test-vir-kinesis-stream",
 "Arn": "arn:aws:kinesis:us-east-1:293279581038:stream/test-vir-kinesis-stream",
 "RetentionPeriodHours": 24,
 "ShardCount": 2,
 "StreamEncryption": {
  "EncryptionType": "KMS",
  "KeyId": "arn:aws:kms:us-east-1:293279581038:key/849cf029-4143-4c59-91f8-
ea76007247eb"
 }
}
```

AwsKms recursos en ASFF

Los siguientes son ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para `AwsKms` los recursos.

AWS Security Hub CSPM normaliza los hallazgos de varias fuentes en el ASFF. Para obtener información general sobre el ASFF, consulte AWS Formato de búsqueda de seguridad (ASFF).

AwsKmsKey

El `AwsKmsKey` objeto proporciona detalles sobre un AWS KMS key.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsKmsKey` objeto. Para ver las descripciones de los atributos `AwsKmsKey`, consulte AwsKmsKeyDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsKmsKey": {
                        "AWSAccountId": "string",
                        "CreationDate": "string",
                        "Description": "string",
                        "KeyId": "string",
                        "KeyManager": "string",
```

```
                        "KeyRotationStatus": boolean,
                        "KeyState": "string",
                        "Origin": "string"
                    }
```

AwsLambda

Los siguientes son ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para los `AwsLambda` recursos.

AWS Security Hub CSPM normaliza los hallazgos de varias fuentes en el ASFF. Para obtener información general sobre el ASFF, consulte AWS Formato de búsqueda de seguridad (ASFF).

AwsLambdaFunction

El objeto `AwsLambdaFunction` proporciona detalles sobre la configuración de una función de Lambda.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsLambdaFunction` objeto. Para ver las descripciones de los atributos `AwsLambdaFunction`, consulte AwsLambdaFunctionDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsLambdaFunction": {
    "Architectures": [
        "x86_64"
    ],
    "Code": {
        "S3Bucket": "amzn-s3-demo-bucket",
        "S3Key": "samplekey",
        "S3ObjectVersion": "2",
        "ZipFile": "myzip.zip"
    },
    "CodeSha256": "1111111111111abcdef",
    "DeadLetterConfig": {
        "TargetArn": "arn:aws:lambda:us-east-2:123456789012:queue:myqueue:2"
    },
    "Environment": {
        "Variables": {
            "Stage": "foobar"
         },
        "Error": {
```

```
            "ErrorCode": "Sample-error-code",
            "Message": "Caller principal is a manager."
        }
    },
    "FunctionName": "CheckOut",
    "Handler": "main.py:lambda_handler",
    "KmsKeyArn": "arn:aws:kms:us-west-2:123456789012:key/mykey",
    "LastModified": "2001-09-11T09:00:00Z",
    "Layers": {
        "Arn": "arn:aws:lambda:us-east-2:123456789012:layer:my-layer:3",
        "CodeSize": 169
    },
    "PackageType": "Zip",
    "RevisionId": "23",
    "Role": "arn:aws:iam::123456789012:role/Accounting-Role",
    "Runtime": "go1.7",
    "Timeout": 15,
    "TracingConfig": {
        "Mode": "Active"
    },
    "Version": "$LATEST$",
    "VpcConfig": {
        "SecurityGroupIds": ["sg-085912345678492fb", "sg-08591234567bdgdc"],
         "SubnetIds": ["subnet-071f712345678e7c8", "subnet-07fd123456788a036"]
    },
    "MasterArn": "arn:aws:lambda:us-east-2:123456789012:\$LATEST",
    "MemorySize": 2048
}
```

AwsLambdaLayerVersion

El objeto `AwsLambdaLayerVersion` proporciona detalles sobre una versión de la capa de Lambda.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsLambdaLayerVersion` objeto. Para ver las descripciones de los atributos `AwsLambdaLayerVersion`, consulte AwsLambdaLayerVersionDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsLambdaLayerVersion": {
    "Version": 2,
    "CompatibleRuntimes": [
```

```
        "java8"
    ],
    "CreatedDate": "2019-10-09T22:02:00.274+0000"
}
```

AwsMsk recursos en ASFF

Los siguientes son ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para los `AwsMsk` recursos.

AWS Security Hub CSPM normaliza los hallazgos de varias fuentes en el ASFF. Para obtener información general sobre el ASFF, consulte AWS Formato de búsqueda de seguridad (ASFF).

AwsMskCluster

El objeto `AwsMskCluster` proporciona información sobre un clúster de Amazon Managed Streaming para Apache Kafka (Amazon MSK).

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsMskCluster` objeto. Para ver las descripciones de los atributos `AwsMskCluster`, consulte AwsMskClusterDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsMskCluster": {
        "ClusterInfo": {
            "ClientAuthentication": {
                "Sasl": {
                    "Scram": {
                        "Enabled": true
                    },
                    "Iam": {
                        "Enabled": true
                    }
                },
                "Tls": {
                    "CertificateAuthorityArnList": [],
                    "Enabled": false
                },
                "Unauthenticated": {
                    "Enabled": false
                }
            },
```

```
            "ClusterName": "my-cluster",
            "CurrentVersion": "K2PWKAKR8XB7XF",
            "EncryptionInfo": {
                "EncryptionAtRest": {
                    "DataVolumeKMSKeyId": "arn:aws:kms:us-east-1:123456789012:key/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
                },
                "EncryptionInTransit": {
                    "ClientBroker": "TLS",
                    "InCluster": true
                }
            },
            "EnhancedMonitoring": "PER_TOPIC_PER_BROKER",
            "NumberOfBrokerNodes": 3
        }
}
```

AwsNetworkFirewall recursos en ASFF

Los siguientes son ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para `AwsNetworkFirewall` los recursos.

AWS Security Hub CSPM normaliza los hallazgos de varias fuentes en el ASFF. Para obtener información general sobre el ASFF, consulte AWS Formato de búsqueda de seguridad (ASFF).

AwsNetworkFirewallFirewall

El objeto `AwsNetworkFirewallFirewall` contiene detalles acerca de un firewall AWS Network Firewall .

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsNetworkFirewallFirewall` objeto. Para ver las descripciones de los atributos `AwsNetworkFirewallFirewall`, consulte AwsNetworkFirewallFirewallDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsNetworkFirewallFirewall": {
    "DeleteProtection": false,
    "FirewallArn": "arn:aws:network-firewall:us-east-1:024665936331:firewall/
testfirewall",
    "FirewallPolicyArn": "arn:aws:network-firewall:us-east-1:444455556666:firewall-
policy/InitialFirewall",
```

```
    "FirewallId": "dea7d8e9-ae38-4a8a-b022-672a830a99fa",
    "FirewallName": "testfirewall",
    "FirewallPolicyChangeProtection": false,
    "SubnetChangeProtection": false,
    "SubnetMappings": [
        {
            "SubnetId": "subnet-0183481095e588cdc"
        },
        {
            "SubnetId": "subnet-01f518fad1b1c90b0"
        }
    ],
    "VpcId": "vpc-40e83c38"
}
```

AwsNetworkFirewallFirewallPolicy

El objeto `AwsNetworkFirewallFirewallPolicy` proporciona detalles sobre una política de firewall. Una política de firewall define el comportamiento de un firewall de red.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsNetworkFirewallFirewallPolicy` objeto. Para ver las descripciones de los atributos `AwsNetworkFirewallFirewallPolicy`, consulte AwsNetworkFirewallFirewallPolicyDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsNetworkFirewallFirewallPolicy": {
   "FirewallPolicy": {
    "StatefulRuleGroupReferences": [
        {
            "ResourceArn": "arn:aws:network-firewall:us-east-1:444455556666:stateful-
rulegroup/PatchesOnly"
        }
    ],
    "StatelessDefaultActions": [ "aws:forward_to_sfe" ],
    "StatelessFragmentDefaultActions": [ "aws:forward_to_sfe" ],
    "StatelessRuleGroupReferences": [
       {
          "Priority": 1,
          "ResourceArn": "arn:aws:network-firewall:us-east-1:444455556666:stateless-
rulegroup/Stateless-1"
       }
```

```
      ]
    },
    "FirewallPolicyArn": "arn:aws:network-firewall:us-east-1:444455556666:firewall-
policy/InitialFirewall",
    "FirewallPolicyId": "9ceeda22-6050-4048-a0ca-50ce47f0cc65",
    "FirewallPolicyName": "InitialFirewall",
    "Description": "Initial firewall"
}
```

AwsNetworkFirewallRuleGroup

El objeto `AwsNetworkFirewallRuleGroup` proporciona detalles sobre un grupo de reglas AWS Network Firewall . Los grupos de reglas se utilizan para inspeccionar y controlar el tráfico de red. Los grupos de reglas sin estado se aplican a paquetes individuales. Los grupos de reglas con estado se aplican a los paquetes en el contexto de su flujo de tráfico.

En las políticas de firewall se hace referencia a los grupos de reglas.

En los siguientes ejemplos se muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsNetworkFirewallRuleGroup` objeto. Para ver las descripciones de los atributos `AwsNetworkFirewallRuleGroup`, consulte AwsNetworkFirewallRuleGroupDetails en la referencia de la API de AWS Security Hub .

Ejemplo: grupo de reglas sin estado

```
"AwsNetworkFirewallRuleGroup": {
    "Capacity": 600,
    "RuleGroupArn": "arn:aws:network-firewall:us-east-1:444455556666:stateless-
rulegroup/Stateless-1",
    "RuleGroupId": "fb13c4df-b6da-4c1e-91ec-84b7a5487493",
    "RuleGroupName": "Stateless-1"
    "Description": "Example of a stateless rule group",
    "Type": "STATELESS",
    "RuleGroup": {
        "RulesSource": {
            "StatelessRulesAndCustomActions": {
                "CustomActions": [],
                "StatelessRules": [
                    {
                        "Priority": 1,
                        "RuleDefinition": {
                            "Actions": [
```

```
                                "aws:pass"
                            ],
                            "MatchAttributes": {
                                "DestinationPorts": [
                                    {
                                        "FromPort": 443,
                                        "ToPort": 443
                                    }
                                ],
                                "Destinations": [
                                    {
                                        "AddressDefinition": "192.0.2.0/24"
                                    }
                                ],
                                "Protocols": [
                                            6
                                ],
                                "SourcePorts": [
                                    {
                                        "FromPort": 0,
                                        "ToPort": 65535
                                    }
                                ],
                                "Sources": [
                                    {
                                         "AddressDefinition": "198.51.100.0/24"
                                    }
                                ]
                            }
                        }
                    }
                ]
            }
        }
    }
}
```

Ejemplo: grupo de reglas con estado

```
"AwsNetworkFirewallRuleGroup": {
    "Capacity": 100,
    "RuleGroupArn": "arn:aws:network-firewall:us-east-1:444455556666:stateful-
rulegroup/tupletest",
```

```
    "RuleGroupId": "38b71c12-da80-4643-a6c5-03337f8933e0",
    "RuleGroupName": "ExampleRuleGroup",
    "Description": "Example of a stateful rule group",
    "Type": "STATEFUL",
    "RuleGroup": {
        "RuleSource": {
             "StatefulRules": [
                 {
                     "Action": "PASS",
                     "Header": {
                         "Destination": "Any",
                         "DestinationPort": "443",
                         "Direction": "ANY",
                         "Protocol": "TCP",
                         "Source": "Any",
                         "SourcePort": "Any"
                     },
                     "RuleOptions": [
                         {
                            "Keyword": "sid:1"
                         }
                     ]
                 }
             ]
         }
    }
}
```

La siguiente es una lista de ejemplos de valores válidos para los atributos `AwsNetworkFirewallRuleGroup`:

- `Action`

  Valores válidos: `PASS` | `DROP` | `ALERT`
- `Protocol`

  Valores válidos: `IP` | `TCP` | `UDP` | `ICMP` | `HTTP` | `FTP` | `TLS` | `SMB` | `DNS` | `DCERPC` | `SSH` | `SMTP` | `IMAP` | `MSN` | `KRB5` | `IKEV2` | `TFTP` | `NTP` | `DHCP`
- `Flags`

  Valores válidos: `FIN` | `SYN` | `RST` | `PSH` | `ACK` | `URG` | `ECE` | `CWR`
- `Masks`

Valores válidos: `FIN` | `SYN` | `RST` | `PSH` | `ACK` | `URG` | `ECE` | `CWR`

AwsOpenSearchService recursos en ASFF

Los siguientes son ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para `AwsOpenSearchService` los recursos.

AWS Security Hub CSPM normaliza los hallazgos de varias fuentes en el ASFF. Para obtener información general sobre el ASFF, consulte AWS Formato de búsqueda de seguridad (ASFF).

AwsOpenSearchServiceDomain

El `AwsOpenSearchServiceDomain` objeto contiene información sobre un dominio de Amazon OpenSearch Service.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsOpenSearchServiceDomain` objeto. Para ver las descripciones de los atributos `AwsOpenSearchServiceDomain`, consulte AwsOpenSearchServiceDomainDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsOpenSearchServiceDomain": {
    "AccessPolicies": "IAM_Id",
    "AdvancedSecurityOptions": {
        "Enabled": true,
        "InternalUserDatabaseEnabled": true,
        "MasterUserOptions": {
            "MasterUserArn": "arn:aws:iam::123456789012:user/third-master-use",
            "MasterUserName": "third-master-use",
            "MasterUserPassword": "some-password"
        }
    },
    "Arn": "arn:aws:Opensearch:us-east-1:111122223333:somedomain",
    "ClusterConfig": {
        "InstanceType": "c5.large.search",
        "InstanceCount": 1,
        "DedicatedMasterEnabled": true,
        "ZoneAwarenessEnabled": false,
        "ZoneAwarenessConfig": {
            "AvailabilityZoneCount": 2
        },
```

```
        "DedicatedMasterType": "c5.large.search",
        "DedicatedMasterCount": 3,
        "WarmEnabled": true,
        "WarmCount": 3,
        "WarmType": "ultrawarm1.large.search"
    },
    "DomainEndpoint": "https://es-2021-06-23t17-04-qowmgghud5vofgb5e4wmi.eu-
central-1.es.amazonaws.com",
    "DomainEndpointOptions": {
        "EnforceHTTPS": false,
        "TLSSecurityPolicy": "Policy-Min-TLS-1-0-2019-07",
        "CustomEndpointCertificateArn": "arn:aws:acm:us-
east-1:111122223333:certificate/bda1bff1-79c0-49d0-abe6-50a15a7477d4",
        "CustomEndpointEnabled": true,
        "CustomEndpoint": "example.com"
    },
    "DomainEndpoints": {
        "vpc": "vpc-endpoint-h2dsd34efgyghrtguk5gt6j2foh4.us-east-1.es.amazonaws.com"
    },
    "DomainName": "my-domain",
    "EncryptionAtRestOptions": {
        "Enabled": false,
        "KmsKeyId": "1a2a3a4-1a2a-3a4a-5a6a-1a2a3a4a5a6a"
    },
    "EngineVersion": "7.1",
    "Id": "123456789012",
    "LogPublishingOptions": {
        "IndexSlowLogs": {
            "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:111122223333:log-
group:/aws/aes/domains/es-index-slow-logs",
            "Enabled": true
        },
        "SearchSlowLogs": {
            "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:111122223333:log-
group:/aws/aes/domains/es-slow-logs",
            "Enabled": true
        },
        "AuditLogs": {
            "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:111122223333:log-
group:/aws/aes/domains/es-slow-logs",
            "Enabled": true
        }
    },
    "NodeToNodeEncryptionOptions": {
```

```
        "Enabled": true
    },
    "ServiceSoftwareOptions": {
        "AutomatedUpdateDate": "2022-04-28T14:08:37.000Z",
        "Cancellable": false,
        "CurrentVersion": "R20210331",
        "Description": "There is no software update available for this domain.",
        "NewVersion": "OpenSearch_1.0",
        "UpdateAvailable": false,
        "UpdateStatus": "COMPLETED",
        "OptionalDeployment": false
    },
    "VpcOptions": {
        "SecurityGroupIds": [
            "sg-2a3a4a5a"
        ],
        "SubnetIds": [
            "subnet-1a2a3a4a"
        ],
    }
}
```

AwsRds recursos en ASFF

Los siguientes son ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para los `AwsRds` recursos.

AWS Security Hub CSPM normaliza los hallazgos de varias fuentes en el ASFF. Para obtener información general sobre el ASFF, consulte AWS Formato de búsqueda de seguridad (ASFF).

AwsRdsDbCluster

El objeto `AwsRdsDbCluster` proporciona detalles sobre un clúster de base de datos de Amazon RDS.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsRdsDbCluster` objeto. Para ver las descripciones de los atributos `AwsRdsDbCluster`, consulte AwsRdsDbClusterDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsRdsDbCluster": {
    "ActivityStreamStatus": "stopped",
```

```
    "AllocatedStorage": 1,
    "AssociatedRoles": [
        {
        "RoleArn": "arn:aws:iam::777788889999:role/aws-service-role/rds.amazonaws.com/
AWSServiceRoleForRDS",
        "Status": "PENDING"
        }
    ],
    "AutoMinorVersionUpgrade": true,
    "AvailabilityZones": [
        "us-east-1a",
        "us-east-1c",
        "us-east-1e"
    ],
    "BackupRetentionPeriod": 1,
    "ClusterCreateTime": "2020-06-22T17:40:12.322Z",
    "CopyTagsToSnapshot": true,
    "CrossAccountClone": false,
    "CustomEndpoints": [],
    "DatabaseName": "Sample name",
    "DbClusterIdentifier": "database-3",
    "DbClusterMembers": [
        {
        "DbClusterParameterGroupStatus": "in-sync",
        "DbInstanceIdentifier": "database-3-instance-1",
        "IsClusterWriter": true,
        "PromotionTier": 1,
        }
    ],
    "DbClusterOptionGroupMemberships": [],
    "DbClusterParameterGroup": "cluster-parameter-group",
    "DbClusterResourceId": "cluster-example",
    "DbSubnetGroup": "subnet-group",
    "DeletionProtection": false,
    "DomainMemberships": [],
    "Status": "modifying",
    "EnabledCloudwatchLogsExports": [
        "audit",
        "error",
        "general",
        "slowquery"
    ],
    "Endpoint": "database-3.cluster-example.us-east-1.rds.amazonaws.com",
    "Engine": "aurora-mysql",
```

```
    "EngineMode": "provisioned",
    "EngineVersion": "5.7.mysql_aurora.2.03.4",
    "HostedZoneId": "ZONE1",
    "HttpEndpointEnabled": false,
    "IamDatabaseAuthenticationEnabled": false,
    "KmsKeyId": "arn:aws:kms:us-east-1:777788889999:key/key1",
    "MasterUsername": "admin",
    "MultiAz": false,
    "Port": 3306,
    "PreferredBackupWindow": "04:52-05:22",
    "PreferredMaintenanceWindow": "sun:09:32-sun:10:02",
    "ReaderEndpoint": "database-3.cluster-ro-example.us-east-1.rds.amazonaws.com",
    "ReadReplicaIdentifiers": [],
    "Status": "Modifying",
    "StorageEncrypted": true,
    "VpcSecurityGroups": [
        {
            "Status": "active",
            "VpcSecurityGroupId": "sg-example-1"
        }
    ],
}
```

AwsRdsDbClusterSnapshot

El objeto `AwsRdsDbClusterSnapshot` contiene información acerca de una instantánea de clúster de base de datos de Amazon RDS.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsRdsDbClusterSnapshot` objeto. Para ver las descripciones de los atributos `AwsRdsDbClusterSnapshot`, consulte AwsRdsDbClusterSnapshotDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsRdsDbClusterSnapshot": {
    "AllocatedStorage": 0,
    "AvailabilityZones": [
        "us-east-1a",
        "us-east-1d",
        "us-east-1e"
    ],
    "ClusterCreateTime": "2020-06-12T13:23:15.577Z",
```

```
    "DbClusterIdentifier": "database-2",
    "DbClusterSnapshotAttributes": [{
        "AttributeName": "restore",
        "AttributeValues": ["123456789012"]
    }],
    "DbClusterSnapshotIdentifier": "rds:database-2-2020-06-23-03-52",
    "Engine": "aurora",
    "EngineVersion": "5.6.10a",
    "IamDatabaseAuthenticationEnabled": false,
    "KmsKeyId": "arn:aws:kms:us-east-1:777788889999:key/key1",
    "LicenseModel": "aurora",
    "MasterUsername": "admin",
    "PercentProgress": 100,
    "Port": 0,
    "SnapshotCreateTime": "2020-06-22T17:40:12.322Z",
    "SnapshotType": "automated",
    "Status": "available",
    "StorageEncrypted": true,
    "VpcId": "vpc-faf7e380"
}
```

AwsRdsDbInstance

El objeto `AwsRdsDbInstance` proporciona detalles sobre una instancia de base de datos de RDS de Amazon.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsRdsDbInstance` objeto. Para ver las descripciones de los atributos `AwsRdsDbInstance`, consulte AwsRdsDbInstanceDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsRdsDbInstance": {
    "AllocatedStorage": 20,
    "AssociatedRoles": [],
    "AutoMinorVersionUpgrade": true,
    "AvailabilityZone": "us-east-1d",
    "BackupRetentionPeriod": 7,
    "CaCertificateIdentifier": "certificate1",
    "CharacterSetName": "",
    "CopyTagsToSnapshot": true,
    "DbClusterIdentifier": "",
    "DbInstanceArn": "arn:aws:rds:us-east-1:111122223333:db:database-1",
```

```
    "DbInstanceClass": "db.t2.micro",
    "DbInstanceIdentifier": "database-1",
    "DbInstancePort": 0,
    "DbInstanceStatus": "available",
    "DbiResourceId": "db-EXAMPLE123",
    "DbName": "",
    "DbParameterGroups": [
        {
            "DbParameterGroupName": "default.mysql5.7",
            "ParameterApplyStatus": "in-sync"
        }
    ],
    "DbSecurityGroups": [],


    "DbSubnetGroup": {
        "DbSubnetGroupName": "my-group-123abc",
        "DbSubnetGroupDescription": "My subnet group",
        "VpcId": "vpc-example1",
        "SubnetGroupStatus": "Complete",
        "Subnets": [
            {
                "SubnetIdentifier": "subnet-123abc",
                "SubnetAvailabilityZone": {
                    "Name": "us-east-1d"
                },
                "SubnetStatus": "Active"
            },
            {
                "SubnetIdentifier": "subnet-456def",
                "SubnetAvailabilityZone": {
                    "Name": "us-east-1c"
                },
                "SubnetStatus": "Active"
            }
      ],
        "DbSubnetGroupArn": ""
    },
    "DeletionProtection": false,
    "DomainMemberships": [],
    "EnabledCloudWatchLogsExports": [],
    "Endpoint": {
        "address": "database-1.example.us-east-1.rds.amazonaws.com",
        "port": 3306,
```

```
        "hostedZoneId": "ZONEID1"
    },
    "Engine": "mysql",
    "EngineVersion": "5.7.22",
    "EnhancedMonitoringResourceArn": "arn:aws:logs:us-east-1:111122223333:log-
group:Example:log-stream:db-EXAMPLE1",
    "IamDatabaseAuthenticationEnabled": false,
    "InstanceCreateTime": "2020-06-22T17:40:12.322Z",
    "Iops": "",
    "KmsKeyId": "",
    "LatestRestorableTime": "2020-06-24T05:50:00.000Z",
    "LicenseModel": "general-public-license",
    "ListenerEndpoint": "",
    "MasterUsername": "admin",
    "MaxAllocatedStorage": 1000,
    "MonitoringInterval": 60,
    "MonitoringRoleArn": "arn:aws:iam::111122223333:role/rds-monitoring-role",
    "MultiAz": false,
    "OptionGroupMemberships": [
        {
            "OptionGroupName": "default:mysql-5-7",
            "Status": "in-sync"
        }
    ],
    "PreferredBackupWindow": "03:57-04:27",
    "PreferredMaintenanceWindow": "thu:10:13-thu:10:43",
    "PendingModifiedValues": {
        "DbInstanceClass": "",
        "AllocatedStorage": "",
        "MasterUserPassword": "",
        "Port": "",
        "BackupRetentionPeriod": "",
        "MultiAZ": "",
        "EngineVersion": "",
        "LicenseModel": "",
        "Iops": "",
        "DbInstanceIdentifier": "",
        "StorageType": "",
        "CaCertificateIdentifier": "",
        "DbSubnetGroupName": "",
        "PendingCloudWatchLogsExports": "",
        "ProcessorFeatures": []
    },
    "PerformanceInsightsEnabled": false,
```

```
    "PerformanceInsightsKmsKeyId": "",
    "PerformanceInsightsRetentionPeriod": "",
    "ProcessorFeatures": [],
    "PromotionTier": "",
    "PubliclyAccessible": false,
    "ReadReplicaDBClusterIdentifiers": [],
    "ReadReplicaDBInstanceIdentifiers": [],
    "ReadReplicaSourceDBInstanceIdentifier": "",
    "SecondaryAvailabilityZone": "",
    "StatusInfos": [],
    "StorageEncrypted": false,
    "StorageType": "gp2",
    "TdeCredentialArn": "",
    "Timezone": "",
    "VpcSecurityGroups": [
        {
            "VpcSecurityGroupId": "sg-example1",
            "Status": "active"
        }
    ]
}
```

AwsRdsDbSecurityGroup

El objeto `AwsRdsDbSecurityGroup` contiene información sobre Amazon Relational Database Service (RDS).

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsRdsDbSecurityGroup` objeto. Para ver las descripciones de los atributos `AwsRdsDbSecurityGroup`, consulte AwsRdsDbSecurityGroupDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsRdsDbSecurityGroup": {
    "DbSecurityGroupArn": "arn:aws:rds:us-west-1:111122223333:secgrp:default",
    "DbSecurityGroupDescription": "default",
    "DbSecurityGroupName": "mysecgroup",
    "Ec2SecurityGroups": [
        {
          "Ec2SecurityGroupuId": "myec2group",
          "Ec2SecurityGroupName": "default",
```

```
          "Ec2SecurityGroupOwnerId": "987654321021",
          "Status": "authorizing"
        }
    ],
    "IpRanges": [
        {
          "Cidrip": "0.0.0.0/0",
          "Status": "authorizing"
        }
    ],
    "OwnerId": "123456789012",
    "VpcId": "vpc-1234567f"
}
```

AwsRdsDbSnapshot

El objeto `AwsRdsDbSnapshot` contiene detalles acerca de una instantánea de clúster de base de datos de Amazon RDS.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsRdsDbSnapshot` objeto. Para ver las descripciones de los atributos `AwsRdsDbSnapshot`, consulte AwsRdsDbSnapshotDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsRdsDbSnapshot": {
    "DbSnapshotIdentifier": "rds:database-1-2020-06-22-17-41",
    "DbInstanceIdentifier": "database-1",
    "SnapshotCreateTime": "2020-06-22T17:41:29.967Z",
    "Engine": "mysql",
    "AllocatedStorage": 20,
    "Status": "available",
    "Port": 3306,
    "AvailabilityZone": "us-east-1d",
    "VpcId": "vpc-example1",
    "InstanceCreateTime": "2020-06-22T17:40:12.322Z",
    "MasterUsername": "admin",
    "EngineVersion": "5.7.22",
    "LicenseModel": "general-public-license",
    "SnapshotType": "automated",
    "Iops": null,
    "OptionGroupName": "default:mysql-5-7",
    "PercentProgress": 100,
```

```
    "SourceRegion": null,
    "SourceDbSnapshotIdentifier": "",
    "StorageType": "gp2",
    "TdeCredentialArn": "",
    "Encrypted": false,
    "KmsKeyId": "",
    "Timezone": "",
    "IamDatabaseAuthenticationEnabled": false,
    "ProcessorFeatures": [],
    "DbiResourceId": "db-resourceexample1"
}
```

AwsRdsEventSubscription

`AwsRdsEventSubscription` contiene detalles sobre una suscripción de notificación de eventos de RDS. La suscripción permite a RDS publicar eventos en un tema de SNS.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsRdsEventSubscription` objeto. Para ver las descripciones de los atributos `AwsRdsEventSubscription`, consulte AwsRdsEventSubscriptionDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsRdsEventSubscription": {
    "CustSubscriptionId": "myawsuser-secgrp",
    "CustomerAwsId": "111111111111",
    "Enabled": true,
    "EventCategoriesList": [
        "configuration change",
        "failure"
    ],
    "EventSubscriptionArn": "arn:aws:rds:us-east-1:111111111111:es:my-instance-events",
    "SnsTopicArn": "arn:aws:sns:us-east-1:111111111111:myawsuser-RDS",
    "SourceIdsList": [
        "si-sample",
        "mysqldb-rr"
    ],
    "SourceType": "db-security-group",
    "Status": "creating",
    "SubscriptionCreationTime": "2021-06-27T01:38:01.090Z"
}
```

AwsRedshift recursos en ASFF

Los siguientes son ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para los `AwsRedshift` recursos.

AWS Security Hub CSPM normaliza los hallazgos de varias fuentes en el ASFF. Para obtener información general sobre el ASFF, consulte AWS Formato de búsqueda de seguridad (ASFF).

AwsRedshiftCluster

El objeto `AwsRedshiftCluster` contiene detalles sobre un clúster de Amazon Redshift.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsRedshiftCluster` objeto. Para ver las descripciones de los atributos `AwsRedshiftCluster`, consulte AwsRedshiftClusterDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsRedshiftCluster": {
    "AllowVersionUpgrade": true,
    "AutomatedSnapshotRetentionPeriod": 1,
    "AvailabilityZone": "us-west-2d",
    "ClusterAvailabilityStatus": "Unavailable",
    "ClusterCreateTime": "2020-08-03T19:22:44.637Z",
    "ClusterIdentifier": "redshift-cluster-1",
    "ClusterNodes": [
        {
            "NodeRole": "LEADER",
            "PrivateIPAddress": "192.0.2.108",
            "PublicIPAddress": "198.51.100.29"
        },
        {
            "NodeRole": "COMPUTE-0",
            "PrivateIPAddress": "192.0.2.22",
            "PublicIPAddress": "198.51.100.63"
        },
        {
             "NodeRole": "COMPUTE-1",
             "PrivateIPAddress": "192.0.2.224",
             "PublicIPAddress": "198.51.100.226"
        }
        ],
    "ClusterParameterGroups": [
        {
```

```
            "ClusterParameterStatusList": [
                {
                    "ParameterName": "max_concurrency_scaling_clusters",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "enable_user_activity_logging",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "auto_analyze",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "query_group",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "datestyle",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "extra_float_digits",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "search_path",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "statement_timeout",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "wlm_json_configuration",
                    "ParameterApplyStatus": "in-sync",
```

```
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "require_ssl",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "use_fips_ssl",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                }
            ],
            "ParameterApplyStatus": "in-sync",
            "ParameterGroupName": "temp"
        }
    ],
    "ClusterPublicKey": "JalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY Amazon-Redshift",
    "ClusterRevisionNumber": 17498,
    "ClusterSecurityGroups": [
        {
            "ClusterSecurityGroupName": "default",
            "Status": "active"
        }
    ],
    "ClusterSnapshotCopyStatus": {
        "DestinationRegion": "us-west-2",
        "ManualSnapshotRetentionPeriod": -1,
        "RetentionPeriod": 1,
        "SnapshotCopyGrantName": "snapshotCopyGrantName"
    },
    "ClusterStatus": "available",
    "ClusterSubnetGroupName": "default",
    "ClusterVersion": "1.0",
    "DBName": "dev",
    "DeferredMaintenanceWindows": [
        {
            "DeferMaintenanceEndTime": "2020-10-07T20:34:01.000Z",
            "DeferMaintenanceIdentifier": "deferMaintenanceIdentifier",
            "DeferMaintenanceStartTime": "2020-09-07T20:34:01.000Z"
        }
     ],
    "ElasticIpStatus": {
        "ElasticIp": "203.0.113.29",
```

```
        "Status": "active"
    },
    "ElasticResizeNumberOfNodeOptions": "4",
    "Encrypted": false,
    "Endpoint": {
        "Address": "redshift-cluster-1.example.us-west-2.redshift.amazonaws.com",
        "Port": 5439
    },
    "EnhancedVpcRouting": false,
    "ExpectedNextSnapshotScheduleTime": "2020-10-13T20:34:01.000Z",
    "ExpectedNextSnapshotScheduleTimeStatus": "OnTrack",
    "HsmStatus": {
        "HsmClientCertificateIdentifier": "hsmClientCertificateIdentifier",
        "HsmConfigurationIdentifier": "hsmConfigurationIdentifier",
        "Status": "applying"
    },
    "IamRoles": [
        {
             "ApplyStatus": "in-sync",
             "IamRoleArn": "arn:aws:iam::111122223333:role/RedshiftCopyUnload"
        }
    ],
    "KmsKeyId": "kmsKeyId",
    "LoggingStatus": {
        "BucketName": "amzn-s3-demo-bucket",
        "LastFailureMessage": "test message",
        "LastFailureTime": "2020-08-09T13:00:00.000Z",
        "LastSuccessfulDeliveryTime": "2020-08-08T13:00:00.000Z",
        "LoggingEnabled": true,
        "S3KeyPrefix": "/"
    },
    "MaintenanceTrackName": "current",
    "ManualSnapshotRetentionPeriod": -1,
    "MasterUsername": "awsuser",
    "NextMaintenanceWindowStartTime": "2020-08-09T13:00:00.000Z",
    "NodeType": "dc2.large",
    "NumberOfNodes": 2,
    "PendingActions": [],
    "PendingModifiedValues": {
        "AutomatedSnapshotRetentionPeriod": 0,
        "ClusterIdentifier": "clusterIdentifier",
        "ClusterType": "clusterType",
        "ClusterVersion": "clusterVersion",
        "EncryptionType": "None",
```

```
        "EnhancedVpcRouting": false,
        "MaintenanceTrackName": "maintenanceTrackName",
        "MasterUserPassword": "masterUserPassword",
        "NodeType": "dc2.large",
        "NumberOfNodes": 1,
        "PubliclyAccessible": true
    },
    "PreferredMaintenanceWindow": "sun:13:00-sun:13:30",
    "PubliclyAccessible": true,
    "ResizeInfo": {
        "AllowCancelResize": true,
        "ResizeType": "ClassicResize"
    },
    "RestoreStatus": {
        "CurrentRestoreRateInMegaBytesPerSecond": 15,
        "ElapsedTimeInSeconds": 120,
        "EstimatedTimeToCompletionInSeconds": 100,
        "ProgressInMegaBytes": 10,
        "SnapshotSizeInMegaBytes": 1500,
        "Status": "restoring"
    },
    "SnapshotScheduleIdentifier": "snapshotScheduleIdentifier",
    "SnapshotScheduleState": "ACTIVE",
     "VpcId": "vpc-example",
    "VpcSecurityGroups": [
        {
            "Status": "active",
            "VpcSecurityGroupId": "sg-example"
        }
    ]
}
```

AwsRoute53 recursos en ASFF

Los siguientes son ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para `AwsRoute53` los recursos.

AWS Security Hub CSPM normaliza los hallazgos de varias fuentes en el ASFF. Para obtener información general sobre el ASFF, consulte AWS Formato de búsqueda de seguridad (ASFF).

AwsRoute53HostedZone

El objeto `AwsRoute53HostedZone` proporciona información acerca de una zona alojada de Amazon Route 53, incluidos los cuatro servidores de nombres asignados a la zona alojada. Una zona alojada representa un conjunto de registros que se pueden administrar juntos y que pertenecen a un único nombre de dominio principal.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsRoute53HostedZone` objeto. Para ver las descripciones de los atributos `AwsRoute53HostedZone`, consulte AwsRoute53HostedZoneDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsRoute53HostedZone": {
    "HostedZone": {
        "Id": "Z06419652JEMGO9TA2XKL",
        "Name": "asff.testing",
        "Config": {
            "Comment": "This is an example comment."
        }
    },
    "NameServers": [
        "ns-470.awsdns-32.net",
        "ns-1220.awsdns-12.org",
        "ns-205.awsdns-13.com",
        "ns-1960.awsdns-51.co.uk"
    ],
    "QueryLoggingConfig": {
        "CloudWatchLogsLogGroupArn": {
            "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:123456789012:log-
group:asfftesting:*",
            "Id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "HostedZoneId": "Z00932193AF5H180PPNZD"
        }
    },
    "Vpcs": [
        {
            "Id": "vpc-05d7c6e36bc03ea76",
            "Region": "us-east-1"
        }
    ]
```

```
}
```

Ass3 recursos en ASFF

Los siguientes son ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para `AwsS3` los recursos.

AWS Security Hub CSPM normaliza los hallazgos de varias fuentes en el ASFF. Para obtener información general sobre el ASFF, consulte AWS Formato de búsqueda de seguridad (ASFF).

AwsS3AccessPoint

`AwsS3AccessPoint` proporciona información acerca de un punto de acceso de Amazon S3. Los puntos de acceso de S3 son puntos de conexión de red con nombre que están asociados a los buckets que se pueden utilizar para llevar a cabo operaciones con objetos de S3.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsS3AccessPoint` objeto. Para ver las descripciones de los atributos `AwsS3AccessPoint`, consulte AwsS3AccessPointDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsS3AccessPoint": {
        "AccessPointArn": "arn:aws:s3:us-east-1:123456789012:accesspoint/asff-access-
point",
        "Alias": "asff-access-point-hrzrlukc5m36ft7okagglf3gmwluquse1b-s3alias",
        "Bucket": "amzn-s3-demo-bucket",
        "BucketAccountId": "123456789012",
        "Name": "asff-access-point",
        "NetworkOrigin": "VPC",
        "PublicAccessBlockConfiguration": {
            "BlockPublicAcls": true,
            "BlockPublicPolicy": true,
            "IgnorePublicAcls": true,
            "RestrictPublicBuckets": true
        },
        "VpcConfiguration": {
            "VpcId": "vpc-1a2b3c4d5e6f1a2b3"
        }
}
```

AwsS3AccountPublicAccessBlock

`AwsS3AccountPublicAccessBlock` proporciona información sobre la configuración del bloque de acceso público de Amazon S3 para las cuentas.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsS3AccountPublicAccessBlock` objeto. Para ver las descripciones de los atributos `AwsS3AccountPublicAccessBlock`, consulte AwsS3AccountPublicAccessBlockDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsS3AccountPublicAccessBlock": {
    "BlockPublicAcls": true,
    "BlockPublicPolicy": true,
    "IgnorePublicAcls": false,
    "RestrictPublicBuckets": true
}
```

AwsS3Bucket

El objeto `AwsS3Bucket` proporciona información detallada sobre un bucket de Amazon S3.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsS3Bucket` objeto. Para ver las descripciones de los atributos `AwsS3Bucket`, consulte AwsS3BucketDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsS3Bucket": {
    "AccessControlList": "{\"grantSet\":null,\"grantList\":[{\"grantee\":{\"id\":
\"4df55416215956920d9d056aa8b99803a294ea221222bb668b55a8c6bca81094\",\"displayName
\":null},\"permission\":\"FullControl\"},{\"grantee\":\"AllUsers\",\"permission\":
\"ReadAcp\"},{\"grantee\":\"AuthenticatedUsers\",\"permission\":\"ReadAcp\"}",,
    "BucketLifecycleConfiguration": {
       "Rules": [
           {
               "AbortIncompleteMultipartUpload": {
                   "DaysAfterInitiation": 5
               },
               "ExpirationDate": "2021-11-10T00:00:00.000Z",
               "ExpirationInDays": 365,
               "ExpiredObjectDeleteMarker": false,
```

```
                "Filter": {
                    "Predicate": {
                        "Operands": [
                            {
                                "Prefix": "tmp/",
                                "Type": "LifecyclePrefixPredicate"
                            },
                            {
                                "Tag": {
                                    "Key": "ArchiveAge",
                                    "Value": "9m"
                                },
                                "Type": "LifecycleTagPredicate"
                            }
                        ],
                        "Type": "LifecycleAndOperator"
                    }
                },
                "ID": "Move rotated logs to Glacier",
                "NoncurrentVersionExpirationInDays": -1,
                "NoncurrentVersionTransitions": [
                    {
                        "Days": 2,
                        "StorageClass": "GLACIER"
                    }
                ],
                "Prefix": "rotated/",
                "Status": "Enabled",
                "Transitions": [
                    {
                        "Date": "2020-11-10T00:00:00.000Z",
                        "Days": 100,
                        "StorageClass": "GLACIER"
                    }
                ]
            }
        ]
    },
    "BucketLoggingConfiguration": {
     "DestinationBucketName": "s3serversideloggingbucket-123456789012",
     "LogFilePrefix": "buckettestreadwrite23435/"
    },
    "BucketName": "amzn-s3-demo-bucket",
    "BucketNotificationConfiguration": {
```

```
      "Configurations": [{
       "Destination": "arn:aws:lambda:us-east-1:123456789012:function:s3_public_write",
       "Events": [
        "s3:ObjectCreated:Put"
       ],
       "Filter": {
        "S3KeyFilter": {
         "FilterRules": [
         {
          "Name": "AffS3BucketNotificationConfigurationS3KeyFilterRuleName.PREFIX",
          "Value": "pre"
         },
         {
          "Name": "AffS3BucketNotificationConfigurationS3KeyFilterRuleName.SUFFIX",
          "Value": "suf"
         },
         ]
        }
       },
       "Type": "LambdaConfiguration"
      }]
     },
     "BucketVersioningConfiguration": {
      "IsMfaDeleteEnabled": true,
      "Status": "Off"
     },
     "BucketWebsiteConfiguration": {
      "ErrorDocument": "error.html",
      "IndexDocumentSuffix": "index.html",
      "RedirectAllRequestsTo": {
       "HostName": "example.com",
       "Protocol": "http"
      },
      "RoutingRules": [{
       "Condition": {
        "HttpErrorCodeReturnedEquals": "Redirected",
        "KeyPrefixEquals": "index"
          },
       "Redirect": {
        "HostName": "example.com",
        "HttpRedirectCode": "401",
        "Protocol": "HTTP",
        "ReplaceKeyPrefixWith": "string",
        "ReplaceKeyWith": "string"
```

```
      }
     }]
    },
    "CreatedAt": "2007-11-30T01:46:56.000Z",
    "ObjectLockConfiguration": {
     "ObjectLockEnabled": "Enabled",
     "Rule": {
      "DefaultRetention": {
       "Days": null,
       "Mode": "GOVERNANCE",
       "Years": 12
      },
     },
    },
    "OwnerId": "AIDACKCEVSQ6C2EXAMPLE",
    "OwnerName": "s3bucketowner",
    "PublicAccessBlockConfiguration": {
        "BlockPublicAcls": true,
        "BlockPublicPolicy": true,
        "IgnorePublicAcls": true,
        "RestrictPublicBuckets": true,
    },
    "ServerSideEncryptionConfiguration": {
        "Rules": [
            {
                "ApplyServerSideEncryptionByDefault": {
                    "SSEAlgorithm": "AES256",
                    "KMSMasterKeyID": "12345678-abcd-abcd-abcd-123456789012"
                }
            }
        ]
     }
}
```

Un objeto WSS3

El objeto `AwsS3Object` proporciona información sobre un objeto de Amazon S3.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsS3Object` objeto. Para ver las descripciones de los atributos `AwsS3Object`, consulte AwsS3ObjectDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsS3Object": {
    "ContentType": "text/html",
    "ETag": "\"30a6ec7e1a9ad79c203d05a589c8b400\"",
    "LastModified": "2012-04-23T18:25:43.511Z",
    "ServerSideEncryption": "aws:kms",
    "SSEKMSKeyId": "arn:aws:kms:us-west-2:123456789012:key/4dff8393-e225-4793-
a9a0-608ec069e5a7",
    "VersionId": "ws31OurgOOjH_HHllIxPE35P.MELYaYh"
}
```

AwsSageMaker recursos en ASFF

Los siguientes son ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para `AwsSageMaker` los recursos.

AWS Security Hub CSPM normaliza los hallazgos de varias fuentes en el ASFF. Para obtener información general sobre el ASFF, consulte AWS Formato de búsqueda de seguridad (ASFF).

AwsSageMakerNotebookInstance

El `AwsSageMakerNotebookInstance` objeto proporciona información sobre una instancia de cuaderno de Amazon SageMaker AI, que es una instancia informática de aprendizaje automático que ejecuta la aplicación Jupyter Notebook.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del objeto. `AwsSageMakerNotebookInstance` Para ver las descripciones de los atributos `AwsSageMakerNotebookInstance`, consulte AwsSageMakerNotebookInstanceDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsSageMakerNotebookInstance": {
    "DirectInternetAccess": "Disabled",
    "InstanceMetadataServiceConfiguration": {
     "MinimumInstanceMetadataServiceVersion": "1",
    },
    "InstanceType": "ml.t2.medium",
    "LastModifiedTime": "2022-09-09 22:48:32.012000+00:00",
    "NetworkInterfaceId": "eni-06c09ac2541a1bed3",
    "NotebookInstanceArn": "arn:aws:sagemaker:us-east-1:001098605940:notebook-instance/
sagemakernotebookinstancerootaccessdisabledcomplia-8myjcyofzixm",
```

```
    "NotebookInstanceName":
 "SagemakerNotebookInstanceRootAccessDisabledComplia-8MYjcyofZiXm",
    "NotebookInstanceStatus": "InService",
    "PlatformIdentifier": "notebook-al1-v1",
    "RoleArn": "arn:aws:iam::001098605940:role/sechub-SageMaker-1-scenar-
SageMakerCustomExecution-1R0X32HGC38IW",
    "RootAccess": "Disabled",
    "SecurityGroups": [
     "sg-06b347359ab068745"
    ],
    "SubnetId": "subnet-02c0deea5fa64578e",
    "Url":
 "sagemakernotebookinstancerootaccessdisabledcomplia-8myjcyofzixm.notebook.us-
east-1.sagemaker.aws",
    "VolumeSizeInGB": 5
}
```

AwsSecretsManager recursos en ASFF

Los siguientes son ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para `AwsSecretsManager` los recursos.

AWS Security Hub CSPM normaliza los hallazgos de varias fuentes en el ASFF. Para obtener información general sobre el ASFF, consulte AWS Formato de búsqueda de seguridad (ASFF).

AwsSecretsManagerSecret

El objeto `AwsSecretsManagerSecret` proporciona detalles sobre un secreto de Secrets Manager.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsSecretsManagerSecret` objeto. Para ver las descripciones de los atributos `AwsSecretsManagerSecret`, consulte AwsSecretsManagerSecretDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsSecretsManagerSecret": {
    "RotationRules": {
        "AutomaticallyAfterDays": 30
    },
    "RotationOccurredWithinFrequency": true,
    "KmsKeyId": "kmsKeyId",
    "RotationEnabled": true,
```

```
    "RotationLambdaArn": "arn:aws:lambda:us-
west-2:777788889999:function:MyTestRotationLambda",
    "Deleted": false,
    "Name": "MyTestDatabaseSecret",
    "Description": "My test database secret"
}
```

AwsSns recursos en ASFF

Los siguientes son ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para los `AwsSns` recursos.

AWS Security Hub CSPM normaliza los hallazgos de varias fuentes en el ASFF. Para obtener información general sobre el ASFF, consulte AWS Formato de búsqueda de seguridad (ASFF).

AwsSnsTopic

El objeto `AwsSnsTopic` contiene detalles sobre un tema de Amazon Simple Notification Service.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsSnsTopic` objeto. Para ver las descripciones de los atributos `AwsSnsTopic`, consulte AwsSnsTopicDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsSnsTopic": {
    "ApplicationSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/
ApplicationSuccessFeedbackRoleArn",
    "FirehoseFailureFeedbackRoleArn": "arn:aws:iam::123456789012:role/
FirehoseFailureFeedbackRoleArn",
    "FirehoseSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/
FirehoseSuccessFeedbackRoleArn",
    "HttpFailureFeedbackRoleArn": "arn:aws:iam::123456789012:role/
HttpFailureFeedbackRoleArn",
    "HttpSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/
HttpSuccessFeedbackRoleArn",
    "KmsMasterKeyId": "alias/ExampleAlias",
    "Owner": "123456789012",
    "SqsFailureFeedbackRoleArn": "arn:aws:iam::123456789012:role/
SqsFailureFeedbackRoleArn",
    "SqsSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/
SqsSuccessFeedbackRoleArn",
    "Subscription": {
```

```
        "Endpoint": "http://sampleendpoint.com",
        "Protocol": "http"
    },
    "TopicName": "SampleTopic"
}
```

AwsSqs recursos en ASFF

Los siguientes son ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para los `AwsSqs` recursos.

AWS Security Hub CSPM normaliza los hallazgos de varias fuentes en el ASFF. Para obtener información general sobre el ASFF, consulte AWS Formato de búsqueda de seguridad (ASFF).

AwsSqsQueue

El objeto `AwsSqsQueue` contiene información acerca de una cola de Amazon Simple Queue Service.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsSqsQueue` objeto. Para ver las descripciones de los atributos `AwsSqsQueue`, consulte AwsSqsQueueDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsSqsQueue": {
    "DeadLetterTargetArn": "arn:aws:sqs:us-west-2:123456789012:queue/target",
    "KmsDataKeyReusePeriodSeconds": 60,,
    "KmsMasterKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
    "QueueName": "sample-queue"
}
```

AwsSsm recursos en ASFF

Los siguientes son ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para los `AwsSsm` recursos.

AWS Security Hub CSPM normaliza los hallazgos de varias fuentes en el ASFF. Para obtener información general sobre el ASFF, consulte AWS Formato de búsqueda de seguridad (ASFF).

AwsSsmPatchCompliance

El objeto `AwsSsmPatchCompliance` proporciona información sobre el estado de un parche en una instancia en función de la línea de base de revisiones que se utilizó para parchear la instancia.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsSsmPatchCompliance` objeto. Para ver las descripciones de los atributos `AwsSsmPatchCompliance`, consulte AwsSsmPatchComplianceDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsSsmPatchCompliance": {
    "Patch": {
        "ComplianceSummary": {
            "ComplianceType": "Patch",
            "CompliantCriticalCount": 0,
            "CompliantHighCount": 0,
            "CompliantInformationalCount": 0,
            "CompliantLowCount": 0,
            "CompliantMediumCount": 0,
            "CompliantUnspecifiedCount": 461,
            "ExecutionType": "Command",
            "NonCompliantCriticalCount": 0,
            "NonCompliantHighCount": 0,
            "NonCompliantInformationalCount": 0,
            "NonCompliantLowCount": 0,
            "NonCompliantMediumCount": 0,
            "NonCompliantUnspecifiedCount": 0,
            "OverallSeverity": "UNSPECIFIED",
            "PatchBaselineId": "pb-0c5b2769ef7cbe587",
            "PatchGroup": "ExamplePatchGroup",
            "Status": "COMPLIANT"
        }
    }
}
```

AwsStepFunctions recursos en ASFF

Los siguientes son ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para `AwsStepFunctions` los recursos.

AWS Security Hub CSPM normaliza los hallazgos de varias fuentes en el ASFF. Para obtener información general sobre el ASFF, consulte AWS Formato de búsqueda de seguridad (ASFF).

AwsStepFunctionStateMachine

El objeto `AwsStepFunctionStateMachine` proporciona información sobre una máquina de estados de AWS Step Functions , que es un flujo de trabajo que consta de una serie de pasos basados en eventos.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsStepFunctionStateMachine` objeto. Para ver las descripciones de los atributos `AwsStepFunctionStateMachine`, consulte AwsStepFunctionStateMachine en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsStepFunctionStateMachine": {
    "StateMachineArn": "arn:aws:states:us-
east-1:123456789012:stateMachine:StepFunctionsLogDisableNonCompliantResource-
fQLujTeXvwsb",
    "Name": "StepFunctionsLogDisableNonCompliantResource-fQLujTeXvwsb",
    "Status": "ACTIVE",
    "RoleArn": "arn:aws:iam::123456789012:role/teststepfunc-
StatesExecutionRole-1PNM71RVO1UKT",
    "Type": "STANDARD",
    "LoggingConfiguration": {
        "Level": "OFF",
        "IncludeExecutionData": false
    },
    "TracingConfiguration": {
        "Enabled": false
    }
}
```

AwsWaf recursos en ASFF

Los siguientes son ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para `AwsWaf` los recursos.

AWS Security Hub CSPM normaliza los hallazgos de varias fuentes en el ASFF. Para obtener información general sobre el ASFF, consulte AWS Formato de búsqueda de seguridad (ASFF).

AwsWafRateBasedRule

El objeto `AwsWafRateBasedRule` contiene detalles sobre una regla basada en tasas de AWS WAF para los recursos globales. Una regla AWS WAF basada en tasas proporciona ajustes para

indicar cuándo permitir, bloquear o contar una solicitud. Rate-based las reglas incluyen el número de solicitudes que llegan durante un período de tiempo específico.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsWafRateBasedRule` objeto. Para ver las descripciones de los atributos `AwsWafRateBasedRule`, consulte AwsWafRateBasedRuleDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsWafRateBasedRule":{
    "MatchPredicates" : [{
        "DataId" : "391b7a7e-5f00-40d2-b114-3f27ceacbbb0",
        "Negated" : "True",
        "Type" : "IPMatch" ,
    }],
    "MetricName" : "MetricName",
    "Name" : "Test",
    "RateKey" : "IP",
    "RateLimit" : 235000,
    "RuleId" : "5dfb4085-f103-4ec6-b39a-d4a0dae5f47f"
}
```

AwsWafRegionalRateBasedRule

El objeto `AwsWafRegionalRateBasedRule` contiene detalles sobre una regla basada en tasas para los recursos Regionales. Una regla basada en tasas proporciona ajustes para indicar cuándo permitir, bloquear o contar una solicitud. Rate-based las reglas incluyen el número de solicitudes que llegan durante un período de tiempo específico.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsWafRegionalRateBasedRule` objeto. Para ver las descripciones de los atributos `AwsWafRegionalRateBasedRule`, consulte AwsWafRegionalRateBasedRuleDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsWafRegionalRateBasedRule":{
    "MatchPredicates" : [{
        "DataId" : "391b7a7e-5f00-40d2-b114-3f27ceacbbb0",
        "Negated" : "True",
        "Type" : "IPMatch" ,
```

```
    }],
    "MetricName" : "MetricName",
    "Name" : "Test",
    "RateKey" : "IP",
    "RateLimit" : 235000,
    "RuleId" : "5dfb4085-f103-4ec6-b39a-d4a0dae5f47f"
}
```

AwsWafRegionalRule

El `AwsWafRegionalRule` objeto proporciona detalles sobre una regla AWS WAF regional. Esta regla identifica las solicitudes web que desea permitir, bloquear o contar.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsWafRegionalRule` objeto. Para ver las descripciones de los atributos `AwsWafRegionalRule`, consulte AwsWafRegionalRuleDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsWafRegionalRule": {
    "MetricName": "SampleWAF_Rule__Metric_1",
    "Name": "bb-waf-regional-rule-not-empty-conditions-compliant",
    "RuleId": "8f651760-24fa-40a6-a9ed-4b60f1de95fe",
    "PredicateList": [{
        "DataId": "127d9346-e607-4e93-9286-c1296fb5445a",
        "Negated": false,
        "Type": "GeoMatch"
    }]
}
```

AwsWafRegionalRuleGroup

El objeto `AwsWafRegionalRuleGroup` proporciona detalles sobre un grupo de reglas Regionales de AWS WAF . Un grupo de reglas es una colección de reglas predefinidas que agrega a una lista de control de acceso web (ACL web).

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsWafRegionalRuleGroup` objeto. Para ver las descripciones de los atributos `AwsWafRegionalRuleGroup`, consulte AwsWafRegionalRuleGroupDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsWafRegionalRuleGroup": {
    "MetricName": "SampleWAF_Metric_1",
    "Name": "bb-WAFClassicRuleGroupWithRuleCompliant",
    "RuleGroupId": "2012ca6d-e66d-4d9b-b766-bfb03ad77cfb",
    "Rules": [{
        "Action": {
            "Type": "ALLOW"
        }
    }],
        "Priority": 1,
        "RuleId": "cdd225da-32cf-4773-8dc5-3bca3ed9c19c",
        "Type": "REGULAR"
}
```

AwsWafRegionalWebAcl

`AwsWafRegionalWebAcl`proporciona detalles sobre una lista AWS WAF regional de control de acceso web (ACL web). Una ACL web contiene las reglas que identifican las solicitudes que desea permitir, bloquear o contar.

A continuación, se muestra un ejemplo de resultado de `AwsWafRegionalWebAcl` en Formato de resultados de seguridad de AWS (ASFF). Para ver las descripciones de los atributos `AwsApiGatewayV2Stage`, consulte AwsWafRegionalWebAclDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsWafRegionalWebAcl": {
    "DefaultAction": "ALLOW",
    "MetricName" : "web-regional-webacl-metric-1",
    "Name": "WebACL_123",
    "RulesList": [
        {
            "Action": {
                "Type": "Block"
            },
            "Priority": 3,
            "RuleId": "24445857-852b-4d47-bd9c-61f05e4d223c",
            "Type": "REGULAR",
            "ExcludedRules": [
                {
```

```
                    "ExclusionType": "Exclusion",
                    "RuleId": "Rule_id_1"
                }
            ],
            "OverrideAction": {
                "Type": "OVERRIDE"
            }
        }
    ],
    "WebAclId": "443c76f4-2e72-4c89-a2ee-389d501c1f67"
}
```

AwsWafRule

`AwsWafRule`proporciona información acerca de una AWS WAF regla. Una AWS WAF regla identifica las solicitudes web que desea permitir, bloquear o contar.

El siguiente es un ejemplo de `AwsWafRule` búsqueda en el formato AWS de búsqueda de seguridad (ASFF). Para ver las descripciones de los atributos `AwsApiGatewayV2Stage`, consulte AwsWafRuleDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsWafRule": {
    "MetricName": "AwsWafRule_Metric_1",
    "Name": "AwsWafRule_Name_1",
    "PredicateList": [{
        "DataId": "cdd225da-32cf-4773-1dc2-3bca3ed9c19c",
        "Negated": false,
        "Type": "GeoMatch"
    }],
    "RuleId": "8f651760-24fa-40a6-a9ed-4b60f1de953e"
}
```

AwsWafRuleGroup

`AwsWafRuleGroup`proporciona información sobre un grupo de AWS WAF reglas. Un grupo de reglas de AWS WAF es un conjunto de reglas predefinidas que agrega a una lista de control de acceso web (ACL web).

A continuación se muestra un ejemplo de `AwsWafRuleGroup` búsqueda en el formato AWS de búsqueda de seguridad (ASFF). Para ver las descripciones de los atributos

`AwsApiGatewayV2Stage`, consulte AwsWafRuleGroupDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsWafRuleGroup": {
    "MetricName": "SampleWAF_Metric_1",
    "Name": "bb-WAFRuleGroupWithRuleCompliant",
    "RuleGroupId": "2012ca6d-e66d-4d9b-b766-bfb03ad77cfb",
    "Rules": [{
        "Action": {
            "Type": "ALLOW",
        },
        "Priority": 1,
        "RuleId": "cdd225da-32cf-4773-8dc5-3bca3ed9c19c",
        "Type": "REGULAR"
    }]
}
```

AwsWafv2RuleGroup

El `AwsWafv2RuleGroup` objeto proporciona detalles sobre un grupo de reglas AWS WAF V2.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsWafv2RuleGroup` objeto. Para ver las descripciones de los atributos `AwsWafv2RuleGroup`, consulte AwsWafv2RuleGroupDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsWafv2RuleGroup": {
    "Arn": "arn:aws:wafv2:us-east-1:123456789012:global/rulegroup/wafv2rulegroupasff/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Capacity": 1000,
    "Description": "Resource for ASFF",
    "Id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Name": "wafv2rulegroupasff",
    "Rules": [{
     "Action": {
     "Allow": {
      "CustomRequestHandling": {
       "InsertHeaders": [
        {
        "Name": "AllowActionHeader1Name",
```

```
        "Value": "AllowActionHeader1Value"
        },
        {
        "Name": "AllowActionHeader2Name",
        "Value": "AllowActionHeader2Value"
        }
       ]
      }
     },
     "Name": "RuleOne",
     "Priority": 1,
     "VisibilityConfig": {
      "CloudWatchMetricsEnabled": true,
      "MetricName": "rulegroupasff",
      "SampledRequestsEnabled": false
     }
    }],
    "VisibilityConfig": {
     "CloudWatchMetricsEnabled": true,
     "MetricName": "rulegroupasff",
     "SampledRequestsEnabled": false
    }
}
```

AwsWafWebAcl

El `AwsWafWebAcl` objeto proporciona detalles sobre una ACL AWS WAF web.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsWafWebAcl` objeto. Para ver las descripciones de los atributos `AwsWafWebAcl`, consulte AwsWafWebAclDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsWafWebAcl": {
    "DefaultAction": "ALLOW",
    "Name": "MyWafAcl",
    "Rules": [
        {
            "Action": {
                "Type": "ALLOW"
            },
            "ExcludedRules": [
```

```
                {
                    "RuleId": "5432a230-0113-5b83-bbb2-89375c5bfa98"
                }
            ],
            "OverrideAction": {
                "Type": "NONE"
            },
            "Priority": 1,
            "RuleId": "5432a230-0113-5b83-bbb2-89375c5bfa98",
            "Type": "REGULAR"
        }
    ],
    "WebAclId": "waf-1234567890"
}
```

AwsWafv2WebAcl

El `AwsWafv2WebAcl` objeto proporciona detalles sobre una ACL web AWS WAF V2.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsWafv2WebAcl` objeto. Para ver las descripciones de los atributos `AwsWafv2WebAcl`, consulte AwsWafv2WebAclDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsWafv2WebAcl": {
    "Arn": "arn:aws:wafv2:us-east-1:123456789012:regional/webacl/WebACL-RoaD4QexqSxG/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Capacity": 1326,
    "CaptchaConfig": {
     "ImmunityTimeProperty": {
      "ImmunityTime": 500
     }
    },
    "DefaultAction": {
     "Block": {}
    },
    "Description": "Web ACL for JsonBody testing",
    "ManagedbyFirewallManager": false,
    "Name": "WebACL-RoaD4QexqSxG",
    "Rules": [{
     "Action": {
      "RuleAction": {
```

```
        "Block": {}
       }
      },
      "Name": "TestJsonBodyRule",
      "Priority": 1,
      "VisibilityConfig": {
       "SampledRequestsEnabled": true,
       "CloudWatchMetricsEnabled": true,
       "MetricName": "JsonBodyMatchMetric"
      }
     }],
     "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "TestingJsonBodyMetric"
     }
}
```

AwsXray recursos en ASFF

Los siguientes son ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para `AwsXray` los recursos.

AWS Security Hub CSPM normaliza los hallazgos de varias fuentes en el ASFF. Para obtener información general sobre el ASFF, consulte AWS Formato de búsqueda de seguridad (ASFF).

AwsXrayEncryptionConfig

El `AwsXrayEncryptionConfig` objeto contiene información sobre la configuración de cifrado de AWS X-Ray.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsXrayEncryptionConfig` objeto. Para ver las descripciones de los atributos `AwsXrayEncryptionConfig`, consulte AwsXrayEncryptionConfigDetails en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsXRayEncryptionConfig":{
    "KeyId": "arn:aws:kms:us-east-2:222222222222:key/example-key",
    "Status": "UPDATING",
    "Type":"KMS"
}
```

CodeRepository objeto en ASFF

El `CodeRepository` objeto proporciona información sobre un repositorio de código externo al que usted conectó a AWS los recursos y configuró Amazon Inspector para detectar vulnerabilidades.

El siguiente ejemplo muestra la sintaxis del formato de búsqueda de AWS seguridad (ASFF) del `CodeRepository` objeto. Para ver las descripciones de los atributos `CodeRepository`, consulte CodeRepositoryDetails en la referencia de la API de AWS Security Hub . Para obtener información general sobre el ASFF, consulte AWS Formato de búsqueda de seguridad (ASFF).

Ejemplo

```
"CodeRepository": {
    "ProviderType": "GITLAB_SELF_MANAGED",
    "ProjectName": "projectName",
    "CodeSecurityIntegrationArn": "arn:aws:inspector2:us-
east-1:123456789012:codesecurity-integration/00000000-0000-0000-0000-000000000000"
}
```

Container objeto en ASFF

El siguiente ejemplo muestra la sintaxis del formato de búsqueda de AWS seguridad (ASFF) del `Container` objeto. Para ver las descripciones de los atributos `Container`, consulte ContainerDetails en la referencia de la API de AWS Security Hub . Para obtener información general sobre el ASFF, consulte AWS Formato de búsqueda de seguridad (ASFF).

Ejemplo

```
"Container": {
    "ContainerRuntime": "docker",
    "ImageId": "image12",
    "ImageName": "1111111/
knotejs@sha256:372131c9fef111111111111115f4ed3ea5f9dce4dc3bd34ce21846588a3",
    "LaunchedAt": "2018-09-29T01:25:54Z",
    "Name": "knote",
    "Privileged": true,
    "VolumeMounts": [{
        "Name": "vol-03909e9",
        "MountPath": "/mnt/etc"
    }]
}
```

Otro objeto en ASFF

En el formato AWS de búsqueda de seguridad (ASFF), el `Other` objeto especifica campos y valores personalizados. Para obtener más información acerca del ASFF, consulte AWS Formato de búsqueda de seguridad (ASFF).

Al usar el objeto `Other`, puede especificar campos personalizados y valores para un recurso. Puede usar el objeto `Other` en los siguientes casos:

- El tipo de recurso no tiene el objeto `Details` correspondiente. Para especificar detalles de un recurso, utilice el objeto `Other`.
- El objeto `Details` para el tipo de recurso no incluye todos los atributos que desea especificar. En este caso, utilice el objeto `Details` correspondiente al tipo de recurso para especificar los atributos disponibles. Use el objeto `Other` para especificar los atributos que no están en el objeto `Details` correspondiente al tipo.
- El tipo de recurso no es uno de los tipos proporcionados. En este caso, establezca `Resource.Type` en `Other` y utilice el objeto `Other` para especificar los detalles.

Tipo: mapa de hasta 50 pares clave-valor

Cada par clave-valor debe cumplir los siguientes requisitos.

- La clave debe tener menos de 128 caracteres.
- El valor debe tener menos de 1024 caracteres.

Visualización de productos de información en el CSPM de Security Hub

En AWS Security Hub CSPM, una visión es una colección de hallazgos relacionados. La información puede identificar un área de seguridad específica que requiera atención e intervención. Por ejemplo, una información podría señalar las instancias EC2 que son objeto de resultados que detectan prácticas de seguridad deficientes. Una información reúne los resultados de todos los proveedores de resultados.

Cada información se define mediante una instrucción GROUP BY y filtros opcionales. La instrucción GROUP BY indica cómo agrupar los resultados coincidentes e identifica el tipo de elemento al que se aplica la información. Por ejemplo, si una información se agrupa por identificador de recurso,

la información genera una lista de identificadores de recursos. Los filtros opcionales reducen los resultados coincidentes para la información. Por ejemplo, es posible que solo desee ver resultados de proveedores específicos o resultados que estén relacionados con tipos específicos de recursos.

El CSPM de Security Hub ofrece varios productos de información administrados integrados. No puede modificar ni eliminar la información administrada. Para realizar un seguimiento de los problemas de seguridad que son exclusivos de su AWS entorno y uso, puede crear información personalizada.

La página Información de la consola CSPM de AWS Security Hub muestra la lista de información disponible.

De forma predeterminada, la lista muestra tanto los hallazgos gestionados como los personalizados. Para filtrar la lista de información en función del tipo de hallazgos, elija el tipo en el menú desplegable que se encuentra junto al campo de filtro.

- Para mostrar todos los hallazgos disponibles, seleccione Todos los hallazgos. Esta es la opción predeterminada.
- Para mostrar solo los productos de información administrados, elija Productos de información administrados del CSPM de Security Hub.
- Para mostrar solo información personalizada, elija Hallazgos personalizados.

También puede filtrar la lista de información en función del nombre de cada una. Para hacerlo, en el campo de filtro, escriba el texto que se utilizará para filtrar la lista. El filtro no distingue entre mayúsculas y minúsculas. El filtro busca hallazgos que contengan el texto en cualquier parte del nombre.

Una información solo devuelve resultados si ha habilitado integraciones o estándares que produzcan resultados coincidentes. Por ejemplo, la información administrada 29. Principales recursos por número de comprobaciones CIS no superadas solo devuelve resultados si habilita una versión del estándar del Indicador de referencia de AWS de Center for Internet Security (CIS).

Revisión de productos de información y medidas al respecto en el CSPM de Security Hub

Para cada información, AWS Security Hub CSPM determina primero las conclusiones que coinciden con los criterios del filtro y, a continuación, utiliza el atributo de agrupación para agrupar las conclusiones coincidentes.

Desde la página Información en la consola puede ver y tomar medidas sobre los resultados y los hallazgos.

Si habilita la agregación entre regiones, los resultados de la información administrada (cuando haya iniciado sesión en la región de agregación) incluirán los resultados de la región de agregación y de las regiones vinculadas. Los resultados de la información personalizada, si la información no se filtra por región, también incluyen los resultados de la región de agregación y las regiones vinculadas (cuando haya iniciado sesión en la región de agregación). En otras regiones, los resultados de la información son solo para esa región.

Para obtener más información acerca de la configuración de agregación entre regiones, consulte the section called “Agregar datos en las regiones”.

Visualización y adopción de medidas sobre los resultados de la información

Los resultados del conocimiento constan de una lista agrupada de los resultados del conocimiento. Por ejemplo, si la información se agrupa por identificadores de recursos, los resultados de la información son la lista de identificadores del recurso. Cada elemento de la lista de resultados indica el número de hallazgos coincidentes para ese elemento.

Si los resultados se agrupan por identificador de recurso o tipo de recurso, los resultados incluyen todos los recursos de los hallazgos correspondientes. Esto incluye los recursos que tienen un tipo diferente del tipo de recurso especificado en los criterios del filtro. Por ejemplo, un hallazgo identifica los resultados asociados a los buckets de S3. Si un resultado coincidente contiene un bucket de S3 y una clave de acceso de IAM, los resultados de información incluyen ambos recursos.

En la consola del CSPM de Security Hub, la lista de resultados se ordena desde los que presentan mayor coincidencia hasta los de menor coincidencia. El CSPM de Security Hub solo puede mostrar 100 hallazgos. Si hay más de 100 valores de agrupamiento, solo verá los primeros 100.

Además de la lista de resultados, los resultados de conocimientos muestran un conjunto de gráficos que resume el número de hallazgos coincidentes para los siguientes atributos.

- Etiqueta de gravedad: número de resultados para cada etiqueta de gravedad
- Cuenta de AWS ID: los cinco identificadores de cuenta principales para los resultados coincidentes
- Tipo de recurso: los cinco tipos de recursos principales para los resultados correspondientes
- ID de recurso: los cinco principales ID de recursos para los resultados correspondientes
- Nombre del producto: los cinco principales proveedores de hallazgos para los resultados correspondientes

Si ha configurado acciones personalizadas, puede enviar los resultados seleccionados a una acción personalizada. La acción debe estar asociada a una CloudWatch regla de Amazon para el tipo de `Security Hub Insight Results` evento. Para obtener más información, consulte the section called "Respuesta y corrección automatizadas". Si no ha configurado acciones personalizadas, el menú Acciones está desactivado.

Security Hub CSPM console

Para visualizar y adoptar medidas sobre los resultados de la información (consola)

1. Abra la consola CSPM de AWS Security Hub en. https://console.aws.amazon.com/securityhub/
2. En el panel de navegación, elija Insights.
3. Para mostrar la lista de resultados de conocimientos, elija el nombre del conocimiento.
4. Seleccione la casilla de verificación de cada resultado que desee enviar a la acción personalizada.
5. En el menú Actions (Acciones), elija la acción personalizada.

Security Hub CSPM API, AWS CLI

Para ver los resultados de la información y tomar medidas al respecto (API,) AWS CLI

Para ver los resultados de producto de información, utilice la operación >GetInsightResults de la API del CSPM de Security Hub. Si usas el AWS CLI, ejecuta el get-insight-results comando.

Para identificar la información para la que obtener resultados, necesita el ARN de la información. Para obtener los ARN de información personalizada, utilice la operación `GetInsights` de la API o el comando get-insight-results.

En el siguiente ejemplo, se recuperan los resultados de la información especificada. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$ aws securityhub get-insight-results --insight-arn "arn:aws:securityhub:us-
west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
```

Para obtener información acerca de cómo crear acciones personalizadas mediante programación, consulte Uso de acciones personalizadas para enviar hallazgos e información a EventBridge.

Para visualizar y tomar medidas sobre los hallazgos en los resultados de la información (consola)

Desde una lista de hallazgos de un producto de información en la consola del CSPM de Security Hub, puede mostrar la lista de resultados para cada hallazgo.

Para visualizar y tomar medidas sobre los resultados de la información (consola)

1. Abra la consola CSPM de AWS Security Hub en. https://console.aws.amazon.com/securityhub/
2. En el panel de navegación, elija Insights.
3. Para mostrar la lista de resultados de conocimientos, elija el nombre del conocimiento.
4. Para mostrar la lista de hallazgos de un resultado de conocimiento, elija el elemento de la lista de resultados. La lista de hallazgos muestra los hallazgos activos del resultado de conocimiento seleccionado que tienen un estado de flujo de trabajo `NEW` o `NOTIFIED`.

En la lista de resultados puede realizar las siguientes acciones:

- Filtrado de resultados en el CSPM de Security Hub
- Revisión de los detalles y el historial de resultados
- Configuración del estado del flujo de trabajo de los resultados en el CSPM de Security Hub
- Envío de resultados a una acción personalizada del CSPM de Security Hub

Productos de información administrados en el CSPM de Security Hub

AWSSecurity Hub CSPM proporciona varios conocimientos gestionados.

Los productos de información administrados del CSPM de Security Hub no se pueden modificar ni eliminar. Puede ver y tomar medidas sobre los resultados y hallazgos de conocimientos. También puede utilizar conocimientos administrados como base para una nuevo conocimiento personalizado.

Al igual que con todos los conocimientos, un conocimiento administrado solo devuelve resultados si ha habilitado integraciones de productos o estándares de seguridad que pueden producir hallazgos coincidentes.

En el caso de los hallazgos agrupados en base al identificador de recursos, los resultados incluyen los identificadores de todos los recursos en los elementos que coinciden con los parámetros. Aquí se incluyen los recursos que poseen un tipo diferente al tipo de recurso que se indica en los criterios del

filtro. Por ejemplo, el hallazgo 2 en la siguiente lista identifica los resultados asociados a los buckets de Amazon S3. Si un resultado coincidente contiene un bucket de S3 y una clave de acceso de IAM, los resultados de información incluyen ambos recursos.

En este momento, el CSPM de Security Hub ofrece los siguientes productos de información administrados:

1. AWSrecursos con la mayoría de los hallazgos

   ARN: `arn:aws:securityhub:::insight/securityhub/default/1`

   Agrupados por: identificador de recursos

   Filtros de resultados:

   - El estado de registro es `ACTIVE`
   - El estado de flujo de trabajo es `NEW` o `NOTIFIED`
2. Buckets de S3 con permisos de lectura o escritura públicos

   ARN: `arn:aws:securityhub:::insight/securityhub/default/10`

   Agrupados por: identificador de recursos

   Filtros de resultados:

   - El tipo comienza con `Effects/Data Exposure`
   - El tipo de recurso es `AwsS3Bucket`
   - El estado de registro es `ACTIVE`
   - El estado de flujo de trabajo es `NEW` o `NOTIFIED`
3. AMI que está generando la mayor cantidad de resultados

   ARN: `arn:aws:securityhub:::insight/securityhub/default/3`

   Agrupados por: ID de imagen de instancia EC2

   Filtros de resultados:

   - El tipo de recurso es `AwsEc2Instance`
   - El estado de registro es `ACTIVE`
   - El estado de flujo de trabajo es `NEW` o `NOTIFIED`

4. Instancias EC2 implicadas en Tácticas, técnicas y procedimientos (TTP) conocidos

   ARN: `arn:aws:securityhub:::insight/securityhub/default/14`

   Agrupados por: ID de recurso

   Filtros de resultados:

   - El tipo comienza con `TTPs`
   - El tipo de recurso es `AwsEc2Instance`
   - El estado de registro es `ACTIVE`
   - El estado de flujo de trabajo es `NEW` o `NOTIFIED`

5. AWSdirectores con actividad sospechosa en las claves de acceso

   ARN: `arn:aws:securityhub:::insight/securityhub/default/9`

   Agrupados por: nombre de entidad principal de la clave de acceso de IAM

   Filtros de resultados:

   - El tipo de recurso es `AwsIamAccessKey`
   - El estado de registro es `ACTIVE`
   - El estado de flujo de trabajo es `NEW` o `NOTIFIED`

6. AWSinstancias de recursos que no cumplen con los estándares o las mejores prácticas de seguridad

   ARN: `arn:aws:securityhub:::insight/securityhub/default/6`

   Agrupados por: ID de recurso

   Filtros de resultados:

   - El tipo es `Software and Configuration Checks/Industry and Regulatory Standards/AWSSecurity Best Practices`
   - El estado de registro es `ACTIVE`
   - El estado de flujo de trabajo es `NEW` o `NOTIFIED`

7. AWSrecursos asociados a la posible exfiltración de datos

   ARN: `arn:aws:securityhub:::insight/securityhub/default/7`

   Agrupados por: ID de recurso

Filtros de resultados:

- El tipo comienza con Exfiltración/ Effects/Data
- El estado de registro es `ACTIVE`
- El estado de flujo de trabajo es `NEW` o `NOTIFIED`

8. AWSrecursos asociados al consumo no autorizado de recursos

   ARN: `arn:aws:securityhub:::insight/securityhub/default/8`

   Agrupados por: ID de recurso

   Filtros de resultados:

   - El tipo comienza con `Effects/Resource Consumption`
   - El estado de registro es `ACTIVE`
   - El estado de flujo de trabajo es `NEW` o `NOTIFIED`

9. Buckets de S3 que no cumplen los estándares o las prácticas recomendadas de seguridad

   ARN: `arn:aws:securityhub:::insight/securityhub/default/11`

   Agrupados por: ID de recurso

   Filtros de resultados:

   - El tipo de recurso es `AwsS3Bucket`
   - El tipo es `Software and Configuration Checks/Industry and Regulatory Standards/AWSSecurity Best Practices`
   - El estado de registro es `ACTIVE`
   - El estado de flujo de trabajo es `NEW` o `NOTIFIED`

10. Buckets de S3 con información confidencial

    ARN: `arn:aws:securityhub:::insight/securityhub/default/12`

    Agrupados por: ID de recurso

    Filtros de resultados:

    - El tipo de recurso es `AwsS3Bucket`
    - El tipo comienza con `Sensitive Data Identifications/`
    - El estado de registro es `ACTIVE`

- El estado de flujo de trabajo es `NEW` o `NOTIFIED`

11. Credenciales que podrían haberse filtrado

    ARN: `arn:aws:securityhub:::insight/securityhub/default/13`

    Agrupados por: ID de recurso

    Filtros de resultados:

    - El tipo comienza con `Sensitive Data Identifications/Passwords/`
    - El estado de registro es `ACTIVE`
    - El estado de flujo de trabajo es `NEW` o `NOTIFIED`

12. Instancias EC2 a las que les faltan parches de seguridad para importantes vulnerabilidades

    ARN: `arn:aws:securityhub:::insight/securityhub/default/16`

    Agrupados por: ID de recurso

    Filtros de resultados:

    - El tipo comienza con `Software and Configuration Checks/Vulnerabilities/CVE`
    - El tipo de recurso es `AwsEc2Instance`
    - El estado de registro es `ACTIVE`
    - El estado de flujo de trabajo es `NEW` o `NOTIFIED`

13. Instancias EC2 con comportamiento inusual en general

    ARN: `arn:aws:securityhub:::insight/securityhub/default/17`

    Agrupados por: ID de recurso

    Filtros de resultados:

    - El tipo comienza con `Unusual Behaviors`
    - El tipo de recurso es `AwsEc2Instance`
    - El estado de registro es `ACTIVE`
    - El estado de flujo de trabajo es `NEW` o `NOTIFIED`

14. Instancias EC2 que tienen puertos accesibles desde Internet

    ARN: `arn:aws:securityhub:::insight/securityhub/default/18`

Agrupados por: ID de recurso

Filtros de resultados:

- El tipo comienza con `Software and Configuration Checks/AWS Security Best Practices/Network Reachability`
- El tipo de recurso es `AwsEc2Instance`
- El estado de registro es `ACTIVE`
- El estado de flujo de trabajo es `NEW` o `NOTIFIED`

15. Instancias EC2 que no cumplen los estándares o las prácticas recomendadas de seguridad

    ARN: `arn:aws:securityhub:::insight/securityhub/default/19`

    Agrupados por: ID de recurso

    Filtros de resultados:

    - El tipo comienza con una de las siguientes opciones:
      - `Software and Configuration Checks/Industry and Regulatory Standards/`
      - `Software and Configuration Checks/AWSSecurity Best Practices`
    - El tipo de recurso es `AwsEc2Instance`
    - El estado de registro es `ACTIVE`
    - El estado de flujo de trabajo es `NEW` o `NOTIFIED`

16. Instancias EC2 que están abiertas a Internet

    ARN: `arn:aws:securityhub:::insight/securityhub/default/21`

    Agrupados por: ID de recurso

    Filtros de resultados:

    - El tipo comienza con `Software and Configuration Checks/AWS Security Best Practices/Network Reachability`
    - El tipo de recurso es `AwsEc2Instance`
    - El estado de registro es `ACTIVE`
    - El estado de flujo de trabajo es `NEW` o `NOTIFIED`

17. Instancias EC2 asociadas con reconocimiento de adversarios

    ARN: `arn:aws:securityhub:::insight/securityhub/default/22`

Agrupados por: ID de recurso

Filtros de resultados:

- El tipo comienza con TTPs/Discovery/Recon
- El tipo de recurso es `AwsEc2Instance`
- El estado de registro es `ACTIVE`
- El estado de flujo de trabajo es `NEW` o `NOTIFIED`

18. AWSrecursos asociados al malware

    ARN: `arn:aws:securityhub:::insight/securityhub/default/23`

    Agrupados por: ID de recurso

    Filtros de resultados:

    - El tipo comienza con una de las siguientes opciones:
      - `Effects/Data Exfiltration/Trojan`
      - `TTPs/Initial Access/Trojan`
      - `TTPs/Command and Control/Backdoor`
      - `TTPs/Command and Control/Trojan`
      - `Software and Configuration Checks/Backdoor`
      - `Unusual Behaviors/VM/Backdoor`
    - El estado de registro es `ACTIVE`
    - El estado de flujo de trabajo es `NEW` o `NOTIFIED`

19. AWSrecursos asociados a problemas de criptomonedas

    ARN: `arn:aws:securityhub:::insight/securityhub/default/24`

    Agrupados por: ID de recurso

    Filtros de resultados:

    - El tipo comienza con una de las siguientes opciones:
      - `Effects/Resource Consumption/Cryptocurrency`
      - `TTPs/Command and Control/CryptoCurrency`
    - El estado de registro es `ACTIVE`
    - El estado de flujo de trabajo es `NEW` o `NOTIFIED`

20. AWSrecursos con intentos de acceso no autorizados

    ARN: `arn:aws:securityhub:::insight/securityhub/default/25`

    Agrupados por: ID de recurso

    Filtros de resultados:

    - El tipo comienza con una de las siguientes opciones:
      - `TTPs/Command and Control/UnauthorizedAccess`
      - `TTPs/Initial Access/UnauthorizedAccess`
      - `Effects/Data Exfiltration/UnauthorizedAccess`
      - `Unusual Behaviors/User/UnauthorizedAccess`
      - `Effects/Resource Consumption/UnauthorizedAccess`
    - El estado de registro es `ACTIVE`
    - El estado de flujo de trabajo es `NEW` o `NOTIFIED`

21. Indicadores de información de amenazas con la mayoría de coincidencias durante la semana pasada

    ARN: `arn:aws:securityhub:::insight/securityhub/default/26`

    Filtros de resultados:

    - Creado en los últimos 7 días

22. Principales cuentas por número de hallazgos

    ARN: `arn:aws:securityhub:::insight/securityhub/default/27`

    Agrupados por: Cuenta de AWS ID

    Filtros de resultados:

    - El estado de registro es `ACTIVE`
    - El estado de flujo de trabajo es `NEW` o `NOTIFIED`

23. Principales productos por número de hallazgos

    ARN: `arn:aws:securityhub:::insight/securityhub/default/28`

    Agrupados por: Nombre del producto

    Filtros de resultados:

- El estado de registro es `ACTIVE`
- El estado de flujo de trabajo es `NEW` o `NOTIFIED`

24. Gravedad por número de hallazgos

    ARN: `arn:aws:securityhub:::insight/securityhub/default/29`

    Agrupados por: etiqueta de gravedad

    Filtros de resultados:

    - El estado de registro es `ACTIVE`
    - El estado de flujo de trabajo es `NEW` o `NOTIFIED`

25. Principales buckets de S3 por número de hallazgos

    ARN: `arn:aws:securityhub:::insight/securityhub/default/30`

    Agrupados por: ID de recurso

    Filtros de resultados:

    - El tipo de recurso es `AwsS3Bucket`
    - El estado de registro es `ACTIVE`
    - El estado de flujo de trabajo es `NEW` o `NOTIFIED`

26. Principales instancias EC2 por número de resultados

    ARN: `arn:aws:securityhub:::insight/securityhub/default/31`

    Agrupados por: ID de recurso

    Filtros de resultados:

    - El tipo de recurso es `AwsEc2Instance`
    - El estado de registro es `ACTIVE`
    - El estado de flujo de trabajo es `NEW` o `NOTIFIED`

27. Principales AMI por número de hallazgos

    ARN: `arn:aws:securityhub:::insight/securityhub/default/32`

    Agrupados por: ID de imagen de instancia EC2

    Filtros de resultados:

    - El tipo de recurso es `AwsEc2Instance`

- El estado de registro es `ACTIVE`
- El estado de flujo de trabajo es `NEW` o `NOTIFIED`

28. Principales usuarios de IAM por número de hallazgos

    ARN: `arn:aws:securityhub:::insight/securityhub/default/33`

    Agrupados por: ID de clave de acceso de IAM

    Filtros de resultados:

    - El tipo de recurso es `AwsIamAccessKey`
    - El estado de registro es `ACTIVE`
    - El estado de flujo de trabajo es `NEW` o `NOTIFIED`

29. Principales recursos por número de comprobaciones CIS no superadas

    ARN: `arn:aws:securityhub:::insight/securityhub/default/34`

    Agrupados por: ID de recurso

    Filtros de resultados:

    - El ID del generador comienza con `arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule`
    - Actualizado en el último día
    - El estado de conformidad es `FAILED`
    - El estado de registro es `ACTIVE`
    - El estado de flujo de trabajo es `NEW` o `NOTIFIED`

30. Principales integraciones por número de hallazgos

    ARN: `arn:aws:securityhub:::insight/securityhub/default/35`

    Agrupados por: ARN del producto

    Filtros de resultados:

    - El estado de registro es `ACTIVE`
    - El estado de flujo de trabajo es `NEW` o `NOTIFIED`

31. Recursos con las comprobaciones de seguridad que más fallan

    ARN: `arn:aws:securityhub:::insight/securityhub/default/36`

Agrupados por: ID de recurso

Filtros de resultados:

- Actualizado en el último día
- El estado de conformidad es `FAILED`
- El estado de registro es `ACTIVE`
- El estado de flujo de trabajo es `NEW` o `NOTIFIED`

32. Usuarios de IAM con actividad sospechosa

    ARN: `arn:aws:securityhub:::insight/securityhub/default/37`

    Agrupados por: usuario de IAM

    Filtros de resultados:

    - El tipo de recurso es `AwsIamUser`
    - El estado de registro es `ACTIVE`
    - El estado de flujo de trabajo es `NEW` o `NOTIFIED`

33. Recursos con la mayoría de los AWS Health hallazgos

    ARN: `arn:aws:securityhub:::insight/securityhub/default/38`

    Agrupados por: ID de recurso

    Filtros de resultados:

    - `ProductName` igual a `Health`

34. Recursos con la mayoría de los AWS Config hallazgos

    ARN: `arn:aws:securityhub:::insight/securityhub/default/39`

    Agrupados por: ID de recurso

    Filtros de resultados:

    - `ProductName` igual a `Config`

35. Aplicaciones con la mayor cantidad de resultados

    ARN: `arn:aws:securityhub:::insight/securityhub/default/40`

    Agrupado por: ResourceApplicationArn

Filtros de resultados:

- `RecordState` igual a `ACTIVE`
- `Workflow.Status` es igual a `NEW` o `NOTIFIED`

Descripción de resultados personalizados en el CSPM de Security Hub

Además de la información gestionada por AWS Security Hub CSPM, puede crear información personalizada en Security Hub CSPM para hacer un seguimiento de los problemas que son específicos de su entorno. Los hallazgos personalizados le permiten realizar un seguimiento de un subconjunto de problemas seleccionados.

Estos son algunos ejemplos de hallazgos personalizados que puede resultar útil configurar:

- Si tiene una cuenta de administrador, puede configurar un hallazgo personalizado para hacer un seguimiento de los resultados críticos y de alta gravedad que estén afectando a las cuentas de los miembros.
- Si confía en un AWS servicio integrado específico, puede configurar una información personalizada para hacer un seguimiento de los hallazgos críticos y de alta gravedad de ese servicio.
- Si confía en una integración de terceros, puede configurar un hallazgo personalizado para realizar un seguimiento de los hallazgos críticos y de alta gravedad de ese producto integrado.

Puede crear conocimientos personalizados completamente nuevos, o comenzar a partir de un conocimiento personalizado o administrado existente.

Cada hallazgo se puede configurar con las siguientes opciones:

- Atributo de agrupación: el atributo de agrupación determina los elementos que se muestran en la lista de resultados del hallazgo. Por ejemplo, si el atributo de agrupación es Nombre del producto, los resultados del hallazgo muestran el número de hallazgos asociados a cada proveedor.
- Filtros opcionales: Los filtros opcionales afinan la cantidad de resultados que coinciden con los parámetros del hallazgo.

  Un hallazgo se incluye en los resultados de la información solo si coincide con todos los filtros proporcionados. Por ejemplo, si los filtros dicen «El nombre del producto es GuardDuty» y `AwsS3Bucket` «El tipo de recurso es», los resultados coincidentes deben cumplir ambos criterios.

Sin embargo, el CSPM de Security Hub aplica la lógica booleana OR a los filtros que utilizan el mismo atributo, pero valores distintos. Por ejemplo, si los filtros son «El nombre del producto es GuardDuty» y «El nombre del producto es Amazon Inspector», la búsqueda coincide si la ha generado Amazon GuardDuty o Amazon Inspector.

Si utiliza el identificador de recurso o el tipo de recurso como atributo de agrupación, los resultados de la información incluirán todos los recursos incluidos en los resultados. La lista no se limita a los recursos que coinciden con un filtro de tipo de recurso. Por ejemplo, un hallazgo identifica los resultados asociados a los buckets de S3 y los agrupa por identificador de recursos. Un resultado coincidente contiene un recurso de bucket de S3 y un recurso de clave de acceso de IAM. Los resultados del hallazgo incluyen ambos recursos.

Si habilitó la agregación entre regiones y, luego, crea un hallazgo personalizado, el hallazgo se aplica a los resultados que coinciden con la región de agregación y las regiones vinculadas. La única excepción es que su información incluya un filtro de región.

Creación de hallazgos personalizados

En AWS Security Hub CSPM, la información personalizada se puede utilizar para recopilar un conjunto específico de hallazgos y realizar un seguimiento de los problemas que son exclusivos de su entorno. Para obtener información general sobre hallazgos personalizados, consulte Descripción de resultados personalizados en el CSPM de Security Hub.

Elija el método que prefiera y siga los pasos para crear un producto de información personalizado en el CSPM de Security Hub.

Security Hub CSPM console

Para crear un hallazgo personalizado (consola)

1. Abra la consola AWS CSPM de Security Hub en. https://console.aws.amazon.com/securityhub/
2. En el panel de navegación, elija Hallazgos.
3. Seleccione Crear hallazgo.
4. Para seleccionar el atributo de agrupación para el conocimiento:
   a. Seleccione el cuadro de búsqueda para ver las opciones de filtro.

   b. Elija Group by (Agrupar por).
   c. Seleccione el atributo que se va a utilizar para agrupar los resultados asociados a este hallazgo.
   d. Seleccione Aplicar.
5. De manera opcional, elija los filtros adicionales que desee utilizar para este hallazgo. Para cada filtro, defina los criterios de filtro y, a continuación, elija Aplicar.
6. Seleccione Crear hallazgo.
7. Escriba un Nombre del hallazgo y elija Crear hallazgo.

Security Hub CSPM API

Para crear un hallazgo personalizado (API)

1. Para crear un producto de información personalizado, use la operación CreateInsight de la API del CSPM de Security Hub. Si usa el AWS CLI, ejecute el create-insight comando.
2. Rellene el parámetro `Name` con un nombre para su hallazgo personalizado.
3. Rellene el parámetro `Filters` para especificar qué resultados incluir en el hallazgo.
4. Rellene el parámetro `GroupByAttribute` para especificar qué atributo se utiliza para agrupar los resultados que se incluyen en el hallazgo.
5. Si lo desea, rellene el parámetro `SortCriteria` para ordenar los resultados por un campo específico.

En el siguiente ejemplo, se crea un hallazgo personalizado que incluye los resultados críticos con el tipo de recurso `AwsIamRole`. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$ aws securityhub create-insight --name "Critical role findings" --filters
 '{"ResourceType": [{ "Comparison": "EQUALS", "Value": "AwsIamRole"}],
 "SeverityLabel": [{"Comparison": "EQUALS", "Value": "CRITICAL"}]}' --group-by-
attribute "ResourceId"
```

PowerShell

Para crear una perspectiva personalizada (PowerShell)

1. Utilice el cmdlet `New-SHUBInsight`.

2. Rellene el parámetro `Name` con un nombre para su hallazgo personalizado.
3. Rellene el parámetro `Filter` para especificar qué resultados incluir en el hallazgo.
4. Rellene el parámetro `GroupByAttribute` para especificar qué atributo se utiliza para agrupar los resultados que se incluyen en el hallazgo.

Si ha habilitado la agregación entre regiones y utiliza este cmdlet desde la región de agregación, el hallazgo se aplica a los resultados de la agregación y las regiones vinculadas.

Ejemplo

```
$Filter = @{
    AwsAccountId = [Amazon.SecurityHub.Model.StringFilter]@{
        Comparison = "EQUALS"
        Value = "XXX"
    }
    ComplianceStatus = [Amazon.SecurityHub.Model.StringFilter]@{
        Comparison = "EQUALS"
        Value = 'FAILED'
    }
}
New-SHUBInsight -Filter $Filter -Name TestInsight -GroupByAttribute ResourceId
```

Creación de un nuevo hallazgo personalizado a partir de un hallazgo administrado (solo para la consola)

No puede guardar los cambios en un hallazgo administrado ni eliminarlo. Sin embargo, puede utilizar hallazgos administrados como base para una nuevo hallazgo personalizado. Esta opción está disponible únicamente en la consola del CSPM de Security Hub.

Para crear un nuevo hallazgo personalizado a partir de un hallazgo administrado (consola)

1. Abra la consola CSPM de AWS Security Hub en. https://console.aws.amazon.com/securityhub/
2. En el panel de navegación, elija Insights.
3. Elija el conocimiento administrado desde el que trabajar.
4. Edite la configuración de los hallazgos si es necesario.
   - Para cambiar el atributo utilizado para agrupar los resultados en el hallazgo:
     a. Para eliminar la agrupación existente, elija la X situada junto al ajuste Agrupar por.

b. Seleccione la barra de búsqueda.

c. Seleccione el atributo que desea utilizar para el agrupamiento.

d. Seleccione Aplicar.

- Para eliminar un filtro del hallazgo, elija la X rodeada de un círculo junto al filtro.
- Cómo agregar un filtro al hallazgo:

  a. Seleccione la barra de búsqueda.

  b. Seleccione el atributo y el valor que desea utilizar como filtro.

  c. Seleccione Aplicar.

5. Cuando se hayan completado las actualizaciones, elija Create insight (Crear conocimiento).
6. Cuando se le solicite, escriba el Nombre del hallazgo; a continuación, elija Crear hallazgo.

Edición de hallazgos personalizados

Puede editar un hallazgo personalizado existente para cambiar el valor de agrupación y los filtros. Después de realizar los cambios, puede guardar las actualizaciones en el conocimiento original o guardar la versión actualizada como un nuevo conocimiento.

En AWS Security Hub CSPM, la información personalizada se puede utilizar para recopilar un conjunto específico de hallazgos y realizar un seguimiento de los problemas que son exclusivos de su entorno. Para obtener información general sobre hallazgos personalizados, consulte Descripción de resultados personalizados en el CSPM de Security Hub.

Para editar un hallazgo personalizado, elija el método que prefiera y siga las instrucciones.

Security Hub CSPM console

Para editar un hallazgo personalizado (consola)

1. Abra la consola AWS CSPM de Security Hub en. https://console.aws.amazon.com/securityhub/
2. En el panel de navegación, elija Insights.
3. Elija el conocimiento personalizado que desea modificar.
4. Edite la configuración de los hallazgos si es necesario.

   - Para cambiar el atributo utilizado para agrupar los resultados en el hallazgo:

     a. Para eliminar la agrupación existente, elija la X situada junto al ajuste Agrupar por.

b. Seleccione la barra de búsqueda.

c. Seleccione el atributo que desea utilizar para el agrupamiento.

d. Seleccione Aplicar.

- Para eliminar un filtro del hallazgo, elija la X rodeada de un círculo junto al filtro.
- Cómo agregar un filtro al hallazgo:

  a. Seleccione la barra de búsqueda.

  b. Seleccione el atributo y el valor que desea utilizar como filtro.

  c. Seleccione Aplicar.

5. Cuando complete las actualizaciones, elija Save insight (Guardar conocimiento).
6. Cuando se le solicite, siga uno de estos procedimientos:

   - Para actualizar la información existente para que refleje los cambios, seleccione Actualizar ***<Insight_Name>*** y, a continuación, seleccione Guardar información.
   - Para crear un nuevo conocimiento con las actualizaciones, elija Save new insight (Guardar nuevo conocimiento). Escriba un Insight name (Nombre del conocimiento) y elija Save insight (Guardar conocimiento).

Security Hub CSPM API

Para editar un hallazgo personalizado (API)

1. Use la operación `UpdateInsight` de la API del CSPM de Security Hub. Si usa el comando, AWS CLI ejecute el update-insight comando.
2. Para identificar el hallazgo personalizado que desea actualizar, debe indicar su nombre de recurso de Amazon (ARN). Para obtener el ARN de un hallazgo personalizado, ejecute la operación `GetInsights` o el comando get-insights.
3. Actualice los parámetros `Name`, `Filters` y `GroupByAttribute` según sea necesario.

En el siguiente ejemplo, se actualizan los hallazgos especificados. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$ aws securityhub update-insight --insight-arn "arn:aws:securityhub:us-
west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111" --filters '{"ResourceType": [{ "Comparison": "EQUALS", "Value":
```

```
 "AwsIamRole"}], "SeverityLabel": [{"Comparison": "EQUALS", "Value": "HIGH"}]}' --
name "High severity role findings"
```

PowerShell

Para editar una perspectiva personalizada (PowerShell)

1. Utilice el cmdlet `Update-SHUBInsight`.
2. Para identificar el hallazgo personalizado, debe indicar su nombre de recurso de Amazon (ARN). Para obtener el ARN de un hallazgo personalizado, utilice el cmdlet `Get-SHUBInsight`.
3. Actualice los parámetros `Name`, `Filter` y `GroupByAttribute` según sea necesario.

Ejemplo

```
$Filter = @{
    ResourceType = [Amazon.SecurityHub.Model.StringFilter]@{
        Comparison = "EQUALS"
        Value = "AwsIamRole"
    }
    SeverityLabel = [Amazon.SecurityHub.Model.StringFilter]@{
        Comparison = "EQUALS"
        Value = "HIGH"
    }
}

Update-SHUBInsight -InsightArn "arn:aws:securityhub:us-
west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111" -Filter $Filter -Name "High severity role findings"
```

Eliminación de hallazgos personalizados

En AWS Security Hub CSPM, la información personalizada se puede utilizar para recopilar un conjunto específico de hallazgos y realizar un seguimiento de los problemas que son exclusivos de su entorno. Para obtener información general sobre hallazgos personalizados, consulte Descripción de resultados personalizados en el CSPM de Security Hub.

Para eliminar un hallazgo personalizado, elija el método que prefiera y siga las instrucciones. No puede eliminar un hallazgo administrado.

Security Hub CSPM console

Para eliminar un hallazgo personalizado (consola)

1. Abra la consola AWS CSPM de Security Hub en. https://console.aws.amazon.com/securityhub/
2. En el panel de navegación, elija Insights.
3. Localice el conocimiento personalizado que desea eliminar.
4. Para obtener ese hallazgo, elija el icono de más opciones (los tres puntos en la esquina superior derecha de la tarjeta).
5. Elija Eliminar.

Security Hub CSPM API

Para eliminar un hallazgo personalizado (API)

1. Use la operación `DeleteInsight` de la API del CSPM de Security Hub. Si usa el comando, AWS CLI ejecute el delete-insight comando.
2. Para identificar el hallazgo personalizado que se va a eliminar, indique su ARN. Para obtener el ARN de un hallazgo personalizado, ejecute la operación `GetInsights` o el comando get-insights.

En el siguiente ejemplo, se elimina el hallazgo especificado. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$ aws securityhub delete-insight --insight-arn "arn:aws:securityhub:us-
west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
```

PowerShell

Para eliminar una visión personalizada (PowerShell)

1. Utilice el cmdlet `Remove-SHUBInsight`.
2. Para identificar el hallazgo personalizado, indique su ARN. Para obtener el ARN de un hallazgo personalizado, utilice el cmdlet `Get-SHUBInsight`.

Ejemplo

```
-InsightArn "arn:aws:securityhub:us-west-1:123456789012:insight/123456789012/custom/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Modificación automática de los resultados del CSPM de Security Hub y adopción de medidas al respecto

AWSSecurity Hub CSPM tiene funciones que modifican automáticamente los hallazgos y toman medidas en función de sus especificaciones.

El CSPM de Security Hub actualmente admite dos tipos de automatizaciones:

- Reglas de automatización: Actualice y suprima automáticamente los resultados casi en tiempo real en función de los criterios que defina.
- Respuesta y corrección automatizadas: cree EventBridge reglas de Amazon personalizadas que definan las acciones automáticas que se deben tomar en función de hallazgos e información específicos.

Las reglas de automatización son útiles cuando se desean actualizar automáticamente los campos de búsqueda en el formato de búsqueda AWS de seguridad (ASFF). Por ejemplo, puede utilizar una regla de automatización para actualizar el nivel de gravedad o el estado del flujo de trabajo de los resultados de una integración específica de terceros. El uso de la regla de automatización elimina la necesidad de actualizar de manera manual el nivel de gravedad o el estado del flujo de trabajo de cada resultado de este producto de terceros.

EventBridge las reglas son útiles cuando quieres tomar medidas fuera del Security Hub CSPM con respecto a hallazgos específicos o enviar hallazgos específicos a herramientas de terceros para su corrección o investigación adicional. Las reglas se pueden utilizar para activar acciones compatibles, como invocar una AWS Lambda función o notificar a un tema del Amazon Simple Notification Service (Amazon SNS) acerca de un hallazgo específico.

Las reglas de automatización entran en vigor antes de que se EventBridge apliquen. Es decir, las reglas de automatización se activan y actualizan un hallazgo EventBridge antes de recibirlo. EventBridge Las reglas se aplican entonces al hallazgo actualizado.

Al configurar automatizaciones para los controles de seguridad, recomendamos filtrar en función del ID del control en vez del título o la descripción. Aunque el CSPM de Security Hub actualiza en ocasiones los títulos y las descripciones de los controles, los ID de los controles permanecen sin cambios.

Temas

- Descripción de las reglas de automatización en el CSPM de Security Hub
- Uso EventBridge para respuesta y remediación automatizadas

Descripción de las reglas de automatización en el CSPM de Security Hub

Puede usar reglas de automatización para actualizar automáticamente los hallazgos en AWS Security Hub CSPM. A medida que se ingieren resultados, el CSPM de Security Hub puede aplicar diversas acciones de regla, como suprimir resultados, modificar su gravedad o agregar notas. Estas acciones de reglas modifican los resultados que coinciden con criterios específicos.

Algunos ejemplos de casos de uso de reglas de automatización son los siguientes:

- Elevar la gravedad de un resultado a `CRITICAL` si el ID de recurso del resultado se refiere a un recurso crítico para la empresa.
- Elevar la gravedad de un resultado de `HIGH` a `CRITICAL` si el resultado afecta a recursos en cuentas de producción específicas.
- Asignar resultados específicos que tengan una gravedad `INFORMATIONAL` un estado de flujo de trabajo `SUPPRESSED`.

Solo puede crear y administrar reglas de automatización desde una cuenta de administrador del CSPM de Security Hub.

Las reglas se aplican a los resultados tanto nuevos como actualizados. Puede crear una regla personalizada desde cero o utilizar una plantilla de regla proporcionada por el CSPM de Security Hub. Además, puede empezar con una plantilla y modificarla según sea necesario.

Definición de criterios de regla y acciones de regla

Desde una cuenta de administrador del CSPM de Security Hub, puede crear una regla de automatización mediante la definición de uno o más criterios de regla y una o más acciones de regla. Cuando un resultado coincide con los criterios definidos, el CSPM de Security Hub aplica

las acciones de la regla al resultado. Para obtener más información sobre los criterios y acciones disponibles, consulte Criterios de regla y acciones de regla disponibles.

El CSPM de Security Hub admite actualmente un máximo de 100 reglas de automatización por cada cuenta de administrador.

La cuenta de administrador del CSPM de Security Hub también puede editar, ver y eliminar reglas de automatización. Una regla se aplica a los resultados que coinciden en la cuenta de administrador y en todas las cuentas de miembro. Al proporcionar los ID de cuentas de miembro como criterios de regla, los administradores del CSPM de Security Hub también pueden utilizar reglas de automatización para actualizar o suprimir resultados en cuentas de miembro específicas.

Una regla de automatización solo se aplica en el lugar Región de AWS en el que se creó. Para aplicar una regla en varias regiones, el administrador debe crear la regla en cada región. Esto se puede hacer mediante la consola del CSPM de Security Hub, la API del CSPM de Security Hub o AWS CloudFormation. Además, puede utilizar un un script de implementación multirregión.

Criterios de regla y acciones de regla disponibles

Los siguientes campos del formato de búsqueda de AWS seguridad (ASFF) se admiten actualmente como criterios para las reglas de automatización:

Criterios de reglas	Operadores de filtro	Tipo de campo
`AwsAccountId`	`CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS`	Cadena
`AwsAccountName`	`CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS`	Cadena
`CompanyName`	`CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS`	Cadena

Criterios de reglas	Operadores de filtro	Tipo de campo
ComplianceAssociatedStandardsId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Cadena
ComplianceSecurityControlId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Cadena
ComplianceStatus	Is, Is Not	Selección: [FAILED, NOT_AVAILABLE , PASSED, WARNING]
Confidence	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	Número
CreatedAt	Start, End, DateRange	Fecha (formateada como 01/12/2022) T21:47:39.269Z
Criticality	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	Número
Description	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Cadena
FirstObservedAt	Start, End, DateRange	Fecha (formateada como 01/12/2022) T21:47:39.269Z

Criterios de reglas	Operadores de filtro	Tipo de campo
`GeneratorId`	`CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS`	Cadena
`Id`	`CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS`	Cadena
`LastObservedAt`	`Start, End, DateRange`	Fecha (formateada como 01/12/2022) T21:47:39.269Z
`NoteText`	`CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS`	Cadena
`NoteUpdatedAt`	`Start, End, DateRange`	Fecha (formateada como 01/12/2022) T21:47:39.269Z
`NoteUpdatedBy`	`CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS`	Cadena
`ProductArn`	`CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS`	Cadena
`ProductName`	`CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS`	Cadena

Criterios de reglas	Operadores de filtro	Tipo de campo
RecordState	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Cadena
RelatedFindingsId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Cadena
RelatedFindingsProductArn	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Cadena
ResourceApplicationArn	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Cadena
ResourceApplicationName	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Cadena
ResourceDetailsOther	CONTAINS, EQUALS, NOT_CONTAINS, NOT_EQUALS	Asignación
ResourceId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Cadena

Criterios de reglas	Operadores de filtro	Tipo de campo
`ResourcePartition`	`CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS`	Cadena
`ResourceRegion`	`CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS`	Cadena
`ResourceTags`	`CONTAINS, EQUALS, NOT_CONTAINS, NOT_EQUALS`	Asignación
`ResourceType`	`Is, Is Not`	Selección (consulte los recursos admitidos por ASFF)
`SeverityLabel`	`Is, Is Not`	Selección: [`CRITICAL`, `HIGH`, `MEDIUM`, `LOW`, `INFORMATIONAL`]
`SourceUrl`	`CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS`	Cadena
`Title`	`CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS`	Cadena
`Type`	`CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS`	Cadena

Criterios de reglas	Operadores de filtro	Tipo de campo
`UpdatedAt`	`Start, End, DateRange`	Fecha (formateada como 01/12/2022) T21:47:39.269Z
`UserDefinedFields`	`CONTAINS, EQUALS, NOT_CONTAINS, NOT_EQUALS`	Asignación
`VerificationState`	`CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS`	Cadena
`WorkflowStatus`	`Is, Is Not`	Selección: [`NEW`, `NOTIFIED`, `RESOLVED`, `SUPPRESSED`]

En el caso de los criterios etiquetados como campos de cadena, el uso de diferentes operadores de filtro en un mismo campo afecta a la lógica de evaluación. Para obtener más información, consulte StringFilter en la Referencia de la API del CSPM de AWS Security Hub.

Cada criterio admite una cantidad máxima de valores que se pueden utilizar para filtrar los resultados que coinciden. Para conocer los límites de cada criterio, consulte AutomationRulesFindingFilters en la Referencia de la API del CSPM de AWS Security Hub.

Actualmente se admiten los siguientes campos ASFF como acciones para las reglas de automatización:

- `Confidence`
- `Criticality`
- `Note`
- `RelatedFindings`
- `Severity`
- `Types`
- `UserDefinedFields`
- `VerificationState`

- `Workflow`

Para obtener más información sobre campos ASFF específicos, consulte Sintaxis del formato de resultado de seguridad de AWS (ASFF).

> **Tip**
>
> Si desea que el CSPM de Security Hub deje de generar resultados para un control específico, recomendamos desactivar el control en lugar de usar una regla de automatización. Cuando desactiva un control, el CSPM de Security Hub deja de ejecutar las comprobaciones de seguridad correspondientes y deja de generar resultados, por lo que no se generan cargos asociados a ese control. Le recomendamos que utilice reglas de automatización para cambiar los valores de campos ASFF específicos para los resultados que coincidan con los criterios definidos. Para obtener más información sobre cómo deshabilitar controles, consulte Desactivación de controles en el CSPM de Security Hub.

Resultados que las reglas de automatización evalúan

Una regla de automatización evalúa los resultados nuevos y actualizados que el CSPM de Security Hub genera o ingiere mediante la operación BatchImportFindings después de que cree la regla. El CSPM de Security Hub actualiza los resultados de los controles cada 12 a 24 horas, o cuando el recurso asociado cambia de estado. Para obtener más información, consulte Programación para ejecutar comprobaciones de seguridad.

Las reglas de automatización evalúan los resultados originales proporcionados por el proveedor. Los proveedores pueden aportar resultados nuevos y actualizar resultados existentes mediante la operación `BatchImportFindings` de la API del CSPM de Security Hub. Si los siguientes campos no existen en el resultado original, el CSPM de Security Hub completa automáticamente esos campos y utiliza los valores completados en la evaluación realizada por la regla de automatización.

- `AwsAccountName`
- `CompanyName`
- `ProductName`
- `Resource.Tags`
- `Workflow.Status`

Después de crear una o más reglas de automatización, estas reglas no se desencadenan si actualiza los campos del resultado mediante la operación BatchUpdateFindings. Si crea una regla de automatización y realiza una actualización `BatchUpdateFindings` que afecten al mismo campo de resultado, la última actualización establecerá el valor de ese campo. Vea el siguiente ejemplo:

1. Utilice la operación `BatchUpdateFindings` para cambiar el valor del campo `Workflow.Status` de un resultado de `NEW` a `NOTIFIED`.
2. Si llama a `GetFindings`, el campo `Workflow.Status` ahora tendrá un valor de `NOTIFIED`.
3. Se crea una regla de automatización que cambia el campo `Workflow.Status` del resultado de `NEW` a `SUPPRESSED`. (Recuerde que las reglas ignoran las actualizaciones realizadas mediante la operación `BatchUpdateFindings`).
4. El proveedor del resultado utiliza la operación `BatchImportFindings` para actualizar el resultado y cambia el valor del campo `Workflow.Status` del resultado a `NEW`.
5. Si llama a `GetFindings`, el campo `Workflow.Status` ahora tendrá un valor de `SUPPRESSED`. Esto ocurre porque se aplicó la regla de automatización y esa regla fue la última acción realizada sobre el resultado.

Cuando crea o edita una regla en la consola del CSPM de Security Hub, la consola muestra una vista preliminar de los resultados que coinciden con los criterios de la regla. Mientras que las reglas de automatización evalúan los resultados originales enviados por el proveedor del resultado, la vista preliminar de la consola refleja los resultados en su estado final tal como aparecerían en una respuesta a la operación GetFindings (es decir, después de aplicar las acciones de la regla u otras actualizaciones al resultado).

Cómo funciona el orden de las reglas

Al crear reglas de automatización, usted asigna a cada regla un orden. Esto determina el orden en el que el CSPM de Security Hub aplica las reglas de automatización y adquiere importancia cuando varias reglas se relacionan con el mismo resultado o con el mismo campo del resultado.

Cuando varias acciones de reglas se refieren al mismo resultado o campo de resultado, la regla con el valor numérico más alto de orden de reglas se aplica en último lugar y tiene el efecto definitivo.

Cuando crea una regla en la consola del CSPM de Security Hub, el CSPM de Security Hub asigna automáticamente un orden basado en el orden de creación de la regla. La regla creada más recientemente tiene el valor numérico más bajo de orden de reglas y, por lo tanto, se aplica primero. El CSPM de Security Hub aplica las reglas posteriores en orden ascendente.

Al crear una regla a través de la API CSPM de Security Hub oAWS CLI, Security Hub CSPM aplica primero la regla con el valor numérico más bajo. `RuleOrder` Luego aplica las reglas subsiguientes en orden ascendente. Si varios resultados tienen el mismo valor de `RuleOrder`, el CSPM de Security Hub aplica primero la regla con un valor anterior en el campo `UpdatedAt` (es decir, la regla editada más recientemente se aplica al final).

Puede modificar el orden de las reglas en cualquier momento.

Ejemplo de orden de reglas:

Regla A (el orden de la regla es**1**):

- Criterios de la regla A
  - `ProductName` = `Security Hub CSPM`
  - `Resources.Type` es `S3 Bucket`
  - `Compliance.Status` = `FAILED`
  - `RecordState` es `NEW`
  - `Workflow.Status` = `ACTIVE`
- Acciones de la regla A
  - Actualizar `Confidence` a `95`
  - Actualizar `Severity` a `CRITICAL`

Regla B (el orden de la regla es**2**):

- Criterios de la regla B
  - `AwsAccountId` = `123456789012`
- Acciones de la regla B
  - Actualizar `Severity` a `INFORMATIONAL`

Las acciones de la regla A se aplican primero a los resultados del CSPM de Security Hub que coinciden con los criterios de la regla A. Luego, se aplican las acciones de la regla B a los resultados del CSPM de Security Hub que coinciden con el ID de cuenta especificado. En este ejemplo, como la regla B se aplica en último lugar, el valor final de `Severity` en los resultados del ID de cuenta especificado es `INFORMATIONAL`. Según la acción de la regla A, el valor final de `Confidence` en los resultados coincidentes es `95`.

Creación de reglas de automatización

Se puede usar una regla de automatización para actualizar automáticamente los hallazgos en AWS Security Hub CSPM. Puede crear una regla de automatización personalizada desde cero o, en la consola del CSPM de Security Hub, usar una plantilla de regla previamente completada. Para obtener información general sobre cómo funcionan las reglas de automatización, consulte Descripción de las reglas de automatización en el CSPM de Security Hub.

Solo puede crear una regla de automatización a la vez. Para crear varias reglas de automatización, siga los procedimientos de la consola tantas veces como necesite o llame a la API o al comando tantas veces como necesite con los parámetros que desee.

Debe crear una regla de automatización en cada región y cuenta en que desee que la regla se aplique a los resultados.

Cuando crea una regla de automatización en la consola del CSPM de Security Hub, el CSPM de Security Hub muestra una versión preliminar de los resultados a los que se aplica la regla. La vista previa no está disponible si los criterios de la regla incluyen un filtro CONTAINS o NOT_CONTAINS. Puede elegir estos filtros para los tipos de campos de mapeo y cadena.

> **Important**
>
> AWSrecomienda no incluir información de identificación personal, confidencial o confidencial en el nombre, la descripción u otros campos de la regla.

Creación de una regla de automatización personalizada

Elija su método preferido y realice los siguientes pasos para crear una regla de automatización personalizada.

Console

Para crear una regla de automatización personalizada (consola)

1. Con las credenciales del administrador CSPM de Security Hub, abra la consola CSPM AWS de Security Hub en. https://console.aws.amazon.com/securityhub/
2. En el panel de navegación, seleccione Automatizaciones.
3. Seleccione Crear regla. En Tipo de regla, seleccione Crear regla personalizada.

4. En la sección Regla, proporcione un nombre de regla único y una descripción de la regla.
5. En Criterios, utilice los menús desplegables de Clave, Operador y Valor para especificar los criterios de la regla. Debe especificar al menos un criterio de regla.

   Si los criterios seleccionados son compatibles, la consola muestra una vista previa de los resultados que cumplen dichos criterios.
6. En Acción automatizada, utilice los menús desplegables para especificar qué campos de resultado desea actualizar cuando los resultados coincidan con los criterios de la regla. Debe especificar al menos una regla de acción.
7. En Estado de la regla, elija si desea que la regla quede Habilitada o Deshabilitada tras su creación.
8. (Opcional) Amplíe la sección Ajustes adicionales. Seleccione Ignorar reglas posteriores para resultados que coincidan con estos criterios si desea que esta regla sea la última que se aplique a los resultados que coincidan con los criterios de la regla.
9. (Opcional) En Etiquetas, añada etiquetas como pares clave-valor para ayudarle a identificar fácilmente la regla.
10. Seleccione Creación de regla.

API

Para crear una regla de automatización personalizada (API)

1. Ejecute `CreateAutomationRule` desde la cuenta de administrador del CSPM de Security Hub. Esta API crea una regla con un nombre de recurso de Amazon (ARN) específico.
2. Introduzca un nombre y una descripción para la regla.
3. Defina el parámetro `IsTerminal` como `true` si desea que esta regla sea la última que se aplique a los resultados que coincidan con los criterios de la regla.
4. En el parámetro `RuleOrder`, indique el orden de la regla. El CSPM de Security Hub aplica primero las reglas con el valor numérico más bajo para este parámetro.
5. En el parámetro `RuleStatus`, especifique si desea que el CSPM de Security Hub habilite la regla y comience a aplicarla a los resultados una vez creada. El valor predeterminado es `ENABLED` si no se especifica ningún valor. Un valor de `DISABLED` significa que la regla queda en pausa tras su creación.
6. En el parámetro `Criteria`, proporcione los criterios que desea que el CSPM de Security Hub utilice para filtrar los resultados. La acción de la regla se aplicará a los resultados que

coincidan con los criterios. Para obtener una lista de los criterios admitidos, consulte Criterios de regla y acciones de regla disponibles.

7. En el parámetro `Actions`, proporcione las acciones que desea que el CSPM de Security Hub ejecute cuando exista una coincidencia entre un resultado y los criterios definidos. Para obtener una lista de las acciones admitidas, consulte Criterios de regla y acciones de regla disponibles.

El siguiente AWS CLI comando de ejemplo crea una regla de automatización que actualiza el estado del flujo de trabajo y anota las coincidencias. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$ aws securityhub create-automation-rule \
--actions '[{
 "Type": "FINDING_FIELDS_UPDATE",
 "FindingFieldsUpdate": {
 "Severity": {
 "Label": "HIGH"
 },
 "Note": {
 "Text": "Known issue that is a risk. Updated by automation rules",
 "UpdatedBy": "sechub-automation"
 }
 }
 }]' \
--criteria '{
 "SeverityLabel": [{
 "Value": "INFORMATIONAL",
 "Comparison": "EQUALS"
 }]
 }' \
--description "A sample rule" \
--no-is-terminal \
--rule-name "sample rule" \
--rule-order 1 \
--rule-status "ENABLED" \
--region us-east-1
```

Crear una regla de automatización a partir de una plantilla (solo en la consola)

Las plantillas de reglas reflejan casos de uso comunes para las reglas de automatización. Actualmente, solo la consola del CSPM de Security Hub admite plantillas de reglas. Complete los siguientes pasos para crear una regla de automatización a partir de una plantilla en la consola.

Para crear una regla de automatización a partir de una plantilla (en la consola)

1. Con las credenciales del administrador CSPM de Security Hub, abra la consola CSPM AWS de Security Hub en. https://console.aws.amazon.com/securityhub/
2. En el panel de navegación, seleccione Automatizaciones.
3. Seleccione Crear regla. En Tipo de regla, seleccione Crear una regla a partir de una plantilla.
4. Seleccione una plantilla de regla en el menú desplegable.
5. (Opcional) De ser necesario para su caso de uso, modifique las secciones Regla, Criterios y Acción automatizada. Debe especificar al menos un criterio de regla y una acción de regla.

   Si los criterios seleccionados son compatibles, la consola muestra una vista previa de los resultados que cumplen dichos criterios.
6. En Estado de la regla, elija si desea que la regla quede Habilitada o Deshabilitada tras su creación.
7. (Opcional) Amplíe la sección Ajustes adicionales. Seleccione Ignorar reglas posteriores para resultados que coincidan con estos criterios si desea que esta regla sea la última que se aplique a los resultados que coincidan con los criterios de la regla.
8. (Opcional) En Etiquetas, añada etiquetas como pares clave-valor para ayudarle a identificar fácilmente la regla.
9. Seleccione Creación de regla.

Visualización de las reglas de automatización

Se puede usar una regla de automatización para actualizar automáticamente los hallazgos en AWS Security Hub CSPM. Para obtener información general sobre cómo funcionan las reglas de automatización, consulte Descripción de las reglas de automatización en el CSPM de Security Hub.

Elija el método que prefiera y siga los pasos para ver sus reglas de automatización existentes y los detalles de cada regla.

Para obtener un historial de cómo las reglas de automatización han modificado sus resultados, consulte Revisión de detalles e historial de resultados en el CSPM de Security Hub.

Console

Para ver las reglas de automatización (consola)

1. Con las credenciales del administrador CSPM de Security Hub, abra la consola CSPM AWS de Security Hub en. https://console.aws.amazon.com/securityhub/
2. En el panel de navegación, seleccione Automatizaciones.
3. Elija un nombre de regla. También puede seleccionar una regla.
4. Seleccione Acciones y luego Ver.

API

Para ver las reglas de automatización (API)

1. Para ver las reglas de automatización de la cuenta, ejecute `ListAutomationRules` desde la cuenta de administrador del CSPM de Security Hub. Esta API devuelve los ARN y otros metadatos de sus reglas. No se requieren parámetros de entrada para esta API, pero puede como opción proporcionar `MaxResults` para limitar el número de resultados y `NextToken` como parámetro de paginación. El valor inicial de `NextToken` debería ser `NULL`.
2. Para obtener más detalles sobre las reglas, incluidos los criterios y las acciones de una regla, ejecute `BatchGetAutomationRules` desde la cuenta de administrador del CSPM de Security Hub. Proporcione los ARN de las reglas de automatización cuyos detalles desee obtener.

   En el siguiente ejemplo, se recuperan los detalles de las reglas de automatización especificadas. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$ aws securityhub batch-get-automation-rules \
--automation-rules-arns '["arn:aws:securityhub:us-
east-1:123456789012:automation-rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
 "arn:aws:securityhub:us-east-1:123456789012:automation-rule/a1b2c3d4-5678-90ab-
cdef-EXAMPLE22222"]' \
--region us-east-1
```

Edición de reglas de automatización

Se puede usar una regla de automatización para actualizar automáticamente los hallazgos en AWS Security Hub CSPM. Para obtener información general sobre cómo funcionan las reglas de automatización, consulte Descripción de las reglas de automatización en el CSPM de Security Hub.

Tras crear una regla de automatización, el administrador delegado del CSPM de Security Hub puede editar la regla. Al editar una regla de automatización, los cambios se aplican a los resultados nuevos y actualizados que el CSPM de Security Hub genera o ingiere después de la edición de la regla.

Elija el método que prefiera y siga los pasos para editar el contenido de una regla de automatización. Puede editar una o más reglas con una sola solicitud. Para obtener instrucciones sobre cómo editar el orden de las reglas, consulte Edición del orden de las reglas de automatización.

Console

Para editar las reglas de automatización (consola)

1. Con las credenciales del administrador CSPM de Security Hub, abra la consola CSPM AWS de Security Hub en. https://console.aws.amazon.com/securityhub/
2. En el panel de navegación, seleccione Automatizaciones.
3. Seleccione la regla que desea editar. Seleccione Acciones y luego Editar.
4. Cambie la regla como desee y seleccione Guardar cambios.

API

Para editar las reglas de automatización (API)

1. Ejecute `BatchUpdateAutomationRules` desde la cuenta de administrador del CSPM de Security Hub.
2. En el parámetro `RuleArn`, proporcione el ARN de las reglas que desee editar.
3. Proporcione los nuevos valores de los parámetros que desee editar. Puede editar cualquier parámetro excepto `RuleArn`.

En el siguiente ejemplo, se actualiza la regla de automatización especificada. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$ aws securityhub batch-update-automation-rules \
--update-automation-rules-request-items '[
    {
      "Actions": [{
        "Type": "FINDING_FIELDS_UPDATE",
        "FindingFieldsUpdate": {
          "Note": {
            "Text": "Known issue that is a risk",
            "UpdatedBy": "sechub-automation"
          },
          "Workflow": {
            "Status": "NEW"
          }
        }
      }],
      "Criteria": {
        "SeverityLabel": [{
         "Value": "LOW",
         "Comparison": "EQUALS"
        }]
      },
      "RuleArn": "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
      "RuleOrder": 14,
      "RuleStatus": "DISABLED",
    }
  ]' \
--region us-east-1
```

Edición del orden de las reglas de automatización

Se puede usar una regla de automatización para actualizar automáticamente los hallazgos en AWS Security Hub CSPM. Para obtener información general sobre cómo funcionan las reglas de automatización, consulte Descripción de las reglas de automatización en el CSPM de Security Hub.

Tras crear una regla de automatización, el administrador delegado del CSPM de Security Hub puede editar la regla.

Si desea mantener los criterios y las acciones de la regla tal como están, pero desea cambiar el orden en que el CSPM de Security Hub aplica una regla de automatización, es posible editar solo el orden de la regla. Elija el método que prefiera y siga los pasos para editar el orden de las reglas.

Para obtener instrucciones acerca de cómo editar los criterios o las acciones de una regla de automatización, consulte Edición de reglas de automatización.

Console

Para editar el orden de una regla de automatización (consola)

1. Con las credenciales del administrador CSPM de Security Hub, abra la consola CSPM AWS de Security Hub en. https://console.aws.amazon.com/securityhub/
2. En el panel de navegación, seleccione Automatizaciones.
3. Seleccione la regla cuyo orden desea modificar. Seleccione Editar prioridad.
4. Seleccione Subir para aumentar la prioridad de la regla en una unidad. Seleccione Bajar para disminuir la prioridad de la regla en una unidad. Seleccione Mover al principio para asignar a la regla un orden de 1 (esto da a la regla precedencia sobre otras existentes).

> **Note**
>
> Cuando crea una regla en la consola del CSPM de Security Hub, el CSPM de Security Hub asigna automáticamente un orden basado en el orden de creación de la regla. La regla creada más recientemente tiene el valor numérico más bajo de orden de reglas y, por lo tanto, se aplica primero.

API

Para editar el orden de una regla de automatización (API)

1. Use la operación `BatchUpdateAutomationRules` desde la cuenta de administrador del CSPM de Security Hub.
2. En el parámetro `RuleArn`, proporcione el ARN de las reglas cuyo orden desea editar.
3. Modifique el valor del campo `RuleOrder`.

> **Note**
>
> Si varias reglas tienen el mismo `RuleOrder`, el CSPM de Security Hub aplica primero una regla con un valor anterior para el campo `UpdatedAt` (es decir, la regla que se editó más recientemente se aplica en último lugar).

Eliminación o desactivación de las reglas de automatización

Se puede usar una regla de automatización para actualizar automáticamente los hallazgos en AWS Security Hub CSPM. Para obtener información general sobre cómo funcionan las reglas de automatización, consulte Descripción de las reglas de automatización en el CSPM de Security Hub.

Al eliminar una regla de automatización, el CSPM de Security Hub la elimina de la cuenta y deja de aplicarla a los resultados. Como alternativa a la eliminación, puede desactivar una regla. Esto retiene la regla para uso futuro, pero el CSPM de Security Hub no aplicará la regla a ningún resultado coincidente hasta que la habilite.

Elija el método que prefiera y siga los pasos para eliminar una regla de automatización. Puede eliminar una o más reglas en una sola solicitud.

Console

Para eliminar o desactivar las reglas de automatización (consola)

1. Con las credenciales del administrador CSPM de Security Hub, abra la consola CSPM AWS de Security Hub en. https://console.aws.amazon.com/securityhub/
2. En el panel de navegación, seleccione Automatizaciones.
3. Seleccione las reglas que desea eliminar. Seleccione Acción y luego Eliminar (para retener una regla, pero temporalmente deshabilitada, seleccione Deshabilitar).
4. Confirme la elección y seleccione Eliminar.

API

Para eliminar o desactivar las reglas de automatización (API)

1. Use la operación `BatchDeleteAutomationRules` desde la cuenta de administrador del CSPM de Security Hub.

2. En el parámetro `AutomationRulesArns`, indique el ARN de las reglas que desea eliminar (para retener una regla, pero temporalmente deshabilitada, indique `DISABLED` en el parámetro `RuleStatus`).

En el siguiente ejemplo, se elimina la regla de automatización que se especificó. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$ aws securityhub batch-delete-automation-rules \
--automation-rules-arns '["arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"]' \
--region us-east-1
```

Ejemplos de reglas de automatización

En esta sección se proporcionan ejemplos de reglas de automatización para casos de uso comunes del CSPM de Security Hub. Estos ejemplos corresponden a plantillas de reglas que están disponibles en la consola del CSPM de Security Hub.

Elevar la gravedad a Crítica cuando un recurso específico como un bucket S3 esté en riesgo

En este ejemplo, los criterios de la regla coinciden cuando el `ResourceId` de un resultado es un bucket específico de Amazon Simple Storage Service (Amazon S3). La acción de la regla es cambiar la gravedad de los resultados coincidentes a `CRITICAL`. Puede modificar esta plantilla para aplicarla a otros recursos.

Ejemplo de solicitud de API:

```
{
    "IsTerminal": true,
    "RuleName": "Elevate severity of findings that relate to important resources",
    "RuleOrder": 1,
    "RuleStatus": "ENABLED",
    "Description": "Elevate finding severity to CRITICAL when specific resource such as
 an S3 bucket is at risk",
    "Criteria": {
        "ProductName": [{
            "Value": "Security Hub CSPM",
            "Comparison": "EQUALS"
        }],
```

```
        "ComplianceStatus": [{
            "Value": "FAILED",
            "Comparison": "EQUALS"
        }],
        "RecordState": [{
            "Value": "ACTIVE",
            "Comparison": "EQUALS"
        }],
        "WorkflowStatus": [{
            "Value": "NEW",
            "Comparison": "EQUALS"
        }],
        "ResourceId": [{
            "Value": "arn:aws:s3:::amzn-s3-demo-bucket/developers/design_info.doc",
            "Comparison": "EQUALS"
        }]
    },
    "Actions": [{
        "Type": "FINDING_FIELDS_UPDATE",
        "FindingFieldsUpdate": {
            "Severity": {
                "Label": "CRITICAL"
            },
            "Note": {
                "Text": "This is a critical resource. Please review ASAP.",
                "UpdatedBy": "sechub-automation"
            }
        }
    }]
}
```

Ejemplo de comando de la CLI:

```
$
aws securityhub create-automation-rule \
--is-terminal \
--rule-name "Elevate severity of findings that relate to important resources" \
--rule-order 1 \
--rule-status "ENABLED" \

--description "Elevate finding severity to CRITICAL when specific resource such as an
 S3 bucket is at risk" \
--criteria '{
```

```
"ProductName": [{
"Value": "Security Hub CSPM",
"Comparison": "EQUALS"
}],
"ComplianceStatus": [{
"Value": "FAILED",
"Comparison": "EQUALS"
}],
"RecordState": [{
"Value": "ACTIVE",
"Comparison": "EQUALS"
}],
"WorkflowStatus": [{
"Value": "NEW",
"Comparison": "EQUALS"
}],
"ResourceId": [{
"Value": "arn:aws:s3:::amzn-s3-demo-bucket/developers/design_info.doc",
"Comparison": "EQUALS"
}]
}' \
--actions '[{
"Type": "FINDING_FIELDS_UPDATE",
"FindingFieldsUpdate": {
"Severity": {
"Label": "CRITICAL"
},
"Note": {
"Text": "This is a critical resource. Please review ASAP.",
"UpdatedBy": "sechub-automation"
}
}
}]' \
--region us-east-1
```

Cómo elevar la gravedad de los resultados relacionados con los recursos en cuentas de producción

En este ejemplo, los criterios de la regla coinciden cuando se genera un resultado de gravedad `HIGH` en cuentas de producción específicas. La acción de la regla es cambiar la gravedad de los resultados coincidentes a `CRITICAL`.

Ejemplo de solicitud de API:

```
{
    "IsTerminal": false,
    "RuleName": "Elevate severity for production accounts",
    "RuleOrder": 1,
    "RuleStatus": "ENABLED",
    "Description": "Elevate finding severity from HIGH to CRITICAL for findings that
 relate to resources in specific production accounts",
    "Criteria": {
        "ProductName": [{
            "Value": "Security Hub CSPM",
            "Comparison": "EQUALS"
        }],
        "ComplianceStatus": [{
            "Value": "FAILED",
            "Comparison": "EQUALS"
        }],
        "RecordState": [{
            "Value": "ACTIVE",
            "Comparison": "EQUALS"
        }],
        "WorkflowStatus": [{
            "Value": "NEW",
            "Comparison": "EQUALS"
        }],
        "SeverityLabel": [{
            "Value": "HIGH",
            "Comparison": "EQUALS"
        }],
        "AwsAccountId": [
        {
            "Value": "111122223333",
            "Comparison": "EQUALS"
        },
        {
            "Value": "123456789012",
            "Comparison": "EQUALS"
        }]
    },
    "Actions": [{
        "Type": "FINDING_FIELDS_UPDATE",
        "FindingFieldsUpdate": {
            "Severity": {
                "Label": "CRITICAL"
```

```
            },
            "Note": {
                "Text": "A resource in production accounts is at risk. Please review
 ASAP.",
                "UpdatedBy": "sechub-automation"
            }
        }
    }]
}
```

Ejemplo de comando de la CLI:

```
aws securityhub create-automation-rule \
--no-is-terminal \
--rule-name "Elevate severity of findings that relate to resources in production
 accounts" \
--rule-order 1 \
--rule-status "ENABLED" \
--description "Elevate finding severity from HIGH to CRITICAL for findings that relate
 to resources in specific production accounts" \
--criteria '{
"ProductName": [{
"Value": "Security Hub CSPM",
"Comparison": "EQUALS"
}],
"ComplianceStatus": [{
"Value": "FAILED",
"Comparison": "EQUALS"
}],
"RecordState": [{
"Value": "ACTIVE",
"Comparison": "EQUALS"
}],
"SeverityLabel": [{
"Value": "HIGH",
"Comparison": "EQUALS"
}],
"AwsAccountId": [
{
"Value": "111122223333",
"Comparison": "EQUALS"
},
```

```
{
"Value": "123456789012",
"Comparison": "EQUALS"
}]
}' \
--actions '[{
"Type": "FINDING_FIELDS_UPDATE",
"FindingFieldsUpdate": {
"Severity": {
"Label": "CRITICAL"
},
"Note": {
"Text": "A resource in production accounts is at risk. Please review ASAP.",
"UpdatedBy": "sechub-automation"
}
}
}]' \
--region us-east-1
```

Cómo suprimir resultados informativos

En este ejemplo, los criterios de la regla coinciden con los hallazgos de `INFORMATIONAL` gravedad enviados a Security Hub CSPM desde Amazon. GuardDuty La acción de la regla es cambiar el estado del flujo de trabajo de los resultados coincidentes a `SUPPRESSED`.

Ejemplo de solicitud de API:

```
{
    "IsTerminal": false,
    "RuleName": "Suppress informational findings",
    "RuleOrder": 1,
    "RuleStatus": "ENABLED",
    "Description": "Suppress GuardDuty findings with INFORMATIONAL severity",
    "Criteria": {
        "ProductName": [{
            "Value": "GuardDuty",
            "Comparison": "EQUALS"
        }],
        "RecordState": [{
            "Value": "ACTIVE",
            "Comparison": "EQUALS"
        }],
        "WorkflowStatus": [{
```

```
            "Value": "NEW",
            "Comparison": "EQUALS"
        }],
        "SeverityLabel": [{
            "Value": "INFORMATIONAL",
            "Comparison": "EQUALS"
        }]
    },
    "Actions": [{
        "Type": "FINDING_FIELDS_UPDATE",
        "FindingFieldsUpdate": {
            "Workflow": {
                "Status": "SUPPRESSED"
            },
            "Note": {
                "Text": "Automatically suppress GuardDuty findings with INFORMATIONAL
 severity",
                "UpdatedBy": "sechub-automation"
            }
        }
    }]
}
```

Ejemplo de comando de la CLI:

```
aws securityhub create-automation-rule \
--no-is-terminal \
--rule-name "Suppress informational findings" \
--rule-order 1 \
--rule-status "ENABLED" \
--description "Suppress GuardDuty findings with INFORMATIONAL severity" \
--criteria '{
"ProductName": [{
"Value": "GuardDuty",
"Comparison": "EQUALS"
}],
"ComplianceStatus": [{
"Value": "FAILED",
"Comparison": "EQUALS"
}],
"RecordState": [{
"Value": "ACTIVE",
```

```
"Comparison": "EQUALS"
}],
"WorkflowStatus": [{
"Value": "NEW",
"Comparison": "EQUALS"
}],
"SeverityLabel": [{
"Value": "INFORMATIONAL",
"Comparison": "EQUALS"
}]
}' \
--actions '[{
"Type": "FINDING_FIELDS_UPDATE",
"FindingFieldsUpdate": {
"Workflow": {
"Status": "SUPPRESSED"
},
"Note": {
"Text": "Automatically suppress GuardDuty findings with INFORMATIONAL severity",
"UpdatedBy": "sechub-automation"
}
}
}]' \
--region us-east-1
```

Uso EventBridge para respuesta y remediación automatizadas

Al crear reglas en Amazon EventBridge, puede responder automáticamente a las conclusiones del CSPM AWS de Security Hub. El CSPM de Security Hub envía las conclusiones en forma de eventos prácticamente en tiempo real. EventBridge Puede crear reglas sencillas para indicar qué eventos le resultan de interés, así como qué acciones automatizadas se van a realizar cuando un evento cumple una de las reglas. Entre las acciones que se pueden activar automáticamente se incluyen las siguientes:

- Invocar una función AWS Lambda
- Invocar el comando de ejecución de Amazon EC2
- Desviar el evento a Amazon Kinesis Data Streams
- Activar una máquina de AWS Step Functions estados
- Notificar un tema de Amazon SNS o una cola de Amazon SQS

- Enviar un resultado a una herramienta de gestión de tickets, chat, de SIEM o respuesta a incidentes de terceros

Security Hub CSPM envía automáticamente todos los hallazgos nuevos y todas las actualizaciones de los hallazgos existentes a un formato de eventos EventBridge . EventBridge También puede crear acciones personalizadas que le permitan enviar los hallazgos seleccionados y los resultados de información a. EventBridge

A continuación, configura EventBridge las reglas para responder a cada tipo de evento.

Para obtener más información sobre el uso EventBridge, consulte la Guía del EventBridge usuario de Amazon .

> **Note**
>
> Como práctica recomendada, asegúrate de que los permisos de acceso concedidos a tus usuarios EventBridge utilicen políticas de mínimos privilegios AWS Identity and Access Management (IAM) que concedan solo los permisos necesarios.
> Para obtener más información, consulte Administración de identidades y accesos en Amazon. EventBridge

En Solutions también hay disponible un conjunto de plantillas para la respuesta y la corrección automatizadas entre cuentas. AWS Las plantillas aprovechan las reglas de EventBridge eventos y las funciones de Lambda. La solución se implementa mediante CloudFormation y AWS Systems Manager. La solución puede crear acciones de respuesta y corrección totalmente automatizadas. También puede utilizar acciones personalizadas del CSPM de Security Hub para crear acciones de respuesta y corrección activadas por el usuario. Para obtener más información sobre cómo configurar y utilizar la solución, consulte la página de la solución Respuesta de seguridad automatizada en AWS.

Temas

- Los tipos de eventos de CSPM de Security Hub en EventBridge
- EventBridge formatos de eventos para Security Hub CSPM
- Configurar una EventBridge regla para las conclusiones del CSPM de Security Hub
- Uso de acciones personalizadas para enviar hallazgos e información a EventBridge

Los tipos de eventos de CSPM de Security Hub en EventBridge

Security Hub CSPM utiliza los siguientes tipos de EventBridge eventos de Amazon para integrarse con ellos. EventBridge

En el EventBridge panel de control de Security Hub CSPM, Todos los eventos incluyen todos estos tipos de eventos.

Todos los hallazgos (Hallazgos de Security Hub: importados)

El CSPM de Security Hub envía automáticamente todos los hallazgos nuevos y todas las actualizaciones de los hallazgos existentes a la categoría de eventos EventBridge . Security Hub Findings - Imported Cada evento Security Hub Findings - Imported contiene un único resultado.

Cada solicitud `BatchImportFindings` y `BatchUpdateFindings` desencadena un evento de Security Hub Findings - Imported.

En el caso de las cuentas de administrador, el feed de eventos EventBridge incluye los eventos de las cuentas de los administradores y de las cuentas de los miembros.

En una región de agregación, el feed de eventos incluye eventos para los hallazgos de la región de agregación y de las regiones vinculadas. Cross-Region los hallazgos se incluyen en el feed de eventos casi en tiempo real. Para obtener información sobre cómo configurar la agregación de resultados, consulte the section called “Agregar datos en las regiones”.

Puede definir reglas EventBridge que dirijan automáticamente los hallazgos a un flujo de trabajo de corrección, a una herramienta de terceros o a otro EventBridge objetivo compatible. Las reglas pueden incluir filtros que solo apliquen la regla si el resultado tiene valores de atributo específicos.

Este método le permite enviar automáticamente todos los resultados ,o todos aquellos con determinadas características, a un flujo de trabajo de corrección o respuesta.

Consulte the section called “Configuración de una regla EventBridge ”.

Hallazgos para acciones personalizadas (Hallazgos de Security Hub: acción personalizada)

El CSPM de Security Hub también envía a los eventos los hallazgos asociados a EventBridge las acciones personalizadas. Security Hub Findings - Custom Action

Esto resulta útil para los analistas que trabajan con la consola del CSPM de Security Hub y desean enviar un resultado específico, o un pequeño conjunto de resultados, a un flujo de trabajo

de respuesta o corrección. Puede seleccionar una acción personalizada para un máximo de 20 resultados a la vez. Cada hallazgo se envía EventBridge como un evento independiente EventBridge .

Al crear una acción personalizada, usted asigna un ID de acción personalizada. Puede usar este identificador para crear una EventBridge regla que lleve a cabo una acción específica después de recibir un hallazgo asociado a ese identificador de acción personalizado.

Consulte the section called “Configuración y uso de acciones personalizadas”.

Por ejemplo, puede crear una acción personalizada en el CSPM de Security Hub llamada `send_to_ticketing`. A continuación EventBridge, crea una regla que se activa cuando EventBridge recibe un hallazgo que incluye el ID de acción `send_to_ticketing` personalizado. La regla incluye lógica para enviar el resultado a su sistema de tickets. Posteriormente, puede seleccionar resultados en el CSPM de Security Hub y utilizar la acción personalizada en el CSPM de Security Hub para enviar manualmente los resultados al sistema de tickets.

Para ver ejemplos de cómo enviar las conclusiones del CSPM de Security Hub EventBridge para su posterior procesamiento, consulte Cómo integrar las acciones personalizadas del CSPM de AWS Security Hub PagerDuty y cómo habilitar las acciones personalizadas en el CSPM de AWS Security Hub en el blog AWS Partner Network (APN).

Resultados detallados sobre las acciones personalizadas (Resultados de Security Hub Insight)

También puede usar acciones personalizadas para enviar conjuntos de resultados de información a EventBridge modo de Security Hub Insight Results eventos. Los resultados de información son los recursos que coinciden con una información. Tenga en cuenta que cuando envía los resultados de información a EventBridge, no envía los hallazgos a EventBridge. Solo está enviando los identificadores de recursos asociados a los resultados de información. Puede enviar hasta 100 identificadores de recursos a la vez.

Al igual que ocurre con las acciones personalizadas para los hallazgos, primero se crea la acción personalizada en Security Hub CSPM y, a continuación, se crea una regla en. EventBridge

Consulte the section called “Configuración y uso de acciones personalizadas”.

Por ejemplo, supongamos que ve un determinado resultado de información de interés que desea compartir con un colega. En ese caso, puede utilizar una acción personalizada para enviar ese resultado de información al colega a través de un chat o de un sistema de tickets.

EventBridge formatos de eventos para Security Hub CSPM

Los tipos de eventos Security Hub Findings - Imported, Security Findings - Custom Action y Security Hub Insight Results utilizan los siguientes formatos de eventos.

El formato de evento es el formato que se usa cuando Security Hub CSPM envía un evento. EventBridge

Hallazgos de Security Hub: importados

Security Hub Findings - Importedlos eventos que se envían desde Security Hub CSPM para EventBridge usar el siguiente formato.

```
{
   "version":"0",
   "id":"CWE-event-id",
   "detail-type":"Security Hub Findings - Imported",
   "source":"aws.securityhub",
   "account":"111122223333",
   "time":"2019-04-11T21:52:17Z",
   "region":"us-west-2",
   "resources":[
      "arn:aws:securityhub:us-west-2::product/aws/macie/arn:aws:macie:us-
west-2:111122223333:integtest/trigger/6294d71b927c41cbab915159a8f326a3/alert/
f2893b211841"
   ],
   "detail":{
      "findings": [{
         <finding content>
       }]
   }
}
```

<finding content> es el contenido, en formato JSON, del resultado que envía el evento. Cada evento envía un único resultado.

Para obtener una lista completa de los atributos de los resultados, consulte AWS Formato de búsqueda de seguridad (ASFF).

Para obtener información sobre cómo configurar EventBridge las reglas que se activan a partir de estos eventos, consulte. the section called “Configuración de una regla EventBridge ”

Conclusiones de Security Hub: acción personalizada

Security Hub Findings - Custom Actionlos eventos que se envían desde el CSPM de Security Hub para EventBridge usar el siguiente formato. Cada resultado se envía en un evento independiente.

```
{
  "version": "0",
  "id": "1a1111a1-b22b-3c33-444d-5555e5ee5555",
  "detail-type": "Security Hub Findings - Custom Action",
  "source": "aws.securityhub",
  "account": "111122223333",
  "time": "2019-04-11T18:43:48Z",
  "region": "us-west-1",
  "resources": [
    "arn:aws:securityhub:us-west-1:111122223333:action/custom/custom-action-name"
  ],
  "detail": {
    "actionName":"custom-action-name",
    "actionDescription": "description of the action",
    "findings": [
      {
        <finding content>
      }
    ]
  }
}
```

<finding content> es el contenido, en formato JSON, del resultado que envía el evento. Cada evento envía un único resultado.

Para obtener una lista completa de los atributos de los resultados, consulte AWS Formato de búsqueda de seguridad (ASFF).

Para obtener información sobre cómo configurar EventBridge las reglas que se activan a partir de estos eventos, consulte. the section called “Configuración y uso de acciones personalizadas”

Resultados de Security Hub Insight

Security Hub Insight Resultslos eventos que se envían desde Security Hub CSPM para EventBridge usar el siguiente formato.

```
{
  "version": "0",
```

```
  "id": "1a1111a1-b22b-3c33-444d-5555e5ee5555",
  "detail-type": "Security Hub Insight Results",
  "source": "aws.securityhub",
  "account": "111122223333",
  "time": "2017-12-22T18:43:48Z",
  "region": "us-west-1",
  "resources": [
      "arn:aws:securityhub:us-west-1:111122223333::product/aws/macie:us-
west-1:222233334444:test/trigger/1ec9cf700ef6be062b19584e0b7d84ec/alert/f2893b211841"
  ],
  "detail": {
    "actionName":"name of the action",
    "actionDescription":"description of the action",
    "insightArn":"ARN of the insight",
    "insightName":"Name of the insight",
    "resultType":"ResourceAwsIamAccessKeyUserName",
    "number of results":"number of results, max of 100",
    "insightResults": [
        {"result 1": 5},
        {"result 2": 6}
    ]
  }
}
```

Para obtener información sobre cómo crear una EventBridge regla que se active a partir de estos eventos, consulte. the section called “Configuración y uso de acciones personalizadas”

Configurar una EventBridge regla para las conclusiones del CSPM de Security Hub

Puede crear una regla en Amazon EventBridge que defina la acción que se debe realizar cuando se recibe un Security Hub Findings - Imported evento. Security Hub Findings - Importedlos eventos se activan por las actualizaciones de las `BatchUpdateFindings` operaciones `BatchImportFindings` y.

Cada regla contiene un patrón de eventos, que identifica los eventos que activan la regla. El patrón de eventos siempre contiene la fuente del evento (`aws.securityhub`) y el tipo de evento (Resultados de Security Hub - Importado). El patrón de eventos también puede especificar filtros para identificar los resultados a los que se aplica la regla.

A continuación, la regla de eventos identifica los objetivos de la regla. Los objetivos son las acciones que se deben tomar cuando se EventBridge recibe un evento de Security Hub llamado Findings: Imported y el resultado coincide con los filtros.

Las instrucciones que se proporcionan aquí utilizan la EventBridge consola. Cuando usas la consola, crea EventBridge automáticamente la política requerida basada en los recursos que te permite EventBridge escribir en Amazon CloudWatch Logs.

También puede utilizar el `PutRule` funcionamiento de la EventBridge API. Sin embargo, si usas la EventBridge API, debes crear la política basada en los recursos. Para obtener información sobre la política requerida, consulte los permisos de CloudWatch registro en la Guía del EventBridge usuario de Amazon.

Formato del patrón de eventos

El formato del patrón de eventos para los eventos Resultados de Security Hub - Importado es el siguiente:

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Security Hub Findings - Imported"
  ],
  "detail": {
    "findings": {
      <attribute filter values>
    }
  }
}
```

- `source` identifica al CSPM de Security Hub como el servicio que genera el evento.
- `detail-type` identifica el tipo de evento.
- `detail` es opcional y proporciona los valores de filtro para el patrón de eventos. Si el patrón de eventos no contiene un campo `detail`, todos los resultados activan la regla.

Puede filtrar los resultados en función de cualquier atributo del resultado. Para cada atributo, proporciona una matriz separada por comas de uno o más valores.

```
"<attribute name>": [ "<value1>", "<value2>"]
```

Si proporciona más de un valor para un atributo, estos valores se unen mediante `OR`. Un resultado coincide con el filtro para un atributo individual si el resultado tiene cualquiera de los valores enumerados. Por ejemplo, si proporciona `INFORMATIONAL` y `LOW` como valores para `Severity.Label`, entonces el resultado coincide si tiene una etiqueta de gravedad de `INFORMATIONAL` o `LOW`.

Los atributos se unen mediante `AND`. Un resultado coincide si este coincide con los criterios de filtrado para todos los atributos proporcionados.

Cuando proporciones un valor de atributo, este debe reflejar la ubicación de ese atributo dentro de la estructura del formato de búsqueda de AWS seguridad (ASFF).

> **Tip**
>
> Para filtrar los resultados de los controles, le recomendamos que utilice los campos ASFF `SecurityControlId` o `SecurityControlArn` como filtros, en vez de `Title` o `Description`. Estos últimos campos podrían cambiar ocasionalmente, mientras que el ID de control y el ARN son identificadores estáticos.

En el siguiente ejemplo, el patrón de eventos proporciona valores de filtro para `ProductArn` y `Severity.Label`, por lo que un resultado coincide si lo genera Amazon Inspector y tiene una etiqueta de gravedad de `INFORMATIONAL` o `LOW`.

```
{
    "source": [
        "aws.securityhub"
     ],
    "detail-type": [
        "Security Hub Findings - Imported"
    ],
    "detail": {
        "findings": {
            "ProductArn": ["arn:aws:securityhub:us-east-1::product/aws/inspector"],
            "Severity": {
                "Label": ["INFORMATIONAL", "LOW"]
            }
        }
    }
}
```

Creación de una regla de eventos

Puede usar un patrón de eventos predefinido o un patrón de eventos personalizado para crear una regla. EventBridge Si seleccionas un patrón predefinido, rellena EventBridge automáticamente `source` y`detail-type`. EventBridge también proporciona campos para especificar los valores de filtro para los siguientes atributos de búsqueda:

- `AwsAccountId`
- `Compliance.Status`
- `Criticality`
- `ProductArn`
- `RecordState`
- `ResourceId`
- `ResourceType`
- `Severity.Label`
- `Types`
- `Workflow.Status`

Para crear una EventBridge regla (consola)

1. Abre la EventBridge consola de Amazon en https://console.aws.amazon.com/events/.
2. Con los siguientes valores, cree una EventBridge regla que supervise la búsqueda de eventos:
   - En Tipo de regla, seleccione Regla con un patrón de evento.
   - Elija cómo crear el patrón de eventos.

Cómo crear el patrón de eventos con...	Haga lo siguiente...	
Una plantilla	En la sección Patrón de eventos, elija una de las siguientes opciones: • En Origen del evento, seleccione Servicios de AWS .	

Cómo crear el patrón de eventos con...	Haga lo siguiente...	
	• En Servicio de AWS , elija Security Hub. • En Tipo de evento, seleccione Resultados de Security Hub - Importado. • (Opcional) Para que la regla sea más específic a, agregue valores de filtro. Por ejemplo, para limitar la regla a resultado s con estados de registro activos, en Estados de registro específicos, seleccione Activo.	

Cómo crear el patrón de eventos con...	Haga lo siguiente...	
Un patrón de eventos personalizado (Utilice un patrón personalizado si desea filtrar los hallazgos en función de los atributos que no aparecen en la EventBridge consola).	• En la sección Patrón de evento, seleccione Patrones personalizados (editor JSON) y luego pegue el siguiente patrón de evento en el área de texto: `{ "source": [ "aws.securityhub" ], "detail-type": [ "Security Hub Findings - Imported" ], "detail": { "findings": { "<attribute name> ": [ "<value1>", "<value2>"] } } }` • Actualice el patrón de eventos para incluir el atributo y los valores del atributo que desee utilizar como filtro. Por ejemplo, para aplicar la regla a los resultados que tengan un estado de	

Cómo crear el patrón de eventos con...	Haga lo siguiente...	
	verificación `TRUE_POSITIVE` , utilice el siguiente patrón de ejemplo:	

```
{
  "source": [
    "aws.secu
rityhub"
  ],
  "detail-type": [
    "Security
 Hub Findings -
 Imported"
  ],
  "detail": {
    "findings": {
      "Verifica
tionState":
 ["TRUE_POSITIVE"]
    }
  }
}
```

- Para los tipos de destino, elija el AWS servicio y, para Seleccionar un objetivo, elija un objetivo, como un tema o una AWS Lambda función de Amazon SNS. El destino se activa cuando se recibe un evento que coincide con el patrón de eventos definido en la regla.

Para obtener más información sobre la creación de reglas, consulte Creación de EventBridge reglas de Amazon que reaccionen a los eventos en la Guía del EventBridge usuario de Amazon.

Uso de acciones personalizadas para enviar hallazgos e información a EventBridge

Para usar las acciones personalizadas de AWS Security Hub CSPM para enviar hallazgos o perspectivas a Amazon EventBridge, primero debe crear la acción personalizada en Security

Hub CSPM. A continuación, puede definir reglas EventBridge que se apliquen a sus acciones personalizadas.

Puede crear hasta 50 acciones personalizadas.

Si habilita la agregación entre regiones y administra los resultados desde la región de agregación, debe crear acciones personalizadas en la región de agregación.

La regla EventBridge utiliza el nombre de recurso de Amazon (ARN) de la acción personalizada.

Crear una acción personalizada

Al crear una acción personalizada en AWS Security Hub CSPM, debe especificar su nombre, descripción y un identificador único.

Una acción personalizada especifica las acciones que se deben realizar cuando un EventBridge evento coincide con una EventBridge regla. El CSPM de Security Hub envía cada hallazgo EventBridge como un evento.

Elija su método preferido y siga los pasos para crear una acción personalizada.

Console

Cómo crear una acción personalizada en el CSPM de Security Hub (consola)

1. Abra la consola AWS CSPM de Security Hub en. https://console.aws.amazon.com/securityhub/
2. En el panel de navegación, elija Settings (Configuración) y luego elija Custom actions (Acciones personalizadas).
3. Seleccione Create custom action (Crear acción personalizada).
4. Proporcione un Name (Nombre), Description (Descripción) e Custom action ID (ID de acción personalizada) para la acción.

   El Name (Nombre) debe tener menos de 20 caracteres.

   El ID de acción personalizada debe ser único por cada cuenta de AWS .
5. Seleccione Create custom action (Crear acción personalizada).
6. Anote el ARN de acción personalizada. Debe usar el ARN cuando cree una regla para asociarla con esta acción en EventBridge.

API

Para crear una acción personalizada (API)

Utilice la operación CreateActionTarget. Si está utilizando el comando create-action-target AWS CLI, ejecute el comando https://docs.aws.amazon.com/cli/latest/reference/securityhub/create-action-target.html create-action-target.

En el siguiente ejemplo, se crea una acción personalizada para enviar resultados a una herramienta de corrección. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$ aws securityhub create-action-target --name "Send to remediation" --description
 "Action to send the finding for remediation tracking" --id "Remediation"
```

Definir una regla en EventBridge

Para activar una acción personalizada en Amazon EventBridge, debes crear la regla correspondiente en. EventBridge La definición de la regla incluye el nombre de recurso de Amazon (ARN) de la acción personalizada.

El patrón de evento para un evento Resultados de Security Hub - Acción personalizada tiene el siguiente formato:

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Security Hub Findings - Custom Action"
  ],
  "resources": [ "<custom action ARN>" ]
}
```

El patrón de evento para un evento Resultados de Security Hub - Acción personalizada tiene el siguiente formato:

```
{
  "source": [
    "aws.securityhub"
```

```
  ],
  "detail-type": [
    "Security Hub Insight Results"
  ],
  "resources": [ "<custom action ARN>" ]
}
```

En ambos patrones, `<custom action ARN>` es el ARN de una acción personalizada. Puede configurar una regla que se aplique a más de una acción personalizada.

Las instrucciones que se proporcionan aquí son para la EventBridge consola. Al usar la consola, crea EventBridge automáticamente la política basada en los recursos requerida que permite EventBridge escribir CloudWatch en los registros.

También puedes usar la operación `PutRule` API de la EventBridge API. Sin embargo, si usas la EventBridge API, debes crear la política basada en los recursos. Para obtener más información sobre la política requerida, consulte los permisos de CloudWatch registro en la Guía del EventBridge usuario de Amazon.

Para definir una regla en EventBridge (EventBridge consola)

1. Abre la EventBridge consola de Amazon en https://console.aws.amazon.com/events/.
2. En el panel de navegación, seleccione Reglas.
3. Elija Creación de regla.
4. Escriba un nombre y una descripción para la regla.
5. En Bus de eventos, elija el bus de eventos que desea asociar a esta regla. Si desea que esta regla coincida con eventos procedentes de su cuenta, seleccione predeterminado. Cuando un servicio de AWS en la cuenta emite un evento, siempre va al bus de eventos predeterminado de la cuenta.
6. En Tipo de regla, seleccione Regla con un patrón de eventos.
7. Seleccione Siguiente.
8. En Origen de eventos, seleccione (Eventos de AWS).
9. En la sección Patrón de eventos, seleccione Formulario de patrón de eventos.
10. En Origen del evento, seleccione Servicios de AWS .
11. En Servicio de AWS , seleccione Security Hub.
12. En Tipo de evento, realice una de las siguientes operaciones:

- Para crear una regla que se aplique al enviar resultados a una acción personalizada, seleccione Resultados de Security Hub - Acción personalizada.
- Para crear una regla que se aplique al enviar resultados de información a una acción personalizada, seleccione Resultados de información de Security Hub.

13. Seleccione ARN de acciones personalizadas específicas y añada un ARN de acción personalizada.

    Si la regla se aplica a varias acciones personalizadas, seleccione Añadir para añadir más ARN de acciones personalizadas.
14. Elija Siguiente.
15. En Seleccionar objetivos, elija y configure el objetivo por invocar cuando esta regla coincida.
16. Elija Siguiente.
17. (Opcional) Introduzca una o varias etiquetas para la regla. Para obtener más información, consulte las EventBridge etiquetas de Amazon en la Guía del EventBridge usuario de Amazon.
18. Elija Siguiente.
19. Revise los detalles de la regla y seleccione Creación de regla.

    Cuando realizas una acción personalizada sobre las conclusiones o los resultados de información de tu cuenta, los eventos se generan en EventBridge.

Selección de una acción personalizada para resultados y resultados de información

Después de crear las acciones personalizadas de CSPM y las EventBridge reglas de Amazon de AWS Security Hub, puede enviar las conclusiones y los resultados de la información EventBridge para su administración y procesamiento automáticos.

Los eventos EventBridge solo se envían a la cuenta en la que se ven. Si ve un hallazgo con una cuenta de administrador, el evento se envía a EventBridge la cuenta de administrador.

Para que las llamadas a la AWS API sean efectivas, las implementaciones del código de destino deben convertir los roles en cuentas de miembros. Esto también significa que el rol al que se cambia debe implementarse en cada miembro en el que sea necesario actuar.

Para enviar los hallazgos a EventBridge (consola)

1. Abra la consola CSPM de AWS Security Hub en. https://console.aws.amazon.com/securityhub/

2. Visualice una lista de resultados:
   - En Resultados, puede ver los resultados de todas las integraciones de productos y controles habilitados.
   - En Estándares de seguridad, puede dirigirse a una lista de resultados generados a partir de un control específico. Para obtener más información, consulte Cómo revisar los detalles de los controles en el CSPM de Security Hub.
   - En Integraciones puede dirigirse a una lista de resultados generada por una de las integraciones habilitadas. Para obtener más información, consulte Visualización de los resultados a partir de una integración con el CSPM de Security Hub.
   - En Información, puede dirigirse a una lista de resultados de un resultado de información. Para obtener más información, consulte Revisión de productos de información y medidas al respecto en el CSPM de Security Hub.
3. Seleccione los hallazgos a los que desea enviarlos. EventBridge Puede seleccionar hasta 20 hallazgos a la vez.
4. En Acciones, elija la acción personalizada que se alinee con la EventBridge regla que se va a aplicar.

   El CSPM de Security Hub envía un evento Resultados de Security Hub - Acción personalizada independiente por cada resultado.

Para enviar los resultados de información a EventBridge (consola)

1. Abra la consola CSPM de AWS Security Hub en. https://console.aws.amazon.com/securityhub/
2. En el panel de navegación, elija Insights.
3. En la página Perspectivas, elija la información que incluya los resultados a los que desea enviarlos. EventBridge
4. Seleccione los resultados de la información a la que desea enviarlos EventBridge. Puede seleccionar hasta 20 resultados a la vez.
5. En Acciones, elija la acción personalizada que se alinee con la EventBridge regla que se va a aplicar.

Uso del panel en el CSPM de Security Hub

En la consola del CSPM de Security Hub, el panel Resumen muestra un resumen de riesgos, secuencias de ataque y cobertura de seguridad. Este panel ayuda a identificar riesgos y secuencias de ataque según la gravedad y la cobertura de la cuenta para distintas capacidades de seguridad. Cada vez que abre el panel, este se actualiza de forma automática. Sin embargo, tenga en cuenta que las puntuaciones de seguridad y los estados de los controles se actualizan cada 24 horas.

Puede personalizar el panel Resumen con distintos widgets de seguridad que puede agregar o quitar. También puede especificar criterios de filtrado para obtener y mostrar tipos específicos de datos. Si personaliza el panel, Security Hub guarda las configuraciones de personalización. Si otros usuarios de la cuenta personalizan el panel, los cambios se guardan de forma independiente de las configuraciones de personalización propias.

Si configuró la agregación entre regiones en el CSPM de Security Hub, el panel Resumen muestra los datos agregados. Si la cuenta es la cuenta administradora delegada de una organización, los datos incluyen los resultados de la cuenta y los de las cuentas de miembro. Si la cuenta es una cuenta de miembro o una cuenta independiente, los datos incluyen únicamente los resultados de la cuenta.

Temas

- Widgets disponibles para el panel Resumen
- Filtrado del panel Resumen en el CSPM de Security Hub
- Personalización del panel Resumen en el CSPM de Security Hub

Widgets disponibles para el panel Resumen

El panel de resumen incluye widgets que reflejan el panorama moderno de las amenazas a la seguridad en la nube, guiados por las operaciones de seguridad y las experiencias de los AWS clientes. Algunos widgets se muestran de forma predeterminada, mientras que otros no. Puede agregar o quitar widgets para personalizar la vista del panel.

Para agregar un widget, seleccione Agregar widget en la parte superior del panel. Luego, puede revisar la lista de widgets disponibles o ingresar el título de un widget en la barra de búsqueda. Cuando encuentre el widget que desea agregar, arrástrelo hasta el lugar donde quiere que aparezca en el panel. Para obtener más información, consulte Personalización del panel de .

Widgets mostrados de forma predeterminada

El panel Resumen incluye los siguientes widgets de forma predeterminada:

Secuencias de amenazas principales

Muestra las secuencias de amenazas con la mayor gravedad. Los hallazgos de la secuencia de amenazas, conocidos como hallazgos de la secuencia de ataque en Amazon GuardDuty, correlacionan varios eventos para identificar posibles amenazas para su AWS entorno. Las secuencias de amenaza pueden incluir comportamientos de ataque en curso o recientes (dentro de un intervalo de 24 horas) en el entorno, lo que a su vez puede derivar en un compromiso adicional. Debe tener GuardDuty habilitada la protección GuardDuty S3 para recibir los resultados de la secuencia de amenazas en Security Hub CSPM.

Principales riesgos

Muestra un resumen de los riesgos principales en el entorno. La parte superior del widget muestra la cantidad de riesgos en cada nivel de gravedad. Puede elegir un nivel de gravedad para ir a la página Riesgos, donde los riesgos aparecen filtrados según el nivel seleccionado. Los riesgos con más ocurrencias en el entorno aparecen primero. Este widget ayuda a priorizar los riesgos que debe mitigar.

Cobertura de seguridad

Resume el alcance de la cobertura de seguridad según los resultados de controles de cobertura. Los controles de cobertura comprueban si una Servicio de AWS información específica y sus capacidades están habilitadas (por ejemplo,[Macie.1] Amazon Macie debería estar activado). Este widget le ayuda a confirmar que cuenta con resultados `PASSED` para los controles de cobertura. La consola del CSPM de Security Hub ofrece enlaces desde este widget para facilitar la habilitación de las capacidades de seguridad faltantes. Recomendamos utilizar una configuración central para habilitar las funciones de seguridad que faltan en varios Cuentas de AWS y Regiones de AWS. Para obtener más información, consulte Descripción de la configuración central en el CSPM de Security Hub.

Estándares de seguridad

Muestra la puntuación de seguridad más reciente y la puntuación correspondiente a cada estándar del CSPM de Security Hub. Las puntuaciones de seguridad, que van del 0 % al 100 %, representan la proporción de controles aprobados en relación con todos los controles habilitados. Para obtener más información acerca de estas puntuaciones, consulte Método de cálculo de las

puntuaciones de seguridad. Este widget le ayuda a entender su posición general en materia de seguridad.

Los activos con más resultados

Proporciona información general de los activos, las cuentas y las aplicaciones que generan más resultados. La lista se ordena por número de resultados de forma descendente. En el widget, cada pestaña muestra los seis elementos principales de esa categoría, agrupados por gravedad y tipo de recurso. Si selecciona un número en la columna Resultados totales, el CSPM de Security Hub abre una página que presenta los resultados del activo. Este widget le ayuda a identificar rápidamente cuáles de sus activos principales presentan posibles amenazas a la seguridad.

Resultados por región

Muestra el número total de resultados, agrupados por gravedad, en cada Región de AWS en la que el CSPM de Security Hub está habilitado. Este widget le ayuda a identificar los problemas de seguridad que pueden afectar a determinadas regiones. Si abre el panel en su región de agregación, este widget le ayudará a supervisar los posibles problemas de seguridad de cada región vinculada.

Tipos de amenazas más comunes

Proporciona un desglose de los 10 tipos de amenazas más comunes en su AWS entorno. Esto incluye amenazas como derivación de privilegios, uso de credenciales expuestas o comunicación con direcciones IP maliciosas.

Para ver estos datos, Amazon GuardDuty debe estar habilitada. Si es así, elige un tipo de amenaza en este widget para abrir la GuardDuty consola y revisar los resultados relacionados con esta amenaza. Este widget le ayuda a evaluar las posibles amenazas en el contexto de otros problemas de seguridad.

Vulnerabilidades de software con exploits

Proporciona un resumen de las vulnerabilidades de software que existen en su AWS entorno y que tienen vulnerabilidades conocidas. También puede revisar un desglose de las vulnerabilidades que tienen soluciones disponibles y las que no.

Para ver estos datos, Amazon Inspector debe estar habilitado. Si es así, seleccione una estadística en este widget para abrir la consola de Amazon Inspector y ver más detalles sobre la vulnerabilidad. Este widget le ayuda a evaluar las vulnerabilidades del software en el contexto de otros problemas de seguridad.

Nuevos resultados a lo largo del tiempo

Muestra las tendencias en el número de nuevos resultados diarios durante los últimos 90 días. Puede desglosar los datos por gravedad o por proveedor para obtener un contexto adicional. Este widget le ayuda a saber si ha aumentado o disminuido el volumen de resultados en momentos específicos durante los últimos 90 días.

Recursos con la mayor cantidad de resultados

Proporciona un resumen de los recursos que han generado la mayor cantidad de hallazgos, desglosados según los siguientes tipos de recursos: depósitos de Amazon Simple Storage Service (Amazon S3), instancias de Amazon Elastic Compute Cloud (Amazon EC2) y funciones. AWS Lambda

En el widget, cada pestaña se centra en uno de los tipos de recursos anteriores y enumera las 10 instancias de recursos que han generado la mayoría de los resultados. Para revisar los resultados de un recurso específico, seleccione la instancia del recurso. Este widget le ayuda a clasificar los resultados de seguridad asociados a los recursos comunes. AWS

Widgets ocultos de forma predeterminada

Los siguientes widgets también están disponibles en el panel Resumen; sin embargo, permanecen ocultos de forma predeterminada.

AMI con la mayor cantidad de resultados

Ofrece una lista de las 10 imágenes de máquina de Amazon (AMI) que han generado más resultados. Estos datos están disponibles únicamente si Amazon EC2 está habilitado en la cuenta. Le ayudan a identificar qué AMI representan posibles riesgos de seguridad.

Entidades principales de IAM con la mayor cantidad de resultados

Proporciona una lista de los 10 usuarios AWS Identity and Access Management (IAM) que han generado el mayor número de hallazgos. Este widget le ayuda a llevar a cabo tareas administrativas y de facturación. Muestra qué usuarios aportan en mayor medida al uso del CSPM de Security Hub.

Cuentas con la mayor cantidad de resultados (por gravedad)

Muestra un gráfico de las 10 cuentas que han generado la mayor cantidad de resultados, agrupadas por gravedad. Este widget le ayuda a determinar en qué cuentas debe centrar los esfuerzos de análisis y corrección.

Cuentas con la mayor cantidad de resultados (por tipo de recurso)

Muestra un gráfico de las 10 cuentas que han generado la mayor cantidad de resultados, agrupadas por tipo de recurso. Este widget le ayuda a determinar qué cuentas y tipos de recursos se deben priorizar en cuestión de análisis y corrección.

Información

Presenta cinco productos de información administrados del CSPM de Security Hub, junto con la cantidad de resultados que generó cada uno. Dichos elementos identifican un área de seguridad específica que requiere atención.

Hallazgos más recientes de las AWS integraciones

Muestra la cantidad de resultados que recibió en el CSPM de Security Hub desde Servicios de AWS integrados. También muestra cuándo recibió por última vez los resultados de cada servicio integrado. Este widget proporciona datos de hallazgos consolidados de múltiples Servicios de AWS. Para obtener más detalles, seleccione un servicio integrado. Luego, el CSPM de Security Hub abre la consola del servicio correspondiente.

Filtrado del panel Resumen en el CSPM de Security Hub

Puede depurar el panel Resumen en la consola del CSPM de Security Hub para incluir solo los datos de seguridad que le resulten más relevantes. Por ejemplo, si es miembro de un equipo de aplicaciones, puede crear una vista específica para una aplicación crítica de su entorno de producción. Si es miembro de un equipo de seguridad, puede crear una vista específica que le ayude a centrarse en los resultados de mayor gravedad.

Para crear estas vistas depuradas, ingrese los criterios de filtrado en el cuadro de filtros situado encima del panel. Si aplica criterios de filtrado, estos se aplican a todos los datos y widgets del panel, excepto a los datos de los widgets Productos de información y Estándares de seguridad. Para ver una lista de los widgets disponibles en el panel de control, consulteWidgets disponibles para el panel Resumen.

Puede filtrar los datos mediante los campos siguientes:

- Nombre de cuenta
- ID de cuenta
- ARN de la aplicación
- Nombre de la aplicación

- Nombre del producto (para un producto Servicio de AWS o un producto de terceros que envía las conclusiones al CSPM de Security Hub)
- Record state (Estado de registro)
- Region
- Etiqueta de recurso
- Gravedad
- Estado del flujo de trabajo

Los datos del panel se filtran, de forma predeterminada, según los siguientes criterios: `Workflow.Status` es `NOTIFIED` o `NEW`, y `RecordState` es `ACTIVE`. Estos criterios aparecen encima del panel, debajo del cuadro de filtro. Para eliminar estos criterios, seleccione X en el token del filtro para los criterios que desea eliminar.

Si aplica criterios de filtro que desea volver a utilizar, puede guardarlos como un conjunto de filtros. Un conjunto de filtros es una agrupación de criterios de filtro que crea y guarda para volver a aplicarlos al revisar los datos que se muestran en el panel Resumen. Puede crear y guardar un conjunto de filtros que use cualquiera de los campos disponibles, excepto los siguientes: ARN de la aplicación, nombre de la aplicación y etiqueta de recurso.

Creación y almacenamiento de conjuntos de filtros

Para crear y guardar un conjunto de filtros, siga estos pasos.

Creación y almacenamiento de un conjunto de filtros

1. Abra la consola AWS CSPM de Security Hub en. https://console.aws.amazon.com/securityhub/
2. En el panel de navegación, elija Resumen.
3. En el cuadro de filtros situado encima del panel Resumen, ingrese los criterios de filtro para el conjunto correspondiente.
4. En el menú Borrar filtros, seleccione Guardar nuevo conjunto de filtros.
5. En el cuadro de diálogo Guardar conjunto de filtros, ingrese un nombre para el conjunto de filtros.
6. (Opcional) Para utilizar el conjunto de filtros predeterminado cada vez que abra la página Resumen, seleccione la opción para establecerlo como vista predeterminada.
7. Seleccione Save.

Para cambiar entre los conjuntos de filtros que ha creado y guardado, utilice el menú Seleccionar un conjunto de filtros situado encima del panel Resumen. Cuando selecciona un conjunto de filtros, el CSPM de Security Hub aplica los criterios del conjunto de filtros a los datos del panel.

Actualización o eliminación de conjuntos de filtros

Siga estos pasos para actualizar o eliminar un conjunto de filtros existente. Si elimina un conjunto de filtros que está configurado como vista predeterminada del panel Resumen, la vista predeterminada vuelve a la vista predeterminada del CSPM de Security Hub.

Actualización o eliminación de un conjunto de filtros

1. Abra la consola AWS CSPM de Security Hub en. https://console.aws.amazon.com/securityhub/
2. En el panel de navegación, elija Resumen.
3. En el menú Seleccionar un conjunto de filtros situado encima de la página Resumen, seleccione el conjunto de filtros.
4. En el menú Borrar filtros, haga una de las siguientes operaciones:
   - Para actualizar el conjunto de filtros, seleccione Actualizar conjunto de filtros actual. A continuación, ingrese sus cambios en el cuadro de diálogo que aparece.
   - Para eliminar el conjunto de filtros, seleccione Eliminar conjunto de filtros actual. A continuación, en el cuadro de diálogo que aparece, seleccione Eliminar.

Personalización del panel Resumen en el CSPM de Security Hub

Puede personalizar el panel Resumen en la consola del CSPM de Security Hub de varias maneras. Por ejemplo, puede agregar y eliminar widgets del panel. También puede reorganizar y cambiar el tamaño de los widgets del panel. Para consultar la lista de widgets disponibles y la descripción de cada uno, consulte Widgets disponibles para el panel Resumen.

Si personaliza el panel, el CSPM de Security Hub aplica los cambios de inmediato y guarda la nueva configuración del panel. Los cambios se aplican a la visualización del panel de control en todos Regiones de AWS los navegadores.

Para personalizar el Resumen panel

1. Abra la consola CSPM de AWS Security Hub en. https://console.aws.amazon.com/securityhub/
2. En el panel de navegación, elija Resumen.

3. Realice uno de los siguientes procedimientos:

   - Para agregar un widget, seleccione Agregar widgets en la esquina superior derecha de la página. En la barra de búsqueda, ingrese el título del widget que desea agregar. A continuación, arrastre el widget a la ubicación que desee.
   - Para eliminar un widget, seleccione los tres puntos que aparecen en la esquina superior derecha del widget.
   - Para mover un widget, seleccione el controlador que está en su esquina superior izquierda y, a continuación, arrastre el widget a la ubicación que desee.
   - Para cambiar el tamaño de un widget, elija el controlador de cambio de tamaño que está en su esquina inferior derecha. Arrastre el borde del widget hasta que tenga el tamaño que prefiera.

Para restaurar posteriormente la configuración original, seleccione Restablecer al diseño predeterminado en la parte superior de la página.

Límites regionales del CSPM de Security Hub

Algunas funciones CSPM de AWS Security Hub solo están disponibles en algunas. Regiones de AWS En las siguientes secciones se especifican estos límites regionales. Para obtener una lista de todas las regiones en las que el CSPM de Security Hub se encuentra actualmente disponible, consulte Puntos de conexión y cuotas del CSPM de AWS Security Hub en la Referencia general de AWS.

Cross-Region restricciones de agregación

EnAWS GovCloud (US) Regions, la agregación entre regiones está disponible AWS GovCloud (US) Regions únicamente para los hallazgos, las actualizaciones de las búsquedas y la información de alcance global. En concreto, puede agregar los hallazgos, las actualizaciones y la información solo entre las regiones AWS GovCloud (US-East) y AWS GovCloud (US-West).

En las regiones de China, la agregación entre regiones solo está disponible para los resultados, las actualizaciones de resultados y los hallazgos de las regiones de China. En concreto, solo puede agregar resultados, actualizaciones de resultados y productos de información entre las regiones China (Pekín) y China (Ningxia).

No puede usar una región que esté desactivada de forma predeterminada como región de agregación. Para ver una lista de las regiones que están deshabilitadas de forma predeterminada,

consulta la sección Habilitar o deshabilitar Regiones de AWS tu cuenta en la Guía de AWS Account Management referencia.

Disponibilidad de las integraciones por región

Algunas integraciones no están disponibles en todasRegiones de AWS. En la consola del CSPM de Security Hub, una integración no aparece en la página de Integraciones si no está disponible en la región en la que ha iniciado sesión.

Integraciones admitidas en las regiones China (Pekín) y China (Ningxia)

En las regiones China (Pekín) y China (Ningxia), el CSPM de Security Hub admite únicamente las siguientes integraciones con Servicios de AWS:

- AWS Firewall Manager
- Amazon GuardDuty
- AWS Identity and Access Management Access Analyzer
- Amazon Inspector
- AWS IoT Device Defender
- AWS Systems Manager Explorer
- AWS Systems ManagerOpsCenter
- AWS Systems ManagerAdministrador de parches

En las regiones China (Pekín) y China (Ningxia), el CSPM de Security Hub admite únicamente las siguientes integraciones con terceros:

- Cloud Custodian
- FireEye Helix
- Helecloud
- IBM QRadar
- PagerDuty
- Palo Alto Networks Cortex XSOAR
- Palo Alto Networks VM-Series
- Prowler
- RSA Archer

- Splunk Enterprise
- Splunk Phantom
- ThreatModeler

Integraciones compatibles con elAWS GovCloud (US-East)andAWS GovCloud (US-West)Regions

En las AWS GovCloud (US-West) regiones AWS GovCloud (US-East) y, Security Hub CSPM solo admite las siguientes integraciones con: Servicios de AWS

- AWS Config
- Amazon Detective
- AWS Firewall Manager
- Amazon GuardDuty
- AWS Health
- Analizador de acceso de IAM
- Amazon Inspector
- AWS IoT Device Defender

En las AWS GovCloud (US-West) regiones AWS GovCloud (US-East) y, Security Hub CSPM solo admite las siguientes integraciones de terceros:

- Atlassian Jira Service Management
- Atlassian Jira Service Management Cloud
- Atlassian OpsGenie
- Caveonix Cloud
- Cloud Custodian
- Cloud Storage Security Antivirus for Amazon S3
- CrowdStrike Falcon
- FireEye Helix
- Forcepoint CASB
- Forcepoint DLP
- Forcepoint NGFW

- Fugue
- Kion
- MicroFocus ArcSight
- NETSCOUT Cyber Investigator
- PagerDuty
- Palo Alto Networks – Prisma Cloud Compute
- Palo Alto Networks – Prisma Cloud Enterprise
- Palo Alto Networks – VM-Series(disponible solo en AWS GovCloud ()) US-West
- Prowler
- Rackspace Technology – Cloud Native Security
- Rapid7 InsightConnect
- RSA Archer
- ServiceNow ITSM
- Slack
- ThreatModeler
- Vectra AI Cognito Detect

Disponibilidad de los estándares por región

El estándar AWS Control Tower de gestión de servicios solo está disponible en aquellos soportesRegiones de AWS. AWS Control Tower Para obtener una lista de las regiones compatibles AWS Control Tower actualmente, consulte Cómo Regiones de AWS trabajar con ellas AWS Control Tower en la Guía del AWS Control Towerusuario.

El estándar AWS de etiquetado de recursos no está disponible en la región de Asia Pacífico (Taipéi).

Hay otros estándares de seguridad disponibles en todas las regiones en las que el CSPM de Security Hub está disponible.

Disponibilidad de los controles por región

Algunos controles CSPM de Security Hub no están disponibles en todos. Regiones de AWS Para obtener una lista de los controles que no están disponibles en cada región, consulte Límites regionales de los controles del CSPM de Security Hub.

En la consola del CSPM de Security Hub, un control no aparece en la lista si no está disponible en la región en la que ha iniciado sesión. La excepción es una región de agregación. Si configuró una región de agregación e inicia sesión en esa región, la consola muestra los controles que están disponibles en la región de agregación o en una o más regiones vinculadas.

Límites regionales de los controles del CSPM de Security Hub

Algunos controles CSPM de AWS Security Hub no están disponibles en todos. Regiones de AWS Esta página indica qué controles no están disponibles en regiones específicas.

En la consola del CSPM de Security Hub, un control no aparece en la lista si no está disponible en la región en la que ha iniciado sesión. La excepción es una región de agregación. Si configuró una región de agregación e inicia sesión en esa región, la consola muestra los controles que están disponibles en la región de agregación o en una o más regiones vinculadas.

Regiones de AWS

- Este de EE. UU. (Norte de Virginia)
- Este de EE. UU. (Ohio)
- Oeste de EE. UU. (Norte de California)
- Oeste de EE. UU. (Oregón)
- África (Ciudad del Cabo)
- Asia-Pacífico (Hong Kong)
- Asia-Pacífico (Hyderabad)
- Asia-Pacífico (Yakarta)
- Asia-Pacífico (Malasia)
- Asia-Pacífico (Melbourne)
- Asia-Pacífico (Mumbai)
- Asia-Pacífico (Nueva Zelanda)
- Asia-Pacífico (Osaka)
- Asia-Pacífico (Seúl)
- Asia-Pacífico (Singapur)
- Asia-Pacífico (Sídney)
- Asia-Pacífico (Taipéi)

- Asia-Pacífico (Tailandia)
- Asia-Pacífico (Tokio)
- Canadá (centro)
- Oeste de Canadá (Calgary)
- China (Pekín)
- China (Ningxia)
- Europa (Fráncfort)
- Europa (Irlanda)
- Europa (Londres)
- Europa (Milán)
- Europa (París)
- Europa (España)
- Europa (Estocolmo)
- Europa (Zúrich)
- Israel (Tel Aviv)
- México (centro)
- Middle East (Bahrain)
- Medio Oriente (EAU)
- América del Sur (São Paulo)
- AWS GovCloud (US-East)
- AWS GovCloud (US-West)

Este de EE. UU. (Norte de Virginia)

Los siguientes controles no se admiten en la región este de EE. UU. (norte de Virginia).

- [ElastiCache.4] los grupos de ElastiCache replicación deben cifrarse en reposo
- [ElastiCache.5] los grupos de ElastiCache replicación deben cifrarse en tránsito
- [ElastiCache.6] ElastiCache (Redis OSS) Los grupos de replicación de versiones anteriores deberían tener habilitada la autenticación de Redis OSS
- [ElastiCache.7] los ElastiCache clústeres no deben usar el grupo de subredes predeterminado

- [GlobalAccelerator.1] Los aceleradores de Global Accelerator deben estar etiquetados
- [S3.24] Los puntos de Multi-Region acceso S3 deben tener habilitada la configuración de bloqueo del acceso público

Este de EE. UU. (Ohio)

Los siguientes controles no se admiten en la región este de EE. UU. (Ohio).

- [AppSync.1]AWS AppSyncLas cachés de las API deben estar cifradas en reposo
- [AppSync.6]AWS AppSyncLas cachés de las API deben cifrarse en tránsito
- [CloudFront.1] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado
- [CloudFront.3] CloudFront las distribuciones deben requerir el cifrado durante el tránsito
- [CloudFront.4] CloudFront las distribuciones deben tener configurada la conmutación por error de origen
- [CloudFront.5] CloudFront las distribuciones deben tener habilitado el registro
- [CloudFront.6] CloudFront las distribuciones deben tener WAF activado
- [CloudFront.7] CloudFront las distribuciones deben usar certificados personalizados SSL/TLS
- [CloudFront.8] CloudFront las distribuciones deben usar el SNI para atender las solicitudes HTTPS
- [CloudFront.9] CloudFront las distribuciones deben cifrar el tráfico para convertirlo en orígenes personalizados
- [CloudFront.10] CloudFront las distribuciones no deben usar protocolos SSL obsoletos entre ubicaciones de borde y orígenes personalizados
- [CloudFront.12] CloudFront las distribuciones no deben apuntar a orígenes de S3 inexistentes
- [CloudFront.13] CloudFront las distribuciones deben usar el control de acceso al origen
- [CloudFront.14] CloudFront las distribuciones deben estar etiquetadas
- [CloudFront.15] CloudFront las distribuciones deben usar la política de seguridad TLS recomendada
- [CloudFront.16] CloudFront las distribuciones deben usar el control de acceso de origen para los orígenes de las URL de las funciones de Lambda
- [CloudFront.17] CloudFront las distribuciones deben usar grupos de claves confiables para las URL y cookies firmadas

- [Connect.1] Los tipos de objetos de los perfiles de clientes de Amazon Connect deben estar etiquetados
- [Connect.2] Las instancias de Connect Customer deben tener el CloudWatch registro habilitado
- [EC2.24] No se deben utilizar los tipos de instancias paravirtuales de Amazon EC2
- [EC2.173] Las solicitudes de EC2 Spot Fleet con parámetros de lanzamiento deberían permitir el cifrado de los volúmenes de EBS adjuntos
- [ECR.4] Los repositorios públicos de ECR deben etiquetarse
- [GlobalAccelerator.1] Los aceleradores de Global Accelerator deben estar etiquetados
- [IAM.26] SSL/TLS Los certificados caducados gestionados en IAM deben eliminarse
- [IoTTwinMaker.1]AWSLos trabajos de TwinMaker sincronización de IoT deben estar etiquetados
- [IoTTwinMaker.2]AWS TwinMaker Los espacios de trabajo de IoT deben estar etiquetados
- [IoTTwinMaker.3]AWS TwinMaker Las escenas de IoT deben estar etiquetadas
- [IoTTwinMaker.4]AWS TwinMaker Las entidades de IoT deben estar etiquetadas
- [IoTWireless.1]AWSLos grupos de multidifusión de IoT Wireless deben estar etiquetados
- [IoTWireless.2]AWSLos perfiles de servicio de IoT Wireless deben estar etiquetados
- [IoTWireless.3]AWSLas tareas de IoT FUOTA deben estar etiquetadas
- [IVS.1] Los pares de teclas de reproducción IVS deben estar etiquetados
- [IVS.2] Las configuraciones de grabación de IVS deben estar etiquetadas
- [IVS.3] Los canales IVS deben estar etiquetados
- [RDS.31] Los grupos de seguridad de la base de datos de RDS deben etiquetarse
- [Route53.1] Los controles de salud de Route 53 deben estar etiquetados
- [Route53.2] Las zonas alojadas públicas de Route 53 deberían registrar las consultas de DNS
- [S3.24] Los puntos de Multi-Region acceso S3 deben tener habilitada la configuración de bloqueo del acceso público
- [WAF.1]AWS WAFEl registro de ACL web global clásico debe estar habilitado
- [WAF.6]AWS WAFLas reglas globales clásicas deben tener al menos una condición
- [WAF.7]AWS WAFLos grupos de reglas globales clásicos deben tener al menos una regla
- [WAF.8]AWS WAFLas ACL web globales clásicas deben tener al menos una regla o grupo de reglas
- [WorkSpaces.1] los volúmenes de WorkSpaces usuarios deben cifrarse en reposo

- [WorkSpaces.2] los volúmenes WorkSpaces raíz deben cifrarse en reposo

Oeste de EE. UU. (Norte de California)

Los siguientes controles no se admiten en la región oeste de EE. UU. (norte de California).

- [AppRunner.1] Los servicios de App Runner deben estar etiquetados
- [AppRunner.2] Los conectores VPC de App Runner deben estar etiquetados
- [AppSync.1]AWS AppSyncLas cachés de las API deben estar cifradas en reposo
- [AppSync.6]AWS AppSyncLas cachés de las API deben cifrarse en tránsito
- [BedrockAgentCore.1] Los AgentCore tiempos de ejecución de Bedrock deben configurarse con el modo de red VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways debería requerir autorización para las solicitudes entrantes
- [BedrockAgentCore.3] Bedrock AgentCore Memory debe estar cifrada y gestionada por el clienteAWS KMSclaves
- [BedrockAgentCore.4] Bedrock AgentCore Gateway debe cifrarse de forma que sea gestionada por el clienteAWS KMSclaves
- [BedrockAgentCore.5] Los navegadores AgentCore personalizados de Bedrock no deberían usar el modo de red pública
- [BedrockAgentCore.6] Los navegadores AgentCore personalizados de Bedrock deberían tener habilitada la grabación de sesiones
- [CloudFront.1] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado
- [CloudFront.3] CloudFront las distribuciones deben requerir el cifrado durante el tránsito
- [CloudFront.4] CloudFront las distribuciones deben tener configurada la conmutación por error de origen
- [CloudFront.5] CloudFront las distribuciones deben tener habilitado el registro
- [CloudFront.6] CloudFront las distribuciones deben tener WAF activado
- [CloudFront.7] CloudFront las distribuciones deben usar certificados personalizados SSL/TLS
- [CloudFront.8] CloudFront las distribuciones deben usar el SNI para atender las solicitudes HTTPS
- [CloudFront.9] CloudFront las distribuciones deben cifrar el tráfico para convertirlo en orígenes personalizados

- [CloudFront.10] CloudFront las distribuciones no deben usar protocolos SSL obsoletos entre ubicaciones de borde y orígenes personalizados
- [CloudFront.12] CloudFront las distribuciones no deben apuntar a orígenes de S3 inexistentes
- [CloudFront.13] CloudFront las distribuciones deben usar el control de acceso al origen
- [CloudFront.14] CloudFront las distribuciones deben estar etiquetadas
- [CloudFront.15] CloudFront las distribuciones deben usar la política de seguridad TLS recomendada
- [CloudFront.16] CloudFront las distribuciones deben usar el control de acceso de origen para los orígenes de las URL de las funciones de Lambda
- [CloudFront.17] CloudFront las distribuciones deben usar grupos de claves confiables para las URL y cookies firmadas
- [CodeArtifact.1] CodeArtifact los repositorios deben estar etiquetados
- [CodeGuruProfiler.1] Los grupos CodeGuru de creación de perfiles de Profiler deben estar etiquetados
- [CodeGuruReviewer.1] Las asociaciones de repositorios de CodeGuru Reviewer deben estar etiquetadas
- [Connect.1] Los tipos de objetos de los perfiles de clientes de Amazon Connect deben estar etiquetados
- [Connect.2] Las instancias de Connect Customer deben tener el CloudWatch registro habilitado
- [DocumentDB.1] Los clústeres de Amazon DocumentDB deben cifrarse en reposo
- [DocumentDB.2] Los clústeres de Amazon DocumentDB deben tener un período de retención de copias de seguridad adecuado
- [DocumentDB.3] Las instantáneas de clústeres manuales de Amazon DocumentDB no deben ser públicas
- [DocumentDB.4] Los clústeres de Amazon DocumentDB deben publicar los registros de auditoría en Logs CloudWatch
- [DocumentDB.5] Los clústeres de Amazon DocumentDB deben tener habilitada la protección contra eliminaciones
- [DocumentDB.6] Los clústeres de Amazon DocumentDB deben cifrarse en tránsito
- [EC2.173] Las solicitudes de EC2 Spot Fleet con parámetros de lanzamiento deberían permitir el cifrado de los volúmenes de EBS adjuntos

- [ECR.4] Los repositorios públicos de ECR deben etiquetarse
- [FraudDetector.1] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.2] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas
- [FraudDetector.3] Los resultados de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.4] Las variables de Amazon Fraud Detector deben estar etiquetadas
- [GlobalAccelerator.1] Los aceleradores de Global Accelerator deben estar etiquetados
- [IAM.26] SSL/TLS Los certificados caducados gestionados en IAM deben eliminarse
- [Inspector.3] El escaneo de código Lambda de Amazon Inspector Lambda debe estar activado
- [IoTSiteWise.1]AWSLos modelos SiteWise de activos de IoT deben estar etiquetados
- [IoTSiteWise.2]AWS SiteWise Los paneles de IoT deben estar etiquetados
- [IoTSiteWise.3]AWS SiteWise Las pasarelas de IoT deben estar etiquetadas
- [IoTSiteWise.4]AWS SiteWise Los portales de IoT deben estar etiquetados
- [IoTSiteWise.5]AWS SiteWise Los proyectos de IoT deben estar etiquetados
- [IoTTwinMaker.1]AWSLos trabajos de TwinMaker sincronización de IoT deben estar etiquetados
- [IoTTwinMaker.2]AWS TwinMaker Los espacios de trabajo de IoT deben estar etiquetados
- [IoTTwinMaker.3]AWS TwinMaker Las escenas de IoT deben estar etiquetadas
- [IoTTwinMaker.4]AWS TwinMaker Las entidades de IoT deben estar etiquetadas
- [IoTWireless.1]AWSLos grupos de multidifusión de IoT Wireless deben estar etiquetados
- [IoTWireless.2]AWSLos perfiles de servicio de IoT Wireless deben estar etiquetados
- [IoTWireless.3]AWSLas tareas de IoT FUOTA deben estar etiquetadas
- [IVS.1] Los pares de teclas de reproducción IVS deben estar etiquetados
- [IVS.2] Las configuraciones de grabación de IVS deben estar etiquetadas
- [IVS.3] Los canales IVS deben estar etiquetados
- [RDS.35] Los clústeres de bases de datos de RDS deben tener habilitada la actualización automática de versiones secundarias
- [RDS.47] Los clústeres de bases de datos de RDS para PostgreSQL deben configurarse para copiar las etiquetas a las instantáneas de bases de datos
- [RDS.48] Los clústeres de bases de datos de RDS para MySQL deben configurarse para copiar etiquetas a las instantáneas de bases de datos

- [Redshift.18] Los clústeres de Redshift deberían tener Multi-AZ las implementaciones habilitadas
- [Route53.1] Los controles de salud de Route 53 deben estar etiquetados
- [Route53.2] Las zonas alojadas públicas de Route 53 deberían registrar las consultas de DNS
- [S3.24] Los puntos de Multi-Region acceso S3 deben tener habilitada la configuración de bloqueo del acceso público
- [S3.25] Los buckets de directorio de S3 deben tener configuraciones de ciclo de vida
- [WAF.1]AWS WAFEl registro de ACL web global clásico debe estar habilitado
- [WAF.6]AWS WAFLas reglas globales clásicas deben tener al menos una condición
- [WAF.7]AWS WAFLos grupos de reglas globales clásicos deben tener al menos una regla
- [WAF.8]AWS WAFLas ACL web globales clásicas deben tener al menos una regla o grupo de reglas
- [WorkSpaces.1] los volúmenes de WorkSpaces usuarios deben cifrarse en reposo
- [WorkSpaces.2] los volúmenes WorkSpaces raíz deben cifrarse en reposo

Oeste de EE. UU. (Oregón)

Los siguientes controles no se admiten en la región oeste de EE. UU. (Oregón).

- [AppSync.1]AWS AppSyncLas cachés de las API deben estar cifradas en reposo
- [AppSync.6]AWS AppSyncLas cachés de las API deben cifrarse en tránsito
- [BedrockAgentCore.3] Bedrock AgentCore Memory debe estar cifrada y gestionada por el clienteAWS KMSclaves
- [CloudFront.1] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado
- [CloudFront.3] CloudFront las distribuciones deben requerir el cifrado durante el tránsito
- [CloudFront.4] CloudFront las distribuciones deben tener configurada la conmutación por error de origen
- [CloudFront.5] CloudFront las distribuciones deben tener habilitado el registro
- [CloudFront.6] CloudFront las distribuciones deben tener WAF activado
- [CloudFront.7] CloudFront las distribuciones deben usar certificados personalizados SSL/TLS
- [CloudFront.8] CloudFront las distribuciones deben usar el SNI para atender las solicitudes HTTPS

- [CloudFront.9] CloudFront las distribuciones deben cifrar el tráfico para convertirlo en orígenes personalizados
- [CloudFront.10] CloudFront las distribuciones no deben usar protocolos SSL obsoletos entre ubicaciones de borde y orígenes personalizados
- [CloudFront.12] CloudFront las distribuciones no deben apuntar a orígenes de S3 inexistentes
- [CloudFront.13] CloudFront las distribuciones deben usar el control de acceso al origen
- [CloudFront.14] CloudFront las distribuciones deben estar etiquetadas
- [CloudFront.15] CloudFront las distribuciones deben usar la política de seguridad TLS recomendada
- [CloudFront.16] CloudFront las distribuciones deben usar el control de acceso de origen para los orígenes de las URL de las funciones de Lambda
- [CloudFront.17] CloudFront las distribuciones deben usar grupos de claves confiables para las URL y cookies firmadas
- [EC2.173] Las solicitudes de EC2 Spot Fleet con parámetros de lanzamiento deberían permitir el cifrado de los volúmenes de EBS adjuntos
- [ECR.4] Los repositorios públicos de ECR deben etiquetarse
- [IAM.26] SSL/TLS Los certificados caducados gestionados en IAM deben eliminarse
- [Route53.1] Los controles de salud de Route 53 deben estar etiquetados
- [Route53.2] Las zonas alojadas públicas de Route 53 deberían registrar las consultas de DNS
- [WAF.1]AWS WAFEl registro de ACL web global clásico debe estar habilitado
- [WAF.6]AWS WAFLas reglas globales clásicas deben tener al menos una condición
- [WAF.7]AWS WAFLos grupos de reglas globales clásicos deben tener al menos una regla
- [WAF.8]AWS WAFLas ACL web globales clásicas deben tener al menos una regla o grupo de reglas

África (Ciudad del Cabo)

Los siguientes controles no se admiten en la región África (Ciudad del Cabo).

- [Amplify.1] Las aplicaciones Amplify deben estar etiquetadas
- [Amplify.2] Amplify branches debe estar etiquetado
- [AppRunner.1] Los servicios de App Runner deben estar etiquetados

- [AppRunner.2] Los conectores VPC de App Runner deben estar etiquetados
- [AppSync.1]AWS AppSyncLas cachés de las API deben estar cifradas en reposo
- [AppSync.6]AWS AppSyncLas cachés de las API deben cifrarse en tránsito
- [BedrockAgentCore.1] Los AgentCore tiempos de ejecución de Bedrock deben configurarse con el modo de red VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways debería requerir autorización para las solicitudes entrantes
- [BedrockAgentCore.3] Bedrock AgentCore Memory debe estar cifrada y gestionada por el clienteAWS KMSclaves
- [BedrockAgentCore.4] Bedrock AgentCore Gateway debe cifrarse de forma que sea gestionada por el clienteAWS KMSclaves
- [BedrockAgentCore.5] Los navegadores AgentCore personalizados de Bedrock no deberían usar el modo de red pública
- [BedrockAgentCore.6] Los navegadores AgentCore personalizados de Bedrock deberían tener habilitada la grabación de sesiones
- [CloudFront.1] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado
- [CloudFront.3] CloudFront las distribuciones deben requerir el cifrado durante el tránsito
- [CloudFront.4] CloudFront las distribuciones deben tener configurada la conmutación por error de origen
- [CloudFront.5] CloudFront las distribuciones deben tener habilitado el registro
- [CloudFront.6] CloudFront las distribuciones deben tener WAF activado
- [CloudFront.7] CloudFront las distribuciones deben usar certificados personalizados SSL/TLS
- [CloudFront.8] CloudFront las distribuciones deben usar el SNI para atender las solicitudes HTTPS
- [CloudFront.9] CloudFront las distribuciones deben cifrar el tráfico para convertirlo en orígenes personalizados
- [CloudFront.10] CloudFront las distribuciones no deben usar protocolos SSL obsoletos entre ubicaciones de borde y orígenes personalizados
- [CloudFront.12] CloudFront las distribuciones no deben apuntar a orígenes de S3 inexistentes
- [CloudFront.13] CloudFront las distribuciones deben usar el control de acceso al origen
- [CloudFront.14] CloudFront las distribuciones deben estar etiquetadas

- [CloudFront.15] CloudFront las distribuciones deben usar la política de seguridad TLS recomendada
- [CloudFront.16] CloudFront las distribuciones deben usar el control de acceso de origen para los orígenes de las URL de las funciones de Lambda
- [CloudFront.17] CloudFront las distribuciones deben usar grupos de claves confiables para las URL y cookies firmadas
- [CodeArtifact.1] CodeArtifact los repositorios deben estar etiquetados
- [CodeGuruProfiler.1] Los grupos CodeGuru de creación de perfiles de Profiler deben estar etiquetados
- [CodeGuruReviewer.1] Las asociaciones de repositorios de CodeGuru Reviewer deben estar etiquetadas
- [Cognito.1] Los grupos de usuarios de Cognito deben tener activada la protección contra amenazas y el modo de aplicación con todas las funciones para la autenticación estándar
- [DMS.10] Los puntos finales de DMS para las bases de datos de Neptune deben tener habilitada la autorización de IAM
- [DocumentDB.1] Los clústeres de Amazon DocumentDB deben cifrarse en reposo
- [DocumentDB.2] Los clústeres de Amazon DocumentDB deben tener un período de retención de copias de seguridad adecuado
- [DocumentDB.3] Las instantáneas de clústeres manuales de Amazon DocumentDB no deben ser públicas
- [DocumentDB.4] Los clústeres de Amazon DocumentDB deben publicar los registros de auditoría en Logs CloudWatch
- [DocumentDB.5] Los clústeres de Amazon DocumentDB deben tener habilitada la protección contra eliminaciones
- [DocumentDB.6] Los clústeres de Amazon DocumentDB deben cifrarse en tránsito
- [DynamoDB.3] Los clústeres de DynamoDB Accelerator (DAX) deben cifrarse en reposo
- [DynamoDB.7] Los clústeres de DynamoDB Accelerator deben cifrarse en tránsito
- [EC2.4] Las instancias EC2 detenidas deben eliminarse después de un período de tiempo específico
- [EC2.14] Los grupos de seguridad no deberían permitir la entrada desde la versión 0.0.0. 0/0 o: :/0 al puerto 3389
- [EC2.24] No se deben utilizar los tipos de instancias paravirtuales de Amazon EC2

- [EC2.58] Las VPC deben configurarse con un punto final de interfaz para los contactos de Systems Manager Incident Manager
- [EC2.60] Las VPC deben configurarse con un punto final de interfaz para Systems Manager Incident Manager
- [EC2.173] Las solicitudes de EC2 Spot Fleet con parámetros de lanzamiento deberían permitir el cifrado de los volúmenes de EBS adjuntos
- [EC2.177] Las sesiones de réplica de tráfico de EC2 deben etiquetarse
- [EC2.179] Los objetivos del espejo de tráfico de EC2 deben estar etiquetados
- [ECR.4] Los repositorios públicos de ECR deben etiquetarse
- [ELB.2] Los balanceadores de carga clásicos con SSL/HTTPS oyentes deben usar un certificado proporcionado por AWS Gestor de certificados
- [ES.3] Los dominios de Elasticsearch deben cifrar los datos enviados entre nodos
- [EventBridge.4] los puntos finales EventBridge globales deberían tener habilitada la replicación de eventos
- [FraudDetector.1] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.2] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas
- [FraudDetector.3] Los resultados de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.4] Las variables de Amazon Fraud Detector deben estar etiquetadas
- [GlobalAccelerator.1] Los aceleradores de Global Accelerator deben estar etiquetados
- [IAM.18] Asegúrese de que se haya creado una función de soporte para gestionar los incidentes conAWS Support
- [IAM.26] SSL/TLS Los certificados caducados gestionados en IAM deben eliminarse
- [Inspector.3] El escaneo de código Lambda de Amazon Inspector Lambda debe estar activado
- [IoT.1]AWS IoT Device Defenderlos perfiles de seguridad deben estar etiquetados
- [IoT.2]AWS IoT Corelas acciones de mitigación deben estar etiquetadas
- [IoT.3]AWS IoT Corelas dimensiones deben estar etiquetadas
- [IoT.4]AWS IoT Corelos autorizadores deben estar etiquetados
- [IoT.5]AWS IoT CoreLos alias de los roles deben estar etiquetados
- [IoT.6]AWS IoT Corelas políticas deben estar etiquetadas
- [IoTSiteWise.1]AWSLos modelos SiteWise de activos de IoT deben estar etiquetados

- [IoTSiteWise.2]AWS SiteWise Los paneles de IoT deben estar etiquetados
- [IoTSiteWise.3]AWS SiteWise Las pasarelas de IoT deben estar etiquetadas
- [IoTSiteWise.4]AWS SiteWise Los portales de IoT deben estar etiquetados
- [IoTSiteWise.5]AWS SiteWise Los proyectos de IoT deben estar etiquetados
- [IoTTwinMaker.1]AWSLos trabajos de TwinMaker sincronización de IoT deben estar etiquetados
- [IoTTwinMaker.2]AWS TwinMaker Los espacios de trabajo de IoT deben estar etiquetados
- [IoTTwinMaker.3]AWS TwinMaker Las escenas de IoT deben estar etiquetadas
- [IoTTwinMaker.4]AWS TwinMaker Las entidades de IoT deben estar etiquetadas
- [IoTWireless.1]AWSLos grupos de multidifusión de IoT Wireless deben estar etiquetados
- [IoTWireless.2]AWSLos perfiles de servicio de IoT Wireless deben estar etiquetados
- [IoTWireless.3]AWSLas tareas de IoT FUOTA deben estar etiquetadas
- [IVS.1] Los pares de teclas de reproducción IVS deben estar etiquetados
- [IVS.2] Las configuraciones de grabación de IVS deben estar etiquetadas
- [IVS.3] Los canales IVS deben estar etiquetados
- [Keyspaces.1] Los espacios clave de Amazon Keyspaces deben estar etiquetados
- [MSK.3] Los conectores MSK Connect deben estar cifrados en tránsito
- [MSK.5] Los conectores MSK deben tener el registro activado
- [RDS.1] La instantánea de RDS debe ser privada
- [RDS.14] Los clústeres de Amazon Aurora deben tener habilitado el retroceso
- [RDS.31] Los grupos de seguridad de la base de datos de RDS deben etiquetarse
- [RedshiftServerless.1] Los grupos de trabajo sin servidor de Amazon Redshift deberían utilizar un enrutamiento de VPC mejorado
- [RedshiftServerless.2] Las conexiones a los grupos de trabajo sin servidor de Redshift deberían ser obligatorias para usar SSL
- [RedshiftServerless.3] Los grupos de trabajo sin servidor de Redshift deberían prohibir el acceso público
- [RedshiftServerless.4] Los espacios de nombres de Redshift Serverless deben cifrarse y administrarse por el clienteAWS KMS keys
- [RedshiftServerless.5] Los espacios de nombres Redshift Serverless no deben usar el nombre de usuario de administrador predeterminado

- [RedshiftServerless.6] Los espacios de nombres Redshift Serverless deberían exportar los registros a los registros CloudWatch
- [Route53.1] Los controles de salud de Route 53 deben estar etiquetados
- [Route53.2] Las zonas alojadas públicas de Route 53 deberían registrar las consultas de DNS
- [S3.24] Los puntos de Multi-Region acceso S3 deben tener habilitada la configuración de bloqueo del acceso público
- [S3.25] Los buckets de directorio de S3 deben tener configuraciones de ciclo de vida
- [SageMaker.9] las definiciones de trabajos de calidad de los SageMaker datos deben tener habilitado el cifrado del tráfico entre contenedores
- [SageMaker.10] Las definiciones de trabajos de explicabilidad del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores
- [SageMaker.11] las definiciones de trabajos SageMaker de calidad de los datos deben tener habilitado el aislamiento de red
- [SageMaker.12] las definiciones de trabajo basadas en el sesgo del SageMaker modelo deben tener habilitado el aislamiento de red
- [SageMaker.13] las definiciones de trabajos de calidad del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores
- [SageMaker.14] los programas SageMaker de monitoreo deben tener habilitado el aislamiento de la red
- [SageMaker.15] Las definiciones de trabajo basadas en el sesgo del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores
- [WAF.1]AWS WAFEl registro de ACL web global clásico debe estar habilitado
- [WAF.6]AWS WAFLas reglas globales clásicas deben tener al menos una condición
- [WAF.7]AWS WAFLos grupos de reglas globales clásicos deben tener al menos una regla
- [WAF.8]AWS WAFLas ACL web globales clásicas deben tener al menos una regla o grupo de reglas

Asia-Pacífico (Hong Kong)

Los siguientes controles no se admiten en la región Asia-Pacífico (Hong Kong).

- [AppFlow.1] AppFlow Los flujos de Amazon deben estar etiquetados
- [AppRunner.1] Los servicios de App Runner deben estar etiquetados

- [AppRunner.2] Los conectores VPC de App Runner deben estar etiquetados
- [AppSync.1]AWS AppSyncLas cachés de las API deben estar cifradas en reposo
- [AppSync.6]AWS AppSyncLas cachés de las API deben cifrarse en tránsito
- [BedrockAgentCore.1] Los AgentCore tiempos de ejecución de Bedrock deben configurarse con el modo de red VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways debería requerir autorización para las solicitudes entrantes
- [BedrockAgentCore.3] Bedrock AgentCore Memory debe estar cifrada y gestionada por el clienteAWS KMSclaves
- [BedrockAgentCore.4] Bedrock AgentCore Gateway debe cifrarse de forma que sea gestionada por el clienteAWS KMSclaves
- [BedrockAgentCore.5] Los navegadores AgentCore personalizados de Bedrock no deberían usar el modo de red pública
- [BedrockAgentCore.6] Los navegadores AgentCore personalizados de Bedrock deberían tener habilitada la grabación de sesiones
- [CloudFront.1] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado
- [CloudFront.3] CloudFront las distribuciones deben requerir el cifrado durante el tránsito
- [CloudFront.4] CloudFront las distribuciones deben tener configurada la conmutación por error de origen
- [CloudFront.5] CloudFront las distribuciones deben tener habilitado el registro
- [CloudFront.6] CloudFront las distribuciones deben tener WAF activado
- [CloudFront.7] CloudFront las distribuciones deben usar certificados personalizados SSL/TLS
- [CloudFront.8] CloudFront las distribuciones deben usar el SNI para atender las solicitudes HTTPS
- [CloudFront.9] CloudFront las distribuciones deben cifrar el tráfico para convertirlo en orígenes personalizados
- [CloudFront.10] CloudFront las distribuciones no deben usar protocolos SSL obsoletos entre ubicaciones de borde y orígenes personalizados
- [CloudFront.12] CloudFront las distribuciones no deben apuntar a orígenes de S3 inexistentes
- [CloudFront.13] CloudFront las distribuciones deben usar el control de acceso al origen
- [CloudFront.14] CloudFront las distribuciones deben estar etiquetadas

- [CloudFront.15] CloudFront las distribuciones deben usar la política de seguridad TLS recomendada
- [CloudFront.16] CloudFront las distribuciones deben usar el control de acceso de origen para los orígenes de las URL de las funciones de Lambda
- [CloudFront.17] CloudFront las distribuciones deben usar grupos de claves confiables para las URL y cookies firmadas
- [CodeArtifact.1] CodeArtifact los repositorios deben estar etiquetados
- [CodeGuruProfiler.1] Los grupos CodeGuru de creación de perfiles de Profiler deben estar etiquetados
- [CodeGuruReviewer.1] Las asociaciones de repositorios de CodeGuru Reviewer deben estar etiquetadas
- [Cognito.1] Los grupos de usuarios de Cognito deben tener activada la protección contra amenazas y el modo de aplicación con todas las funciones para la autenticación estándar
- [Connect.1] Los tipos de objetos de los perfiles de clientes de Amazon Connect deben estar etiquetados
- [Connect.2] Las instancias de Connect Customer deben tener el CloudWatch registro habilitado
- [DynamoDB.3] Los clústeres de DynamoDB Accelerator (DAX) deben cifrarse en reposo
- [DynamoDB.7] Los clústeres de DynamoDB Accelerator deben cifrarse en tránsito
- [EC2.24] No se deben utilizar los tipos de instancias paravirtuales de Amazon EC2
- [EC2.58] Las VPC deben configurarse con un punto final de interfaz para los contactos de Systems Manager Incident Manager
- [EC2.60] Las VPC deben configurarse con un punto final de interfaz para Systems Manager Incident Manager
- [EC2.173] Las solicitudes de EC2 Spot Fleet con parámetros de lanzamiento deberían permitir el cifrado de los volúmenes de EBS adjuntos
- [ECR.4] Los repositorios públicos de ECR deben etiquetarse
- [EventBridge.4] los puntos finales EventBridge globales deberían tener habilitada la replicación de eventos
- [FraudDetector.1] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.2] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas
- [FraudDetector.3] Los resultados de Amazon Fraud Detector deben estar etiquetados

- [FraudDetector.4] Las variables de Amazon Fraud Detector deben estar etiquetadas
- [GlobalAccelerator.1] Los aceleradores de Global Accelerator deben estar etiquetados
- [IAM.26] SSL/TLS Los certificados caducados gestionados en IAM deben eliminarse
- [Inspector.3] El escaneo de código Lambda de Amazon Inspector Lambda debe estar activado
- [IoTSiteWise.1]AWSLos modelos SiteWise de activos de IoT deben estar etiquetados
- [IoTSiteWise.2]AWS SiteWise Los paneles de IoT deben estar etiquetados
- [IoTSiteWise.3]AWS SiteWise Las pasarelas de IoT deben estar etiquetadas
- [IoTSiteWise.4]AWS SiteWise Los portales de IoT deben estar etiquetados
- [IoTSiteWise.5]AWS SiteWise Los proyectos de IoT deben estar etiquetados
- [IoTTwinMaker.1]AWSLos trabajos de TwinMaker sincronización de IoT deben estar etiquetados
- [IoTTwinMaker.2]AWS TwinMaker Los espacios de trabajo de IoT deben estar etiquetados
- [IoTTwinMaker.3]AWS TwinMaker Las escenas de IoT deben estar etiquetadas
- [IoTTwinMaker.4]AWS TwinMaker Las entidades de IoT deben estar etiquetadas
- [IoTWireless.1]AWSLos grupos de multidifusión de IoT Wireless deben estar etiquetados
- [IoTWireless.2]AWSLos perfiles de servicio de IoT Wireless deben estar etiquetados
- [IoTWireless.3]AWSLas tareas de IoT FUOTA deben estar etiquetadas
- [IVS.1] Los pares de teclas de reproducción IVS deben estar etiquetados
- [IVS.2] Las configuraciones de grabación de IVS deben estar etiquetadas
- [IVS.3] Los canales IVS deben estar etiquetados
- [MSK.3] Los conectores MSK Connect deben estar cifrados en tránsito
- [MSK.5] Los conectores MSK deben tener el registro activado
- [RDS.14] Los clústeres de Amazon Aurora deben tener habilitado el retroceso
- [RDS.31] Los grupos de seguridad de la base de datos de RDS deben etiquetarse
- [RedshiftServerless.1] Los grupos de trabajo sin servidor de Amazon Redshift deberían utilizar un enrutamiento de VPC mejorado
- [RedshiftServerless.2] Las conexiones a los grupos de trabajo sin servidor de Redshift deberían ser obligatorias para usar SSL
- [Route53.1] Los controles de salud de Route 53 deben estar etiquetados
- [Route53.2] Las zonas alojadas públicas de Route 53 deberían registrar las consultas de DNS

- [S3.24] Los puntos de Multi-Region acceso S3 deben tener habilitada la configuración de bloqueo del acceso público
- [S3.25] Los buckets de directorio de S3 deben tener configuraciones de ciclo de vida
- [SES.1] Las listas de contactos de SES deben estar etiquetadas
- [SES.2] Los conjuntos de configuración de SES deben estar etiquetados
- [SES.3] Los conjuntos de configuración de SES deben tener el TLS habilitado para enviar correos electrónicos
- [WAF.1]AWS WAFEl registro de ACL web global clásico debe estar habilitado
- [WAF.6]AWS WAFLas reglas globales clásicas deben tener al menos una condición
- [WAF.7]AWS WAFLos grupos de reglas globales clásicos deben tener al menos una regla
- [WAF.8]AWS WAFLas ACL web globales clásicas deben tener al menos una regla o grupo de reglas
- [WorkSpaces.1] los volúmenes de WorkSpaces usuarios deben cifrarse en reposo
- [WorkSpaces.2] los volúmenes WorkSpaces raíz deben cifrarse en reposo

Asia-Pacífico (Hyderabad)

Los siguientes controles no se admiten en la región Asia-Pacífico (Hyderabad).

- [Account.2]Cuentas de AWSdebe formar parte de unAWS Organizationsorganización
- [APIGateway.8] Las rutas de API Gateway deben especificar un tipo de autorización
- [APIGateway.9] El registro de acceso debe configurarse para las etapas V2 de API Gateway
- [Amplify.1] Las aplicaciones Amplify deben estar etiquetadas
- [Amplify.2] Amplify branches debe estar etiquetado
- [AppConfig.1]AWS AppConfiglas aplicaciones deben estar etiquetadas
- [AppConfig.2]AWS AppConfiglos perfiles de configuración deben estar etiquetados
- [AppConfig.3]AWS AppConfiglos entornos deben estar etiquetados
- [AppFlow.1] AppFlow Los flujos de Amazon deben estar etiquetados
- [AppRunner.1] Los servicios de App Runner deben estar etiquetados
- [AppRunner.2] Los conectores VPC de App Runner deben estar etiquetados
- [AppSync.1]AWS AppSyncLas cachés de las API deben estar cifradas en reposo

- [AppSync.6]AWS AppSyncLas cachés de las API deben cifrarse en tránsito
- [Backup.1]AWS Backuplos puntos de recuperación deben estar cifrados en reposo
- [BedrockAgentCore.1] Los AgentCore tiempos de ejecución de Bedrock deben configurarse con el modo de red VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways debería requerir autorización para las solicitudes entrantes
- [BedrockAgentCore.3] Bedrock AgentCore Memory debe estar cifrada y gestionada por el clienteAWS KMSclaves
- [BedrockAgentCore.4] Bedrock AgentCore Gateway debe cifrarse de forma que sea gestionada por el clienteAWS KMSclaves
- [BedrockAgentCore.5] Los navegadores AgentCore personalizados de Bedrock no deberían usar el modo de red pública
- [BedrockAgentCore.6] Los navegadores AgentCore personalizados de Bedrock deberían tener habilitada la grabación de sesiones
- [CloudFormation.3] las CloudFormation pilas deben tener habilitada la protección de terminación
- [CloudFormation.4] las CloudFormation pilas deben tener funciones de servicio asociadas
- [CloudFront.1] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado
- [CloudFront.3] CloudFront las distribuciones deben requerir el cifrado durante el tránsito
- [CloudFront.4] CloudFront las distribuciones deben tener configurada la conmutación por error de origen
- [CloudFront.5] CloudFront las distribuciones deben tener habilitado el registro
- [CloudFront.6] CloudFront las distribuciones deben tener WAF activado
- [CloudFront.7] CloudFront las distribuciones deben usar certificados personalizados SSL/TLS
- [CloudFront.8] CloudFront las distribuciones deben usar el SNI para atender las solicitudes HTTPS
- [CloudFront.9] CloudFront las distribuciones deben cifrar el tráfico para convertirlo en orígenes personalizados
- [CloudFront.10] CloudFront las distribuciones no deben usar protocolos SSL obsoletos entre ubicaciones de borde y orígenes personalizados
- [CloudFront.12] CloudFront las distribuciones no deben apuntar a orígenes de S3 inexistentes
- [CloudFront.13] CloudFront las distribuciones deben usar el control de acceso al origen

- [CloudFront.14] CloudFront las distribuciones deben estar etiquetadas
- [CloudFront.15] CloudFront las distribuciones deben usar la política de seguridad TLS recomendada
- [CloudFront.16] CloudFront las distribuciones deben usar el control de acceso de origen para los orígenes de las URL de las funciones de Lambda
- [CloudFront.17] CloudFront las distribuciones deben usar grupos de claves confiables para las URL y cookies firmadas
- [CloudTrail.6] Asegúrese de que el depósito de S3 que se utiliza para almacenar CloudTrail los registros no sea de acceso público
- [CloudTrail.7] Asegúrese de que el registro de acceso al bucket de S3 esté habilitado en el CloudTrail bucket de S3
- [CodeArtifact.1] CodeArtifact los repositorios deben estar etiquetados
- [CodeGuruProfiler.1] Los grupos CodeGuru de creación de perfiles de Profiler deben estar etiquetados
- [CodeGuruReviewer.1] Las asociaciones de repositorios de CodeGuru Reviewer deben estar etiquetadas
- [Cognito.1] Los grupos de usuarios de Cognito deben tener activada la protección contra amenazas y el modo de aplicación con todas las funciones para la autenticación estándar
- [Cognito.2] Los grupos de identidades de Cognito no deben permitir identidades no autenticadas
- [Connect.1] Los tipos de objetos de los perfiles de clientes de Amazon Connect deben estar etiquetados
- [Connect.2] Las instancias de Connect Customer deben tener el CloudWatch registro habilitado
- [Detective.1] Los gráficos de comportamiento de los detectives deben estar etiquetados
- [DMS.2] Los certificados DMS deben estar etiquetados
- [DMS.3] Las suscripciones a eventos de DMS deben estar etiquetadas
- [DMS.4] Las instancias de replicación de DMS deben estar etiquetadas
- [DMS.5] Los grupos de subredes de replicación del DMS deben estar etiquetados
- [DMS.6] Las instancias de replicación de DMS deben tener habilitada la actualización automática de las versiones secundarias
- [DMS.7] Las tareas de replicación del DMS para la base de datos de destino deben tener el registro habilitado

- [DMS.8] Las tareas de replicación del DMS para la base de datos de origen deben tener el registro activado
- [DMS.9] Los puntos finales del DMS deben usar SSL
- [DMS.10] Los puntos finales de DMS para las bases de datos de Neptune deben tener habilitada la autorización de IAM
- [DMS.11] Los puntos finales de DMS para MongoDB deben tener un mecanismo de autenticación habilitado
- [DMS.12] Los puntos finales de DMS para Redis OSS deben tener el TLS habilitado
- [DMS.13] Las instancias de replicación de DMS deben configurarse para usar varias zonas de disponibilidad
- [DynamoDB.3] Los clústeres de DynamoDB Accelerator (DAX) deben cifrarse en reposo
- [DynamoDB.7] Los clústeres de DynamoDB Accelerator deben cifrarse en tránsito
- [EC2.14] Los grupos de seguridad no deberían permitir la entrada desde la versión 0.0.0. 0/0 o: :/0 al puerto 3389
- [EC2.22] Deben eliminarse los grupos de seguridad de Amazon EC2 no utilizados
- [EC2.24] No se deben utilizar los tipos de instancias paravirtuales de Amazon EC2
- [EC2.25] Las plantillas de lanzamiento de Amazon EC2 no deben asignar direcciones IP públicas a las interfaces de red
- [EC2.34] Las tablas de rutas de la pasarela de tránsito EC2 deben estar etiquetadas
- [EC2.40] Las pasarelas NAT EC2 deben estar etiquetadas
- [EC2.51] Los puntos finales EC2 Client VPN deben tener habilitado el registro de conexiones de clientes
- [EC2.58] Las VPC deben configurarse con un punto final de interfaz para los contactos de Systems Manager Incident Manager
- [EC2.60] Las VPC deben configurarse con un punto final de interfaz para Systems Manager Incident Manager
- [EC2.170] Las plantillas de lanzamiento de EC2 deben utilizar la versión 2 del servicio de metadatos de instancias (IMDSv2)
- [EC2.173] Las solicitudes de EC2 Spot Fleet con parámetros de lanzamiento deberían permitir el cifrado de los volúmenes de EBS adjuntos
- [EC2.175] Las plantillas de lanzamiento de EC2 deben estar etiquetadas

- [EC2.177] Las sesiones de réplica de tráfico de EC2 deben etiquetarse
- [EC2.179] Los objetivos del espejo de tráfico de EC2 deben estar etiquetados
- [EC2.180] Las interfaces de red EC2 deberían tener habilitada source/destination la verificación
- [EC2.181] Las plantillas de lanzamiento de EC2 deberían permitir el cifrado de los volúmenes de EBS adjuntos
- [ECR.4] Los repositorios públicos de ECR deben etiquetarse
- [EFS.1] Elastic File System debe configurarse para cifrar los datos de los archivos en reposo mediante AWS KMS
- [EFS.2] Los volúmenes de Amazon EFS deben figurar en los planes de copia de seguridad
- [ELB.14] El balanceador de carga clásico debe configurarse con el modo defensivo o de mitigación de desincronización más estricto
- [ELB.17] Los balanceadores de cargas de aplicaciones y redes con oyentes deben usar las políticas de seguridad recomendadas
- [ELB.18] Los oyentes del balanceador de cargas de red y aplicaciones deben usar protocolos seguros para cifrar los datos en tránsito
- [ElastiCache.1] ElastiCache (Redis OSS) los clústeres deben tener habilitadas las copias de seguridad automáticas
- [ElastiCache.6] ElastiCache (Redis OSS) Los grupos de replicación de versiones anteriores deberían tener habilitada la autenticación de Redis OSS
- [ElastiCache.7] los ElastiCache clústeres no deben usar el grupo de subredes predeterminado
- [ElasticBeanstalk.1] Los entornos de Elastic Beanstalk deberían tener habilitados los informes de estado mejorados
- [ElasticBeanstalk.2] Las actualizaciones de la plataforma gestionada de Elastic Beanstalk deben estar habilitadas
- [ElasticBeanstalk.3] Elastic Beanstalk debería transmitir los registros a CloudWatch
- [EMR.1] Los nodos principales del clúster de Amazon EMR no deben tener direcciones IP públicas
- [ES.4] Debería estar habilitado el registro de errores de dominio de Elasticsearch en Logs CloudWatch
- [EventBridge.4] los puntos finales EventBridge globales deberían tener habilitada la replicación de eventos
- [FraudDetector.1] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados

- [FraudDetector.2] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas
- [FraudDetector.3] Los resultados de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.4] Las variables de Amazon Fraud Detector deben estar etiquetadas
- [GlobalAccelerator.1] Los aceleradores de Global Accelerator deben estar etiquetados
- [Glue.4]AWS GlueLos trabajos de Spark deberían ejecutarse en versiones compatibles deAWS Glue
- GuardDuty Los filtros [GuardDuty.2] deben estar etiquetados
- [IAM.1] Las políticas de IAM no deberían permitir todos los privilegios administrativos «*»
- [IAM.2] Los usuarios de IAM no deberían tener políticas de IAM adjuntas
- [IAM.3] Las claves de acceso de los usuarios de IAM deben rotarse cada 90 días o menos
- [IAM.5] La MFA debe estar habilitada para todos los usuarios de IAM que tengan una contraseña de consola
- [IAM.8] Se deben eliminar las credenciales de usuario de IAM no utilizadas
- [IAM.18] Asegúrese de que se haya creado una función de soporte para gestionar los incidentes conAWS Support
- [IAM.19] La MFA debe estar habilitada para todos los usuarios de IAM
- [IAM.21] Las políticas de IAM gestionadas por el cliente que cree no deberían permitir acciones comodín en los servicios
- [IAM.22] Se deben eliminar las credenciales de usuario de IAM que no se hayan utilizado durante 45 días
- [IAM.24] Las funciones de IAM deben estar etiquetadas
- [IAM.25] Los usuarios de IAM deben estar etiquetados
- [IAM.26] SSL/TLS Los certificados caducados gestionados en IAM deben eliminarse
- [IAM.27] Las identidades de IAM no deberían tener la AWSCloudShellFullAccess política adjunta
- [Inspector.1] El escaneo EC2 de Amazon Inspector debe estar activado
- [Inspector.2] El escaneo ECR de Amazon Inspector debe estar activado
- [Inspector.3] El escaneo de código Lambda de Amazon Inspector Lambda debe estar activado
- [Inspector.4] El escaneo estándar de Amazon Inspector Lambda debe estar activado
- [IoT.1]AWS IoT Device Defenderlos perfiles de seguridad deben estar etiquetados
- [IoT.2]AWS IoT Corelas acciones de mitigación deben estar etiquetadas

- [IoT.3]AWS IoT Corelas dimensiones deben estar etiquetadas
- [IoT.4]AWS IoT Corelos autorizadores deben estar etiquetados
- [IoT.5]AWS IoT CoreLos alias de los roles deben estar etiquetados
- [IoT.6]AWS IoT Corelas políticas deben estar etiquetadas
- [IoTSiteWise.1]AWSLos modelos SiteWise de activos de IoT deben estar etiquetados
- [IoTSiteWise.2]AWS SiteWise Los paneles de IoT deben estar etiquetados
- [IoTSiteWise.3]AWS SiteWise Las pasarelas de IoT deben estar etiquetadas
- [IoTSiteWise.4]AWS SiteWise Los portales de IoT deben estar etiquetados
- [IoTSiteWise.5]AWS SiteWise Los proyectos de IoT deben estar etiquetados
- [IoTTwinMaker.1]AWSLos trabajos de TwinMaker sincronización de IoT deben estar etiquetados
- [IoTTwinMaker.2]AWS TwinMaker Los espacios de trabajo de IoT deben estar etiquetados
- [IoTTwinMaker.3]AWS TwinMaker Las escenas de IoT deben estar etiquetadas
- [IoTTwinMaker.4]AWS TwinMaker Las entidades de IoT deben estar etiquetadas
- [IoTWireless.1]AWSLos grupos de multidifusión de IoT Wireless deben estar etiquetados
- [IoTWireless.2]AWSLos perfiles de servicio de IoT Wireless deben estar etiquetados
- [IoTWireless.3]AWSLas tareas de IoT FUOTA deben estar etiquetadas
- [IVS.1] Los pares de teclas de reproducción IVS deben estar etiquetados
- [IVS.2] Las configuraciones de grabación de IVS deben estar etiquetadas
- [IVS.3] Los canales IVS deben estar etiquetados
- [Keyspaces.1] Los espacios clave de Amazon Keyspaces deben estar etiquetados
- [KMS.1] Las políticas gestionadas por los clientes de IAM no deberían permitir acciones de descifrado en todas las claves de KMS
- [KMS.2] Los directores de IAM no deberían tener políticas integradas de IAM que permitan realizar acciones de descifrado en todas las claves de KMS
- [Lambda.7] Las funciones de Lambda deberían tener AWS X-Ray el rastreo activo está habilitado
- [Macie.1] Amazon Macie debería estar activado
- [Macie.2] La detección automática de datos confidenciales por parte de Macie debería estar habilitada
- [MQ.2] Los corredores de ActiveMQ deben transmitir los registros de auditoría a CloudWatch
- [MQ.4] Los corredores de Amazon MQ deben estar etiquetados

- [MQ.5] Los corredores de ActiveMQ deberían usar el modo de implementación active/standby
- [MQ.6] Los corredores de RabbitMQ deberían usar el modo de despliegue de clústeres
- [MSK.3] Los conectores MSK Connect deben estar cifrados en tránsito
- [MSK.4] Los clústeres de MSK deben tener el acceso público deshabilitado
- [MSK.5] Los conectores MSK deben tener el registro activado
- [MSK.6] Los clústeres de MSK deberían deshabilitar el acceso no autenticado
- [Neptune.1] Los clústeres de bases de datos de Neptune deben cifrarse en reposo
- [Neptune.2] Los clústeres de bases de datos de Neptune deberían publicar registros de auditoría en Logs CloudWatch
- [Neptune.3] Las instantáneas del clúster de base de datos de Neptune no deben ser públicas
- [Neptune.4] Los clústeres de base de datos de Neptune deben tener habilitada la protección contra eliminación
- [Neptune.5] Los clústeres de Neptune DB deberían tener habilitadas las copias de seguridad automatizadas
- [Neptune.6] Las instantáneas del clúster de base de datos de Neptune deben cifrarse en reposo
- [Neptune.7] Los clústeres de base de datos de Neptune deben tener habilitada la autenticación de bases de datos de IAM
- [Neptune.8] Los clústeres de bases de datos de Neptune deben configurarse para copiar etiquetas a las instantáneas
- [Neptune.9] Los clústeres de base de datos Neptune deben implementarse en varias zonas de disponibilidad
- [Opensearch.1] OpenSearch los dominios deben tener activado el cifrado en reposo
- [Opensearch.2] OpenSearch los dominios no deben ser de acceso público
- [Opensearch.3] OpenSearch los dominios deben cifrar los datos enviados entre nodos
- [Opensearch.4] El registro de errores de OpenSearch dominio en Logs debe estar habilitado CloudWatch
- [Opensearch.5] OpenSearch los dominios deben tener activado el registro de auditoría
- [Opensearch.6] OpenSearch los dominios deben tener al menos tres nodos de datos
- [Opensearch.7] OpenSearch los dominios deben tener habilitado un control de acceso detallado
- [Opensearch.8] Las conexiones a los OpenSearch dominios deben cifrarse con la última política de seguridad de TLS

- [Opensearch.9] OpenSearch los dominios deben estar etiquetados
- [Opensearch.10] OpenSearch los dominios deben tener instalada la última actualización de software
- [Opensearch.11] OpenSearch los dominios deben tener al menos tres nodos principales dedicados
- [RDS.14] Los clústeres de Amazon Aurora deben tener habilitado el retroceso
- [RDS.31] Los grupos de seguridad de la base de datos de RDS deben etiquetarse
- [RDS.35] Los clústeres de bases de datos de RDS deben tener habilitada la actualización automática de versiones secundarias
- [RDS.37] Los clústeres de bases de datos de Aurora PostgreSQL deben publicar los registros en Logs CloudWatch
- [Redshift.10] Los clústeres de Redshift deben cifrarse en reposo
- [Redshift.18] Los clústeres de Redshift deberían tener Multi-AZ las implementaciones habilitadas
- [RedshiftServerless.1] Los grupos de trabajo sin servidor de Amazon Redshift deberían utilizar un enrutamiento de VPC mejorado
- [RedshiftServerless.2] Las conexiones a los grupos de trabajo sin servidor de Redshift deberían ser obligatorias para usar SSL
- [RedshiftServerless.3] Los grupos de trabajo sin servidor de Redshift deberían prohibir el acceso público
- [RedshiftServerless.4] Los espacios de nombres de Redshift Serverless deben cifrarse y administrarse por el clienteAWS KMS keys
- [RedshiftServerless.5] Los espacios de nombres Redshift Serverless no deben usar el nombre de usuario de administrador predeterminado
- [RedshiftServerless.6] Los espacios de nombres Redshift Serverless deberían exportar los registros a los registros CloudWatch
- [Route53.1] Los controles de salud de Route 53 deben estar etiquetados
- [Route53.2] Las zonas alojadas públicas de Route 53 deberían registrar las consultas de DNS
- [S3.24] Los puntos de Multi-Region acceso S3 deben tener habilitada la configuración de bloqueo del acceso público
- [S3.25] Los buckets de directorio de S3 deben tener configuraciones de ciclo de vida
- [SageMaker.1] Las instancias de Amazon SageMaker Notebook no deberían tener acceso directo a Internet

- [SageMaker.2] las instancias de SageMaker cuadernos deben lanzarse en una VPC personalizada
- [SageMaker.3] Los usuarios no deben tener acceso root a las instancias de los SageMaker cuadernos
- SageMaker Los modelos [SageMaker.5] deben tener habilitado el aislamiento de red
- [SageMaker.6] las configuraciones de imagen de la SageMaker aplicación deben estar etiquetadas
- [SageMaker.7] SageMaker las imágenes deben estar etiquetadas
- [SageMaker.9] las definiciones de trabajos de calidad de los SageMaker datos deben tener habilitado el cifrado del tráfico entre contenedores
- [SageMaker.10] Las definiciones de trabajos de explicabilidad del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores
- [SageMaker.11] las definiciones de trabajos SageMaker de calidad de los datos deben tener habilitado el aislamiento de red
- [SageMaker.12] las definiciones de trabajo basadas en el sesgo del SageMaker modelo deben tener habilitado el aislamiento de red
- [SageMaker.13] las definiciones de trabajos de calidad del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores
- [SageMaker.14] los programas SageMaker de monitoreo deben tener habilitado el aislamiento de la red
- [SageMaker.15] Las definiciones de trabajo basadas en el sesgo del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores
- SageMaker Los modelos [SageMaker.16] deben usar un registro privado en la VPC para los contenedores principales
- [SageMaker.17] SageMaker Las tiendas offline de los grupos de funciones deben cifrarse con AWS KMS claves
- [SageMaker.18] las tiendas en línea de grupos de SageMaker funciones con almacenamiento estándar deben cifrarse con AWS KMS claves
- [SageMaker.19] SageMaker los modelos deben usar un registro privado en la VPC para las canalizaciones de inferencia de varios contenedores
- [SES.3] Los conjuntos de configuración de SES deben tener el TLS habilitado para enviar correos electrónicos
- [SQS.1] Las colas de Amazon SQS deben cifrarse en reposo
- [SQS.2] Las colas de SQS deben estar etiquetadas

- [SQS.3] Las políticas de acceso a las colas de SQS no deberían permitir el acceso público
- [SSM.6] SSM Automation debería tener el registro habilitado CloudWatch
- [SSM.7] Los documentos SSM deben tener habilitada la configuración de bloqueo para compartir en público
- [Transfer.3] Los conectores Transfer Family deben tener habilitado el registro
- [Transfer.4] Los acuerdos Transfer Family deben estar etiquetados
- [WAF.1]AWS WAFEl registro de ACL web global clásico debe estar habilitado
- [WAF.3]AWS WAFLos grupos de reglas regionales clásicos deben tener al menos una regla
- [WAF.6]AWS WAFLas reglas globales clásicas deben tener al menos una condición
- [WAF.7]AWS WAFLos grupos de reglas globales clásicos deben tener al menos una regla
- [WAF.8]AWS WAFLas ACL web globales clásicas deben tener al menos una regla o grupo de reglas
- [WAF.10]AWS WAFLas ACL web deben tener al menos una regla o grupo de reglas
- [WorkSpaces.1] los volúmenes de WorkSpaces usuarios deben cifrarse en reposo
- [WorkSpaces.2] los volúmenes WorkSpaces raíz deben cifrarse en reposo

Asia-Pacífico (Yakarta)

Los siguientes controles no se admiten en la región Asia-Pacífico (Yakarta).

- [Account.2]Cuentas de AWSdebe formar parte de unAWS Organizationsorganización
- [APIGateway.8] Las rutas de API Gateway deben especificar un tipo de autorización
- [APIGateway.9] El registro de acceso debe configurarse para las etapas V2 de API Gateway
- [Amplify.1] Las aplicaciones Amplify deben estar etiquetadas
- [Amplify.2] Amplify branches debe estar etiquetado
- [AppFlow.1] AppFlow Los flujos de Amazon deben estar etiquetados
- [AppRunner.1] Los servicios de App Runner deben estar etiquetados
- [AppRunner.2] Los conectores VPC de App Runner deben estar etiquetados
- [AppSync.1]AWS AppSyncLas cachés de las API deben estar cifradas en reposo
- [AppSync.6]AWS AppSyncLas cachés de las API deben cifrarse en tránsito
- [Backup.1]AWS Backuplos puntos de recuperación deben estar cifrados en reposo

- [BedrockAgentCore.1] Los AgentCore tiempos de ejecución de Bedrock deben configurarse con el modo de red VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways debería requerir autorización para las solicitudes entrantes
- [BedrockAgentCore.3] Bedrock AgentCore Memory debe estar cifrada y gestionada por el clienteAWS KMSclaves
- [BedrockAgentCore.4] Bedrock AgentCore Gateway debe cifrarse de forma que sea gestionada por el clienteAWS KMSclaves
- [BedrockAgentCore.5] Los navegadores AgentCore personalizados de Bedrock no deberían usar el modo de red pública
- [BedrockAgentCore.6] Los navegadores AgentCore personalizados de Bedrock deberían tener habilitada la grabación de sesiones
- [CloudFormation.3] las CloudFormation pilas deben tener habilitada la protección de terminación
- [CloudFormation.4] las CloudFormation pilas deben tener funciones de servicio asociadas
- [CloudFront.1] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado
- [CloudFront.3] CloudFront las distribuciones deben requerir el cifrado durante el tránsito
- [CloudFront.4] CloudFront las distribuciones deben tener configurada la conmutación por error de origen
- [CloudFront.5] CloudFront las distribuciones deben tener habilitado el registro
- [CloudFront.6] CloudFront las distribuciones deben tener WAF activado
- [CloudFront.7] CloudFront las distribuciones deben usar certificados personalizados SSL/TLS
- [CloudFront.8] CloudFront las distribuciones deben usar el SNI para atender las solicitudes HTTPS
- [CloudFront.9] CloudFront las distribuciones deben cifrar el tráfico para convertirlo en orígenes personalizados
- [CloudFront.10] CloudFront las distribuciones no deben usar protocolos SSL obsoletos entre ubicaciones de borde y orígenes personalizados
- [CloudFront.12] CloudFront las distribuciones no deben apuntar a orígenes de S3 inexistentes
- [CloudFront.13] CloudFront las distribuciones deben usar el control de acceso al origen
- [CloudFront.14] CloudFront las distribuciones deben estar etiquetadas
- [CloudFront.15] CloudFront las distribuciones deben usar la política de seguridad TLS recomendada

- [CloudFront.16] CloudFront las distribuciones deben usar el control de acceso de origen para los orígenes de las URL de las funciones de Lambda
- [CloudFront.17] CloudFront las distribuciones deben usar grupos de claves confiables para las URL y cookies firmadas
- [CodeArtifact.1] CodeArtifact los repositorios deben estar etiquetados
- [CodeBuild.1] Las URL del repositorio fuente de CodeBuild Bitbucket no deben contener credenciales confidenciales
- [CodeBuild.2] las variables de entorno CodeBuild del proyecto no deben contener credenciales de texto claro
- [CodeBuild.3] Los registros de CodeBuild S3 deben estar cifrados
- [CodeBuild.4] los entornos de CodeBuild proyectos deben tener un registroAWS ConfigDuración
- [CodeGuruProfiler.1] Los grupos CodeGuru de creación de perfiles de Profiler deben estar etiquetados
- [CodeGuruReviewer.1] Las asociaciones de repositorios de CodeGuru Reviewer deben estar etiquetadas
- [Cognito.1] Los grupos de usuarios de Cognito deben tener activada la protección contra amenazas y el modo de aplicación con todas las funciones para la autenticación estándar
- [Connect.1] Los tipos de objetos de los perfiles de clientes de Amazon Connect deben estar etiquetados
- [Connect.2] Las instancias de Connect Customer deben tener el CloudWatch registro habilitado
- [Detective.1] Los gráficos de comportamiento de los detectives deben estar etiquetados
- [DMS.2] Los certificados DMS deben estar etiquetados
- [DMS.3] Las suscripciones a eventos de DMS deben estar etiquetadas
- [DMS.4] Las instancias de replicación de DMS deben estar etiquetadas
- [DMS.5] Los grupos de subredes de replicación del DMS deben estar etiquetados
- [DMS.6] Las instancias de replicación de DMS deben tener habilitada la actualización automática de las versiones secundarias
- [DMS.7] Las tareas de replicación del DMS para la base de datos de destino deben tener el registro habilitado
- [DMS.8] Las tareas de replicación del DMS para la base de datos de origen deben tener el registro activado

- [DMS.9] Los puntos finales del DMS deben usar SSL
- [DMS.10] Los puntos finales de DMS para las bases de datos de Neptune deben tener habilitada la autorización de IAM
- [DMS.11] Los puntos finales de DMS para MongoDB deben tener un mecanismo de autenticación habilitado
- [DMS.12] Los puntos finales de DMS para Redis OSS deben tener el TLS habilitado
- [DMS.13] Las instancias de replicación de DMS deben configurarse para usar varias zonas de disponibilidad
- [DocumentDB.1] Los clústeres de Amazon DocumentDB deben cifrarse en reposo
- [DocumentDB.2] Los clústeres de Amazon DocumentDB deben tener un período de retención de copias de seguridad adecuado
- [DocumentDB.3] Las instantáneas de clústeres manuales de Amazon DocumentDB no deben ser públicas
- [DocumentDB.4] Los clústeres de Amazon DocumentDB deben publicar los registros de auditoría en Logs CloudWatch
- [DocumentDB.5] Los clústeres de Amazon DocumentDB deben tener habilitada la protección contra eliminaciones
- [DocumentDB.6] Los clústeres de Amazon DocumentDB deben cifrarse en tránsito
- [DynamoDB.3] Los clústeres de DynamoDB Accelerator (DAX) deben cifrarse en reposo
- [DynamoDB.7] Los clústeres de DynamoDB Accelerator deben cifrarse en tránsito
- [EC2.14] Los grupos de seguridad no deberían permitir la entrada desde la versión 0.0.0. 0/0 o: :/0 al puerto 3389
- [EC2.22] Deben eliminarse los grupos de seguridad de Amazon EC2 no utilizados
- [EC2.24] No se deben utilizar los tipos de instancias paravirtuales de Amazon EC2
- [EC2.51] Los puntos finales EC2 Client VPN deben tener habilitado el registro de conexiones de clientes
- [EC2.58] Las VPC deben configurarse con un punto final de interfaz para los contactos de Systems Manager Incident Manager
- [EC2.60] Las VPC deben configurarse con un punto final de interfaz para Systems Manager Incident Manager
- [EC2.173] Las solicitudes de EC2 Spot Fleet con parámetros de lanzamiento deberían permitir el cifrado de los volúmenes de EBS adjuntos

- [EC2.177] Las sesiones de réplica de tráfico de EC2 deben etiquetarse
- [EC2.179] Los objetivos del espejo de tráfico de EC2 deben estar etiquetados
- [ECR.4] Los repositorios públicos de ECR deben etiquetarse
- [EFS.1] Elastic File System debe configurarse para cifrar los datos de los archivos en reposo mediante AWS KMS
- [EFS.2] Los volúmenes de Amazon EFS deben figurar en los planes de copia de seguridad
- [ELB.17] Los balanceadores de cargas de aplicaciones y redes con oyentes deben usar las políticas de seguridad recomendadas
- [ELB.18] Los oyentes del balanceador de cargas de red y aplicaciones deben usar protocolos seguros para cifrar los datos en tránsito
- [ElastiCache.1] ElastiCache (Redis OSS) los clústeres deben tener habilitadas las copias de seguridad automáticas
- [ElastiCache.6] ElastiCache (Redis OSS) Los grupos de replicación de versiones anteriores deberían tener habilitada la autenticación de Redis OSS
- [ElastiCache.7] los ElastiCache clústeres no deben usar el grupo de subredes predeterminado
- [ElasticBeanstalk.1] Los entornos de Elastic Beanstalk deberían tener habilitados los informes de estado mejorados
- [EventBridge.4] los puntos finales EventBridge globales deberían tener habilitada la replicación de eventos
- [FraudDetector.1] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.2] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas
- [FraudDetector.3] Los resultados de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.4] Las variables de Amazon Fraud Detector deben estar etiquetadas
- [GlobalAccelerator.1] Los aceleradores de Global Accelerator deben estar etiquetados
- GuardDuty Los filtros [GuardDuty.2] deben estar etiquetados
- [IAM.18] Asegúrese de que se haya creado una función de soporte para gestionar los incidentes conAWS Support
- [IAM.26] SSL/TLS Los certificados caducados gestionados en IAM deben eliminarse
- [Inspector.3] El escaneo de código Lambda de Amazon Inspector Lambda debe estar activado
- [IoT.1]AWS IoT Device Defenderlos perfiles de seguridad deben estar etiquetados
- [IoT.2]AWS IoT Corelas acciones de mitigación deben estar etiquetadas

- [IoT.3]AWS IoT Corelas dimensiones deben estar etiquetadas
- [IoT.4]AWS IoT Corelos autorizadores deben estar etiquetados
- [IoT.5]AWS IoT CoreLos alias de los roles deben estar etiquetados
- [IoT.6]AWS IoT Corelas políticas deben estar etiquetadas
- [IoTSiteWise.1]AWSLos modelos SiteWise de activos de IoT deben estar etiquetados
- [IoTSiteWise.2]AWS SiteWise Los paneles de IoT deben estar etiquetados
- [IoTSiteWise.3]AWS SiteWise Las pasarelas de IoT deben estar etiquetadas
- [IoTSiteWise.4]AWS SiteWise Los portales de IoT deben estar etiquetados
- [IoTSiteWise.5]AWS SiteWise Los proyectos de IoT deben estar etiquetados
- [IoTTwinMaker.1]AWSLos trabajos de TwinMaker sincronización de IoT deben estar etiquetados
- [IoTTwinMaker.2]AWS TwinMaker Los espacios de trabajo de IoT deben estar etiquetados
- [IoTTwinMaker.3]AWS TwinMaker Las escenas de IoT deben estar etiquetadas
- [IoTTwinMaker.4]AWS TwinMaker Las entidades de IoT deben estar etiquetadas
- [IoTWireless.1]AWSLos grupos de multidifusión de IoT Wireless deben estar etiquetados
- [IoTWireless.2]AWSLos perfiles de servicio de IoT Wireless deben estar etiquetados
- [IoTWireless.3]AWSLas tareas de IoT FUOTA deben estar etiquetadas
- [IVS.1] Los pares de teclas de reproducción IVS deben estar etiquetados
- [IVS.2] Las configuraciones de grabación de IVS deben estar etiquetadas
- [IVS.3] Los canales IVS deben estar etiquetados
- [Keyspaces.1] Los espacios clave de Amazon Keyspaces deben estar etiquetados
- [Macie.1] Amazon Macie debería estar activado
- [Macie.2] La detección automática de datos confidenciales por parte de Macie debería estar habilitada
- [MSK.3] Los conectores MSK Connect deben estar cifrados en tránsito
- [MSK.5] Los conectores MSK deben tener el registro activado
- [Neptune.1] Los clústeres de bases de datos de Neptune deben cifrarse en reposo
- [Neptune.2] Los clústeres de bases de datos de Neptune deberían publicar registros de auditoría en Logs CloudWatch
- [Neptune.3] Las instantáneas del clúster de base de datos de Neptune no deben ser públicas

- [Neptune.4] Los clústeres de base de datos de Neptune deben tener habilitada la protección contra eliminación
- [Neptune.5] Los clústeres de Neptune DB deberían tener habilitadas las copias de seguridad automatizadas
- [Neptune.6] Las instantáneas del clúster de base de datos de Neptune deben cifrarse en reposo
- [Neptune.7] Los clústeres de base de datos de Neptune deben tener habilitada la autenticación de bases de datos de IAM
- [Neptune.8] Los clústeres de bases de datos de Neptune deben configurarse para copiar etiquetas a las instantáneas
- [Neptune.9] Los clústeres de base de datos Neptune deben implementarse en varias zonas de disponibilidad
- [Opensearch.5] OpenSearch los dominios deben tener activado el registro de auditoría
- [Opensearch.6] OpenSearch los dominios deben tener al menos tres nodos de datos
- [RDS.14] Los clústeres de Amazon Aurora deben tener habilitado el retroceso
- [RDS.31] Los grupos de seguridad de la base de datos de RDS deben etiquetarse
- [RedshiftServerless.1] Los grupos de trabajo sin servidor de Amazon Redshift deberían utilizar un enrutamiento de VPC mejorado
- [RedshiftServerless.2] Las conexiones a los grupos de trabajo sin servidor de Redshift deberían ser obligatorias para usar SSL
- [Route53.1] Los controles de salud de Route 53 deben estar etiquetados
- [Route53.2] Las zonas alojadas públicas de Route 53 deberían registrar las consultas de DNS
- [S3.11] Los cubos de uso general de S3 deben tener habilitadas las notificaciones de eventos
- [S3.24] Los puntos de Multi-Region acceso S3 deben tener habilitada la configuración de bloqueo del acceso público
- [S3.25] Los buckets de directorio de S3 deben tener configuraciones de ciclo de vida
- [SageMaker.9] las definiciones de trabajos de calidad de los SageMaker datos deben tener habilitado el cifrado del tráfico entre contenedores
- [SageMaker.10] Las definiciones de trabajos de explicabilidad del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores
- [SageMaker.11] las definiciones de trabajos SageMaker de calidad de los datos deben tener habilitado el aislamiento de red

- [SageMaker.12] las definiciones de trabajo basadas en el sesgo del SageMaker modelo deben tener habilitado el aislamiento de red
- [SageMaker.13] las definiciones de trabajos de calidad del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores
- [SageMaker.14] los programas SageMaker de monitoreo deben tener habilitado el aislamiento de la red
- [SageMaker.15] Las definiciones de trabajo basadas en el sesgo del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores
- SageMaker Los modelos [SageMaker.16] deben usar un registro privado en la VPC para los contenedores principales
- [SageMaker.19] SageMaker los modelos deben usar un registro privado en la VPC para las canalizaciones de inferencia de varios contenedores
- [ServiceCatalog.1] Las carteras de Service Catalog deben compartirse dentro de unAWSsolo una organización
- [SQS.1] Las colas de Amazon SQS deben cifrarse en reposo
- [SQS.2] Las colas de SQS deben estar etiquetadas
- [SQS.3] Las políticas de acceso a las colas de SQS no deberían permitir el acceso público
- [WAF.1]AWS WAFEl registro de ACL web global clásico debe estar habilitado
- [WAF.3]AWS WAFLos grupos de reglas regionales clásicos deben tener al menos una regla
- [WAF.6]AWS WAFLas reglas globales clásicas deben tener al menos una condición
- [WAF.7]AWS WAFLos grupos de reglas globales clásicos deben tener al menos una regla
- [WAF.8]AWS WAFLas ACL web globales clásicas deben tener al menos una regla o grupo de reglas
- [WAF.10]AWS WAFLas ACL web deben tener al menos una regla o grupo de reglas
- [WorkSpaces.1] los volúmenes de WorkSpaces usuarios deben cifrarse en reposo
- [WorkSpaces.2] los volúmenes WorkSpaces raíz deben cifrarse en reposo

Asia-Pacífico (Malasia)

Los siguientes controles no se admiten en la región Asia-Pacífico (Malasia).

- [ACM.1] ACM-issued Los certificados importados y renovados deben renovarse después de un período de tiempo específico

- [ACM.2] Los certificados RSA gestionados por ACM deben utilizar una longitud de clave de al menos 2048 bits
- [Account.1] La información de contacto de seguridad debe proporcionarse para unCuenta de AWS
- [Account.2]Cuentas de AWSdebe formar parte de unAWS Organizationsorganización
- [APIGateway.8] Las rutas de API Gateway deben especificar un tipo de autorización
- [APIGateway.9] El registro de acceso debe configurarse para las etapas V2 de API Gateway
- [Amplify.1] Las aplicaciones Amplify deben estar etiquetadas
- [Amplify.2] Amplify branches debe estar etiquetado
- [AppConfig.1]AWS AppConfiglas aplicaciones deben estar etiquetadas
- [AppConfig.2]AWS AppConfiglos perfiles de configuración deben estar etiquetados
- [AppConfig.3]AWS AppConfiglos entornos deben estar etiquetados
- [AppConfig.4]AWS AppConfiglas asociaciones de extensiones deben estar etiquetadas
- [AppFlow.1] AppFlow Los flujos de Amazon deben estar etiquetados
- [AppRunner.1] Los servicios de App Runner deben estar etiquetados
- [AppRunner.2] Los conectores VPC de App Runner deben estar etiquetados
- [AppSync.1]AWS AppSyncLas cachés de las API deben estar cifradas en reposo
- [AppSync.2]AWS AppSyncdebe tener habilitado el registro a nivel de campo
- [AppSync.5]AWS AppSyncLas API de GraphQL no deben autenticarse con claves de API
- [AppSync.6]AWS AppSyncLas cachés de las API deben cifrarse en tránsito
- [Athena.4] Los grupos de trabajo de Athena deberían tener habilitado el registro
- [AutoScaling.2] El grupo Amazon EC2 Auto Scaling debe cubrir varias zonas de disponibilidad
- [AutoScaling.3] Las configuraciones de lanzamiento grupal de Auto Scaling deberían configurar las instancias EC2 para que requieran la versión 2 del Servicio de Metadatos de Instancia (IMDSv2)
- [AutoScaling.6] Los grupos de Auto Scaling deben usar varios tipos de instancias en múltiples zonas de disponibilidad
- [AutoScaling.9] Los grupos de Amazon EC2 Auto Scaling deben utilizar las plantillas de lanzamiento de Amazon EC2
- [Backup.1]AWS Backuplos puntos de recuperación deben estar cifrados en reposo
- [Backup.2]AWS Backuplos puntos de recuperación deben estar etiquetados

- [Backup.4]AWS Backuplos planes de informes deben estar etiquetados
- [Batch.1] Las colas de trabajos por lotes deben estar etiquetadas
- [Batch.2] Las políticas de programación de lotes deben estar etiquetadas
- [Batch.3] Los entornos de procesamiento por lotes deben etiquetarse
- [Batch.4] Las propiedades de los recursos de cómputo en los entornos de cómputo por lotes gestionados deben estar etiquetadas
- [BedrockAgentCore.1] Los AgentCore tiempos de ejecución de Bedrock deben configurarse con el modo de red VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways debería requerir autorización para las solicitudes entrantes
- [BedrockAgentCore.3] Bedrock AgentCore Memory debe estar cifrada y gestionada por el clienteAWS KMSclaves
- [BedrockAgentCore.4] Bedrock AgentCore Gateway debe cifrarse de forma que sea gestionada por el clienteAWS KMSclaves
- [BedrockAgentCore.5] Los navegadores AgentCore personalizados de Bedrock no deberían usar el modo de red pública
- [BedrockAgentCore.6] Los navegadores AgentCore personalizados de Bedrock deberían tener habilitada la grabación de sesiones
- [CloudFormation.3] las CloudFormation pilas deben tener habilitada la protección de terminación
- [CloudFormation.4] las CloudFormation pilas deben tener funciones de servicio asociadas
- [CloudFront.1] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado
- [CloudFront.3] CloudFront las distribuciones deben requerir el cifrado durante el tránsito
- [CloudFront.4] CloudFront las distribuciones deben tener configurada la conmutación por error de origen
- [CloudFront.5] CloudFront las distribuciones deben tener habilitado el registro
- [CloudFront.6] CloudFront las distribuciones deben tener WAF activado
- [CloudFront.7] CloudFront las distribuciones deben usar certificados personalizados SSL/TLS
- [CloudFront.8] CloudFront las distribuciones deben usar el SNI para atender las solicitudes HTTPS
- [CloudFront.9] CloudFront las distribuciones deben cifrar el tráfico para convertirlo en orígenes personalizados

- [CloudFront.10] CloudFront las distribuciones no deben usar protocolos SSL obsoletos entre ubicaciones de borde y orígenes personalizados
- [CloudFront.12] CloudFront las distribuciones no deben apuntar a orígenes de S3 inexistentes
- [CloudFront.13] CloudFront las distribuciones deben usar el control de acceso al origen
- [CloudFront.14] CloudFront las distribuciones deben estar etiquetadas
- [CloudFront.15] CloudFront las distribuciones deben usar la política de seguridad TLS recomendada
- [CloudFront.16] CloudFront las distribuciones deben usar el control de acceso de origen para los orígenes de las URL de las funciones de Lambda
- [CloudFront.17] CloudFront las distribuciones deben usar grupos de claves confiables para las URL y cookies firmadas
- [CloudTrail.6] Asegúrese de que el depósito de S3 que se utiliza para almacenar CloudTrail los registros no sea de acceso público
- [CloudTrail.7] Asegúrese de que el registro de acceso al bucket de S3 esté habilitado en el CloudTrail bucket de S3
- [CloudTrail.10] Los almacenes de datos de eventos de CloudTrail Lake deben estar cifrados y gestionados por el clienteAWS KMS keys
- [CloudWatch.17] las acciones CloudWatch de alarma deben estar activadas
- [CodeArtifact.1] CodeArtifact los repositorios deben estar etiquetados
- [CodeBuild.1] Las URL del repositorio fuente de CodeBuild Bitbucket no deben contener credenciales confidenciales
- [CodeBuild.2] las variables de entorno CodeBuild del proyecto no deben contener credenciales de texto claro
- [CodeBuild.3] Los registros de CodeBuild S3 deben estar cifrados
- [CodeBuild.4] los entornos de CodeBuild proyectos deben tener un registroAWS ConfigDuración
- [CodeBuild.7] las exportaciones de grupos de CodeBuild informes deben cifrarse en reposo
- [CodeGuruProfiler.1] Los grupos CodeGuru de creación de perfiles de Profiler deben estar etiquetados
- [CodeGuruReviewer.1] Las asociaciones de repositorios de CodeGuru Reviewer deben estar etiquetadas
- [Cognito.1] Los grupos de usuarios de Cognito deben tener activada la protección contra amenazas y el modo de aplicación con todas las funciones para la autenticación estándar

- [Cognito.2] Los grupos de identidades de Cognito no deben permitir identidades no autenticadas
- [Cognito.3] Las políticas de contraseñas para los grupos de usuarios de Cognito deben tener configuraciones sólidas
- [Cognito.4] Los grupos de usuarios de Cognito deben tener activada la protección contra amenazas y el modo de aplicación con todas las funciones para la autenticación personalizada
- [Cognito.5] La MFA debe estar habilitada para los grupos de usuarios de Cognito
- [Cognito.6] Los grupos de usuarios de Cognito deben tener habilitada la protección contra la eliminación
- [Connect.1] Los tipos de objetos de los perfiles de clientes de Amazon Connect deben estar etiquetados
- [Connect.2] Las instancias de Connect Customer deben tener el CloudWatch registro habilitado
- [DataFirehose.1] Los flujos de entrega de Firehose deben cifrarse en reposo
- [DataSync.1] DataSync las tareas deberían tener el registro activado
- [DataSync.2] DataSync las tareas deben estar etiquetadas
- [Detective.1] Los gráficos de comportamiento de los detectives deben estar etiquetados
- [DMS.2] Los certificados DMS deben estar etiquetados
- [DMS.3] Las suscripciones a eventos de DMS deben estar etiquetadas
- [DMS.4] Las instancias de replicación de DMS deben estar etiquetadas
- [DMS.5] Los grupos de subredes de replicación del DMS deben estar etiquetados
- [DMS.6] Las instancias de replicación de DMS deben tener habilitada la actualización automática de las versiones secundarias
- [DMS.7] Las tareas de replicación del DMS para la base de datos de destino deben tener el registro habilitado
- [DMS.8] Las tareas de replicación del DMS para la base de datos de origen deben tener el registro activado
- [DMS.9] Los puntos finales del DMS deben usar SSL
- [DMS.10] Los puntos finales de DMS para las bases de datos de Neptune deben tener habilitada la autorización de IAM
- [DMS.11] Los puntos finales de DMS para MongoDB deben tener un mecanismo de autenticación habilitado
- [DMS.12] Los puntos finales de DMS para Redis OSS deben tener el TLS habilitado

- [DMS.13] Las instancias de replicación de DMS deben configurarse para usar varias zonas de disponibilidad
- [DocumentDB.1] Los clústeres de Amazon DocumentDB deben cifrarse en reposo
- [DocumentDB.2] Los clústeres de Amazon DocumentDB deben tener un período de retención de copias de seguridad adecuado
- [DocumentDB.3] Las instantáneas de clústeres manuales de Amazon DocumentDB no deben ser públicas
- [DocumentDB.4] Los clústeres de Amazon DocumentDB deben publicar los registros de auditoría en Logs CloudWatch
- [DocumentDB.5] Los clústeres de Amazon DocumentDB deben tener habilitada la protección contra eliminaciones
- [DocumentDB.6] Los clústeres de Amazon DocumentDB deben cifrarse en tránsito
- [DynamoDB.3] Los clústeres de DynamoDB Accelerator (DAX) deben cifrarse en reposo
- [DynamoDB.4] Las tablas de DynamoDB deben estar presentes en un plan de respaldo
- [DynamoDB.6] Las tablas de DynamoDB deben tener habilitada la protección de eliminación
- [DynamoDB.7] Los clústeres de DynamoDB Accelerator deben cifrarse en tránsito
- [EC2.4] Las instancias EC2 detenidas deben eliminarse después de un período de tiempo específico
- [EC2.21] Las ACL de red no deberían permitir la entrada desde la versión 0.0.0. 0/0 al puerto 22 o al puerto 3389
- [EC2.22] Deben eliminarse los grupos de seguridad de Amazon EC2 no utilizados
- [EC2.23] Amazon EC2 Transit Gateways no debe aceptar automáticamente las solicitudes de adjuntos de VPC
- [EC2.24] No se deben utilizar los tipos de instancias paravirtuales de Amazon EC2
- [EC2.25] Las plantillas de lanzamiento de Amazon EC2 no deben asignar direcciones IP públicas a las interfaces de red
- [EC2.28] Los volúmenes de EBS deben estar cubiertos por un plan de respaldo
- [EC2.34] Las tablas de rutas de la pasarela de tránsito EC2 deben estar etiquetadas
- [EC2.40] Las pasarelas NAT EC2 deben estar etiquetadas
- [EC2.51] Los puntos finales EC2 Client VPN deben tener habilitado el registro de conexiones de clientes

- [EC2.53] Los grupos de seguridad de EC2 no deberían permitir la entrada desde la versión 0.0.0.0/0 a los puertos de administración remota del servidor
- [EC2.54] Los grupos de seguridad de EC2 no deberían permitir la entrada desde: :/0 a los puertos de administración remota del servidor
- [EC2.55] Las VPC deben configurarse con un punto final de interfaz para la API de ECR
- [EC2.56] Las VPC deben configurarse con un punto final de interfaz para Docker Registry
- [EC2.57] Las VPC deben configurarse con un punto final de interfaz para Systems Manager
- [EC2.58] Las VPC deben configurarse con un punto final de interfaz para los contactos de Systems Manager Incident Manager
- [EC2.60] Las VPC deben configurarse con un punto final de interfaz para Systems Manager Incident Manager
- [EC2.170] Las plantillas de lanzamiento de EC2 deben utilizar la versión 2 del servicio de metadatos de instancias (IMDSv2)
- [EC2.171] Las conexiones VPN de EC2 deberían tener el registro habilitado
- [EC2.173] Las solicitudes de EC2 Spot Fleet con parámetros de lanzamiento deberían permitir el cifrado de los volúmenes de EBS adjuntos
- [EC2.174] Los conjuntos de opciones DHCP de EC2 deben estar etiquetados
- [EC2.175] Las plantillas de lanzamiento de EC2 deben estar etiquetadas
- [EC2.176] Las listas de prefijos de EC2 deben estar etiquetadas
- [EC2.177] Las sesiones de réplica de tráfico de EC2 deben etiquetarse
- [EC2.178] Los filtros espejo de tráfico EC2 deben estar etiquetados
- [EC2.179] Los objetivos del espejo de tráfico de EC2 deben estar etiquetados
- [EC2.180] Las interfaces de red EC2 deberían tener habilitada source/destination la verificación
- [EC2.181] Las plantillas de lanzamiento de EC2 deberían permitir el cifrado de los volúmenes de EBS adjuntos
- [EC2.183] Las conexiones VPN de EC2 deben utilizar el protocolo IKEv2
- [ECR.1] Los repositorios privados de ECR deben tener configurado el escaneo de imágenes
- [ECR.2] Los repositorios privados de ECR deben tener configurada la inmutabilidad de etiquetas
- [ECR.3] Los repositorios de ECR deben tener configurada al menos una política de ciclo de vida
- [ECR.4] Los repositorios públicos de ECR deben etiquetarse

- [ECR.5] Los repositorios de ECR deben estar cifrados y ser gestionados por el cliente AWS KMS keys
- [ECS.3] Las definiciones de tareas de ECS no deben compartir el espacio de nombres del proceso del host
- [ECS.4] Los contenedores ECS deben ejecutarse sin privilegios
- [ECS.5] Las definiciones de tareas de ECS deben configurar los contenedores para que se limiten al acceso de solo lectura a los sistemas de archivos raíz
- [ECS.8] Los secretos no deben transmitirse como variables de entorno de contenedores
- [ECS.9] Las definiciones de tareas de ECS deben tener una configuración de registro
- [ECS.10] Los servicios Fargate de ECS deberían ejecutarse en la última versión de la plataforma Fargate
- [ECS.12] Los clústeres de ECS deben usar Container Insights
- [ECS.17] Las definiciones de tareas de ECS no deben usar el modo de red host
- [ECS.19] Los proveedores de capacidad de ECS deberían tener habilitada la protección de terminación gestionada
- [EFS.1] Elastic File System debe configurarse para cifrar los datos de los archivos en reposo mediante AWS KMS
- [EFS.2] Los volúmenes de Amazon EFS deben figurar en los planes de copia de seguridad
- [EFS.3] Los puntos de acceso EFS deben exigir un directorio raíz
- [EFS.4] Los puntos de acceso EFS deben exigir la identidad del usuario
- [EFS.6] Los destinos de montaje de EFS no deben asociarse a subredes que asignan direcciones IP públicas en el momento del lanzamiento
- [] Los sistemas de archivos EFS deben tener habilitadas las copias de seguridad automáticas EFS.7
- [EFS.8] Los sistemas de archivos EFS deben cifrarse en reposo
- [EKS.2] Los clústeres de EKS deben ejecutarse en una versión de Kubernetes compatible
- [EKS.3] Los clústeres de EKS deben usar secretos de Kubernetes cifrados
- [EKS.7] Las configuraciones del proveedor de identidad de EKS deben etiquetarse
- [EKS.8] Los clústeres de EKS deben tener habilitado el registro de auditoría
- [ELB.10] El balanceador de carga clásico debe abarcar varias zonas de disponibilidad

- [ELB.12] El balanceador de carga de aplicaciones debe configurarse con el modo defensivo o de mitigación de desincronización más estricto
- [ELB.13] Los balanceadores de carga de aplicaciones, redes y puertas de enlace deben abarcar varias zonas de disponibilidad
- [ELB.14] El balanceador de carga clásico debe configurarse con el modo defensivo o de mitigación de desincronización más estricto
- [ELB.17] Los balanceadores de cargas de aplicaciones y redes con oyentes deben usar las políticas de seguridad recomendadas
- [ELB.18] Los oyentes del balanceador de cargas de red y aplicaciones deben usar protocolos seguros para cifrar los datos en tránsito
- [ElastiCache.1] ElastiCache (Redis OSS) los clústeres deben tener habilitadas las copias de seguridad automáticas
- [ElastiCache.2] ElastiCache los clústeres deberían tener habilitadas las actualizaciones automáticas de las versiones secundarias
- [ElastiCache.3] los grupos de ElastiCache replicación deberían tener habilitada la conmutación por error automática
- [ElastiCache.4] los grupos de ElastiCache replicación deben cifrarse en reposo
- [ElastiCache.5] los grupos de ElastiCache replicación deben cifrarse en tránsito
- [ElastiCache.6] ElastiCache (Redis OSS) Los grupos de replicación de versiones anteriores deberían tener habilitada la autenticación de Redis OSS
- [ElastiCache.7] los ElastiCache clústeres no deben usar el grupo de subredes predeterminado
- [ElasticBeanstalk.1] Los entornos de Elastic Beanstalk deberían tener habilitados los informes de estado mejorados
- [ElasticBeanstalk.2] Las actualizaciones de la plataforma gestionada de Elastic Beanstalk deben estar habilitadas
- [ElasticBeanstalk.3] Elastic Beanstalk debería transmitir los registros a CloudWatch
- [EMR.1] Los nodos principales del clúster de Amazon EMR no deben tener direcciones IP públicas
- [EMR.2] La configuración de acceso público del bloque Amazon EMR debe estar habilitada
- [EMR.3] Las configuraciones de seguridad de Amazon EMR deben cifrarse en reposo
- [EMR.4] Las configuraciones de seguridad de Amazon EMR deben cifrarse en tránsito
- [ES.4] Debería estar habilitado el registro de errores de dominio de Elasticsearch en Logs CloudWatch

- [ES.9] Los dominios de Elasticsearch deben etiquetarse
- [EventBridge.3] los autobuses de eventos EventBridge personalizados deben tener adjunta una política basada en los recursos
- [EventBridge.4] los puntos finales EventBridge globales deberían tener habilitada la replicación de eventos
- [FraudDetector.1] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.2] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas
- [FraudDetector.3] Los resultados de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.4] Las variables de Amazon Fraud Detector deben estar etiquetadas
- [FSx.1] FSx para sistemas de archivos OpenZFS debe configurarse para copiar etiquetas en copias de seguridad y volúmenes
- [FSx.2] Los sistemas de archivos FSx for Lustre deben configurarse para copiar etiquetas a las copias de seguridad
- [FSx.3] FSx para sistemas de archivos OpenZFS debe configurarse para su implementación Multi-AZ
- [FSx.4] FSx para sistemas de archivos NetApp ONTAP debe configurarse para su implementación Multi-AZ
- [FSx.5] Los sistemas de archivos FSx for Windows File Server deben configurarse para Multi-AZ su implementación
- [GlobalAccelerator.1] Los aceleradores de Global Accelerator deben estar etiquetados
- [Glue.1]AWS Gluelos trabajos deben estar etiquetados
- [Glue.3]AWS GlueLas transformaciones de aprendizaje automático deben cifrarse en reposo
- [Glue.4]AWS GlueLos trabajos de Spark deberían ejecutarse en versiones compatibles deAWS Glue
- GuardDuty Los filtros [GuardDuty.2] deben estar etiquetados
- [GuardDuty.5] La monitorización del registro de auditoría de GuardDuty EKS debe estar habilitada
- [GuardDuty.6] GuardDuty La protección Lambda debe estar habilitada
- [GuardDuty.7] La monitorización del tiempo de ejecución de GuardDuty EKS debe estar habilitada
- [GuardDuty.8] La protección contra GuardDuty malware para EC2 debe estar habilitada
- [GuardDuty.9] La protección GuardDuty RDS debe estar habilitada
- [GuardDuty.10] La protección GuardDuty S3 debe estar habilitada

- [GuardDuty.11] La monitorización del GuardDuty tiempo de ejecución debe estar habilitada
- [GuardDuty.12] La monitorización del tiempo de ejecución de GuardDuty ECS debe estar habilitada
- [GuardDuty.13] La monitorización del tiempo de ejecución de GuardDuty EC2 debe estar habilitada
- [IAM.1] Las políticas de IAM no deberían permitir todos los privilegios administrativos «*»
- [IAM.2] Los usuarios de IAM no deberían tener políticas de IAM adjuntas
- [IAM.3] Las claves de acceso de los usuarios de IAM deben rotarse cada 90 días o menos
- [IAM.4] La clave de acceso del usuario raíz de IAM no debería existir
- [IAM.5] La MFA debe estar habilitada para todos los usuarios de IAM que tengan una contraseña de consola
- [IAM.6] La MFA de hardware debe estar habilitada para el usuario root
- [IAM.7] Las políticas de contraseñas para los usuarios de IAM deben tener configuraciones sólidas
- [IAM.8] Se deben eliminar las credenciales de usuario de IAM no utilizadas
- [IAM.9] La MFA debe estar habilitada para el usuario root
- [IAM.10] Las políticas de contraseñas para los usuarios de IAM deben tener configuraciones sólidas
- [IAM.11] Asegúrese de que la política de contraseñas de IAM requiera al menos una letra mayúscula
- [IAM.12] Asegúrese de que la política de contraseñas de IAM requiera al menos una letra minúscula
- [IAM.13] Asegúrese de que la política de contraseñas de IAM requiera al menos un símbolo
- [IAM.14] Asegúrese de que la política de contraseñas de IAM requiera al menos un número
- [IAM.15] Asegúrese de que la política de contraseñas de IAM exija una longitud de contraseña mínima de 14 o más
- [IAM.16] Asegúrese de que la política de contraseñas de IAM impida la reutilización de contraseñas
- [IAM.17] Asegúrese de que la política de contraseñas de IAM haga caducar las contraseñas en un plazo de 90 días o menos
- [IAM.18] Asegúrese de que se haya creado una función de soporte para gestionar los incidentes conAWS Support
- [IAM.19] La MFA debe estar habilitada para todos los usuarios de IAM

- [IAM.21] Las políticas de IAM gestionadas por el cliente que cree no deberían permitir acciones comodín en los servicios
- [IAM.22] Se deben eliminar las credenciales de usuario de IAM que no se hayan utilizado durante 45 días
- [IAM.24] Las funciones de IAM deben estar etiquetadas
- [IAM.25] Los usuarios de IAM deben estar etiquetados
- [IAM.26] SSL/TLS Los certificados caducados gestionados en IAM deben eliminarse
- [IAM.27] Las identidades de IAM no deberían tener la AWSCloudShellFullAccess política adjunta
- [IAM.28] El analizador de acceso externo de IAM Access Analyzer debe estar habilitado
- [Inspector.1] El escaneo EC2 de Amazon Inspector debe estar activado
- [Inspector.2] El escaneo ECR de Amazon Inspector debe estar activado
- [Inspector.3] El escaneo de código Lambda de Amazon Inspector Lambda debe estar activado
- [Inspector.4] El escaneo estándar de Amazon Inspector Lambda debe estar activado
- [IoTSiteWise.1]AWSLos modelos SiteWise de activos de IoT deben estar etiquetados
- [IoTSiteWise.2]AWS SiteWise Los paneles de IoT deben estar etiquetados
- [IoTSiteWise.3]AWS SiteWise Las pasarelas de IoT deben estar etiquetadas
- [IoTSiteWise.4]AWS SiteWise Los portales de IoT deben estar etiquetados
- [IoTSiteWise.5]AWS SiteWise Los proyectos de IoT deben estar etiquetados
- [IoTTwinMaker.1]AWSLos trabajos de TwinMaker sincronización de IoT deben estar etiquetados
- [IoTTwinMaker.2]AWS TwinMaker Los espacios de trabajo de IoT deben estar etiquetados
- [IoTTwinMaker.3]AWS TwinMaker Las escenas de IoT deben estar etiquetadas
- [IoTTwinMaker.4]AWS TwinMaker Las entidades de IoT deben estar etiquetadas
- [IoTWireless.1]AWSLos grupos de multidifusión de IoT Wireless deben estar etiquetados
- [IoTWireless.2]AWSLos perfiles de servicio de IoT Wireless deben estar etiquetados
- [IoTWireless.3]AWSLas tareas de IoT FUOTA deben estar etiquetadas
- [IVS.1] Los pares de teclas de reproducción IVS deben estar etiquetados
- [IVS.2] Las configuraciones de grabación de IVS deben estar etiquetadas
- [IVS.3] Los canales IVS deben estar etiquetados
- [Keyspaces.1] Los espacios clave de Amazon Keyspaces deben estar etiquetados

- [Kinesis.1] Las transmisiones de Kinesis deben cifrarse en reposo
- [Kinesis.3] Las transmisiones de Kinesis deben tener un período de retención de datos adecuado
- [KMS.1] Las políticas gestionadas por los clientes de IAM no deberían permitir acciones de descifrado en todas las claves de KMS
- [KMS.2] Los directores de IAM no deberían tener políticas integradas de IAM que permitan realizar acciones de descifrado en todas las claves de KMS
- [KMS.5] Las claves KMS no deben ser de acceso público
- [Lambda.5] Las funciones de VPC Lambda deben funcionar en varias zonas de disponibilidad
- [Lambda.7] Las funciones de Lambda deberían tener AWS X-Ray el rastreo activo está habilitado
- [Macie.1] Amazon Macie debería estar activado
- [Macie.2] La detección automática de datos confidenciales por parte de Macie debería estar habilitada
- [MQ.2] Los corredores de ActiveMQ deben transmitir los registros de auditoría a CloudWatch
- [MQ.4] Los corredores de Amazon MQ deben estar etiquetados
- [MQ.5] Los corredores de ActiveMQ deberían usar el modo de implementación active/standby
- [MQ.6] Los corredores de RabbitMQ deberían usar el modo de despliegue de clústeres
- [MSK.1] Los clústeres de MSK deben cifrarse en tránsito entre los nodos de intermediación
- [MSK.2] Los clústeres de MSK deberían tener configurada una supervisión mejorada
- [MSK.3] Los conectores MSK Connect deben estar cifrados en tránsito
- [MSK.4] Los clústeres de MSK deben tener el acceso público deshabilitado
- [MSK.5] Los conectores MSK deben tener el registro activado
- [MSK.6] Los clústeres de MSK deberían deshabilitar el acceso no autenticado
- [Neptune.1] Los clústeres de bases de datos de Neptune deben cifrarse en reposo
- [Neptune.2] Los clústeres de bases de datos de Neptune deberían publicar registros de auditoría en Logs CloudWatch
- [Neptune.3] Las instantáneas del clúster de base de datos de Neptune no deben ser públicas
- [Neptune.4] Los clústeres de base de datos de Neptune deben tener habilitada la protección contra eliminación
- [Neptune.5] Los clústeres de Neptune DB deberían tener habilitadas las copias de seguridad automatizadas

- [Neptune.6] Las instantáneas del clúster de base de datos de Neptune deben cifrarse en reposo
- [Neptune.7] Los clústeres de base de datos de Neptune deben tener habilitada la autenticación de bases de datos de IAM
- [Neptune.8] Los clústeres de bases de datos de Neptune deben configurarse para copiar etiquetas a las instantáneas
- [Neptune.9] Los clústeres de base de datos Neptune deben implementarse en varias zonas de disponibilidad
- [NetworkFirewall.1] Los firewalls de Network Firewall deben implementarse en varias zonas de disponibilidad
- [NetworkFirewall.2] El registro de Network Firewall debe estar habilitado
- [NetworkFirewall.3] Las políticas de Network Firewall deben tener asociado al menos un grupo de reglas
- [NetworkFirewall.4] La acción sin estado predeterminada para las políticas de Network Firewall debe ser eliminar o reenviar paquetes completos
- [NetworkFirewall.5] La acción sin estado predeterminada para las políticas de Network Firewall debe ser eliminar o reenviar paquetes fragmentados
- [NetworkFirewall.6] El grupo de reglas de Stateless Network Firewall no debe estar vacío
- [NetworkFirewall.9] Los firewalls de Network Firewall deben tener habilitada la protección de eliminación
- [NetworkFirewall.10] Los firewalls de Network Firewall deben tener habilitada la protección contra cambios de subred
- [Opensearch.1] OpenSearch los dominios deben tener activado el cifrado en reposo
- [Opensearch.2] OpenSearch los dominios no deben ser de acceso público
- [Opensearch.3] OpenSearch los dominios deben cifrar los datos enviados entre nodos
- [Opensearch.4] El registro de errores de OpenSearch dominio en Logs debe estar habilitado CloudWatch
- [Opensearch.5] OpenSearch los dominios deben tener activado el registro de auditoría
- [Opensearch.6] OpenSearch los dominios deben tener al menos tres nodos de datos
- [Opensearch.7] OpenSearch los dominios deben tener habilitado un control de acceso detallado
- [Opensearch.8] Las conexiones a los OpenSearch dominios deben cifrarse con la última política de seguridad de TLS

- [Opensearch.9] OpenSearch los dominios deben estar etiquetados
- [Opensearch.10] OpenSearch los dominios deben tener instalada la última actualización de software
- [Opensearch.11] OpenSearch los dominios deben tener al menos tres nodos principales dedicados
- [PCA.1]AWS Privada CALa autoridad emisora de certificados raíz debe estar deshabilitada
- [PCA.2]AWSLas autoridades de certificación de CA privadas deben estar etiquetadas
- [RDS.14] Los clústeres de Amazon Aurora deben tener habilitado el retroceso
- [RDS.24] Los clústeres de bases de datos de RDS deben usar un nombre de usuario de administrador personalizado
- [RDS.25] Las instancias de bases de datos de RDS deben usar un nombre de usuario de administrador personalizado
- [RDS.26] Las instancias de base de datos de RDS deben protegerse mediante un plan de respaldo
- [RDS.27] Los clústeres de bases de datos de RDS deben cifrarse en reposo
- [RDS.31] Los grupos de seguridad de la base de datos de RDS deben etiquetarse
- [RDS.34] Los clústeres de bases de datos Aurora MySQL deben publicar los registros de auditoría en Logs CloudWatch
- [RDS.35] Los clústeres de bases de datos de RDS deben tener habilitada la actualización automática de versiones secundarias
- [RDS.36] Las instancias de base de datos de RDS para PostgreSQL deben publicar los registros en Logs CloudWatch
- [RDS.37] Los clústeres de bases de datos de Aurora PostgreSQL deben publicar los registros en Logs CloudWatch
- [RDS.38] Las instancias de base de datos de RDS para PostgreSQL deben cifrarse en tránsito
- [RDS.39] Las instancias de base de datos de RDS para MySQL deben cifrarse en tránsito
- [RDS.40] Las instancias de base de datos de RDS para SQL Server deben publicar los registros en Logs CloudWatch
- [RDS.41] Las instancias de base de datos de RDS para SQL Server deben cifrarse en tránsito
- [RDS.42] Las instancias de base de datos de RDS para MariaDB deben publicar los registros en Logs CloudWatch
- [RDS.43] Los proxies de bases de datos de RDS deben requerir el cifrado TLS para las conexiones

- [RDS.44] Las instancias de base de datos de RDS para MariaDB deben cifrarse durante el tránsito
- [RDS.45] Los clústeres de bases de datos Aurora MySQL deben tener habilitado el registro de auditoría
- [RDS.46] Las instancias de base de datos de RDS no deben implementarse en subredes públicas con rutas a pasarelas de Internet
- [RDS.47] Los clústeres de bases de datos de RDS para PostgreSQL deben configurarse para copiar las etiquetas a las instantáneas de bases de datos
- [RDS.51] Los clústeres globales de RDS deben ejecutarse en una versión compatible de Aurora MySQL
- [Redshift.8] Los clústeres de Amazon Redshift no deben usar el nombre de usuario de administrador predeterminado
- [Redshift.10] Los clústeres de Redshift deben cifrarse en reposo
- [Redshift.15] Los grupos de seguridad de Redshift deberían permitir la entrada en el puerto del clúster solo desde orígenes restringidos
- [Redshift.16] Los grupos de subredes de clústeres de Redshift deben tener subredes de varias zonas de disponibilidad
- [Redshift.17] Los grupos de parámetros del clúster de Redshift deben estar etiquetados
- [Redshift.18] Los clústeres de Redshift deberían tener Multi-AZ las implementaciones habilitadas
- [RedshiftServerless.1] Los grupos de trabajo sin servidor de Amazon Redshift deberían utilizar un enrutamiento de VPC mejorado
- [RedshiftServerless.2] Las conexiones a los grupos de trabajo sin servidor de Redshift deberían ser obligatorias para usar SSL
- [RedshiftServerless.3] Los grupos de trabajo sin servidor de Redshift deberían prohibir el acceso público
- [RedshiftServerless.4] Los espacios de nombres de Redshift Serverless deben cifrarse y administrarse por el clienteAWS KMS keys
- [RedshiftServerless.5] Los espacios de nombres Redshift Serverless no deben usar el nombre de usuario de administrador predeterminado
- [RedshiftServerless.6] Los espacios de nombres Redshift Serverless deberían exportar los registros a los registros CloudWatch
- [Route53.1] Los controles de salud de Route 53 deben estar etiquetados
- [Route53.2] Las zonas alojadas públicas de Route 53 deberían registrar las consultas de DNS

- [S3.7] Los cubos de uso general de S3 deben utilizar la replicación entre regiones
- [S3.10] Los cubos de uso general de S3 con el control de versiones habilitado deben tener configuraciones de ciclo de vida
- [S3.11] Los cubos de uso general de S3 deben tener habilitadas las notificaciones de eventos
- [S3.12] Las ACL no deben usarse para administrar el acceso de los usuarios a los cubos de uso general de S3
- [S3.13] Los cubos de uso general de S3 deben tener configuraciones de ciclo de vida
- [S3.19] Los puntos de acceso S3 deben tener habilitada la configuración de bloqueo de acceso público
- [S3.20] Los cubos de uso general de S3 deben tener habilitada la eliminación de MFA
- [S3.22] Los cubos de uso general de S3 deben registrar los eventos de escritura a nivel de objeto
- [S3.23] Los cubos de uso general de S3 deben registrar los eventos de lectura a nivel de objeto
- [S3.24] Los puntos de Multi-Region acceso S3 deben tener habilitada la configuración de bloqueo del acceso público
- [S3.25] Los buckets de directorio de S3 deben tener configuraciones de ciclo de vida
- [SageMaker.1] Las instancias de Amazon SageMaker Notebook no deberían tener acceso directo a Internet
- [SageMaker.2] las instancias de SageMaker cuadernos deben lanzarse en una VPC personalizada
- [SageMaker.3] Los usuarios no deben tener acceso root a las instancias de los SageMaker cuadernos
- [SageMaker.4] Las variantes de producción de SageMaker terminales deben tener un recuento inicial de instancias superior a 1
- SageMaker Los modelos [SageMaker.5] deben tener habilitado el aislamiento de red
- [SageMaker.6] las configuraciones de imagen de la SageMaker aplicación deben estar etiquetadas
- [SageMaker.7] SageMaker las imágenes deben estar etiquetadas
- [SageMaker.8] las instancias de SageMaker notebooks deben ejecutarse en plataformas compatibles
- [SageMaker.9] las definiciones de trabajos de calidad de los SageMaker datos deben tener habilitado el cifrado del tráfico entre contenedores
- [SageMaker.10] Las definiciones de trabajos de explicabilidad del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores

- [SageMaker.11] las definiciones de trabajos SageMaker de calidad de los datos deben tener habilitado el aislamiento de red
- [SageMaker.12] las definiciones de trabajo basadas en el sesgo del SageMaker modelo deben tener habilitado el aislamiento de red
- [SageMaker.13] las definiciones de trabajos de calidad del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores
- [SageMaker.14] los programas SageMaker de monitoreo deben tener habilitado el aislamiento de la red
- [SageMaker.15] Las definiciones de trabajo basadas en el sesgo del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores
- SageMaker Los modelos [SageMaker.16] deben usar un registro privado en la VPC para los contenedores principales
- [SageMaker.17] SageMaker Las tiendas offline de los grupos de funciones deben cifrarse con AWS KMS claves
- [SageMaker.18] las tiendas en línea de grupos de SageMaker funciones con almacenamiento estándar deben cifrarse con AWS KMS claves
- [SageMaker.19] SageMaker los modelos deben usar un registro privado en la VPC para las canalizaciones de inferencia de varios contenedores
- [SES.3] Los conjuntos de configuración de SES deben tener el TLS habilitado para enviar correos electrónicos
- [ServiceCatalog.1] Las carteras de Service Catalog deben compartirse dentro de unAWSsolo una organización
- [SNS.4] Las políticas de acceso a los temas de SNS no deberían permitir el acceso público
- [SQS.1] Las colas de Amazon SQS deben cifrarse en reposo
- [SQS.2] Las colas de SQS deben estar etiquetadas
- [SQS.3] Las políticas de acceso a las colas de SQS no deberían permitir el acceso público
- [SSM.4] Los documentos SSM no deben ser públicos
- [SSM.5] Los documentos SSM deben estar etiquetados
- [SSM.6] SSM Automation debería tener el registro habilitado CloudWatch
- [SSM.7] Los documentos SSM deben tener habilitada la configuración de bloqueo para compartir en público

- [StepFunctions.1] Step Functions indica que las máquinas deben tener el registro activado
- [Transfer.2] Los servidores Transfer Family no deben usar el protocolo FTP para la conexión de puntos finales
- [Transfer.3] Los conectores Transfer Family deben tener habilitado el registro
- [Transfer.4] Los acuerdos Transfer Family deben estar etiquetados
- [Transfer.5] Los certificados Transfer Family deben estar etiquetados
- [Transfer.6] Los conectores Transfer Family deben estar etiquetados
- [Transfer.7] Los perfiles de Transfer Family deben estar etiquetados
- [WAF.1]AWS WAFEl registro de ACL web global clásico debe estar habilitado
- [WAF.2]AWS WAFLas reglas regionales clásicas deben tener al menos una condición
- [WAF.3]AWS WAFLos grupos de reglas regionales clásicos deben tener al menos una regla
- [WAF.4]AWS WAFLas ACL web regionales clásicas deben tener al menos una regla o grupo de reglas
- [WAF.6]AWS WAFLas reglas globales clásicas deben tener al menos una condición
- [WAF.7]AWS WAFLos grupos de reglas globales clásicos deben tener al menos una regla
- [WAF.8]AWS WAFLas ACL web globales clásicas deben tener al menos una regla o grupo de reglas
- [WAF.10]AWS WAFLas ACL web deben tener al menos una regla o grupo de reglas
- [WAF.12]AWS WAFlas reglas deben tener CloudWatch las métricas habilitadas
- [WorkSpaces.1] los volúmenes de WorkSpaces usuarios deben cifrarse en reposo
- [WorkSpaces.2] los volúmenes WorkSpaces raíz deben cifrarse en reposo

Asia-Pacífico (Melbourne)

Los siguientes controles no se admiten en la región Asia-Pacífico (Melbourne).

- [APIGateway.8] Las rutas de API Gateway deben especificar un tipo de autorización
- [APIGateway.9] El registro de acceso debe configurarse para las etapas V2 de API Gateway
- [Amplify.1] Las aplicaciones Amplify deben estar etiquetadas
- [Amplify.2] Amplify branches debe estar etiquetado
- [AppFlow.1] AppFlow Los flujos de Amazon deben estar etiquetados

- [AppRunner.1] Los servicios de App Runner deben estar etiquetados
- [AppRunner.2] Los conectores VPC de App Runner deben estar etiquetados
- [AppSync.1]AWS AppSyncLas cachés de las API deben estar cifradas en reposo
- [AppSync.2]AWS AppSyncdebe tener habilitado el registro a nivel de campo
- [AppSync.5]AWS AppSyncLas API de GraphQL no deben autenticarse con claves de API
- [AppSync.6]AWS AppSyncLas cachés de las API deben cifrarse en tránsito
- [Backup.1]AWS Backuplos puntos de recuperación deben estar cifrados en reposo
- [Batch.1] Las colas de trabajos por lotes deben estar etiquetadas
- [Batch.3] Los entornos de procesamiento por lotes deben etiquetarse
- [Batch.4] Las propiedades de los recursos de cómputo en los entornos de cómputo por lotes gestionados deben estar etiquetadas
- [BedrockAgentCore.1] Los AgentCore tiempos de ejecución de Bedrock deben configurarse con el modo de red VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways debería requerir autorización para las solicitudes entrantes
- [BedrockAgentCore.3] Bedrock AgentCore Memory debe estar cifrada y gestionada por el clienteAWS KMSclaves
- [BedrockAgentCore.4] Bedrock AgentCore Gateway debe cifrarse de forma que sea gestionada por el clienteAWS KMSclaves
- [BedrockAgentCore.5] Los navegadores AgentCore personalizados de Bedrock no deberían usar el modo de red pública
- [BedrockAgentCore.6] Los navegadores AgentCore personalizados de Bedrock deberían tener habilitada la grabación de sesiones
- [CloudFormation.3] las CloudFormation pilas deben tener habilitada la protección de terminación
- [CloudFormation.4] las CloudFormation pilas deben tener funciones de servicio asociadas
- [CloudFront.1] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado
- [CloudFront.3] CloudFront las distribuciones deben requerir el cifrado durante el tránsito
- [CloudFront.4] CloudFront las distribuciones deben tener configurada la conmutación por error de origen
- [CloudFront.5] CloudFront las distribuciones deben tener habilitado el registro

- [CloudFront.6] CloudFront las distribuciones deben tener WAF activado
- [CloudFront.7] CloudFront las distribuciones deben usar certificados personalizados SSL/TLS
- [CloudFront.8] CloudFront las distribuciones deben usar el SNI para atender las solicitudes HTTPS
- [CloudFront.9] CloudFront las distribuciones deben cifrar el tráfico para convertirlo en orígenes personalizados
- [CloudFront.10] CloudFront las distribuciones no deben usar protocolos SSL obsoletos entre ubicaciones de borde y orígenes personalizados
- [CloudFront.12] CloudFront las distribuciones no deben apuntar a orígenes de S3 inexistentes
- [CloudFront.13] CloudFront las distribuciones deben usar el control de acceso al origen
- [CloudFront.14] CloudFront las distribuciones deben estar etiquetadas
- [CloudFront.15] CloudFront las distribuciones deben usar la política de seguridad TLS recomendada
- [CloudFront.16] CloudFront las distribuciones deben usar el control de acceso de origen para los orígenes de las URL de las funciones de Lambda
- [CloudFront.17] CloudFront las distribuciones deben usar grupos de claves confiables para las URL y cookies firmadas
- [CodeArtifact.1] CodeArtifact los repositorios deben estar etiquetados
- [CodeGuruProfiler.1] Los grupos CodeGuru de creación de perfiles de Profiler deben estar etiquetados
- [CodeGuruReviewer.1] Las asociaciones de repositorios de CodeGuru Reviewer deben estar etiquetadas
- [Cognito.1] Los grupos de usuarios de Cognito deben tener activada la protección contra amenazas y el modo de aplicación con todas las funciones para la autenticación estándar
- [Connect.1] Los tipos de objetos de los perfiles de clientes de Amazon Connect deben estar etiquetados
- [Connect.2] Las instancias de Connect Customer deben tener el CloudWatch registro habilitado
- [Detective.1] Los gráficos de comportamiento de los detectives deben estar etiquetados
- [DMS.2] Los certificados DMS deben estar etiquetados
- [DMS.3] Las suscripciones a eventos de DMS deben estar etiquetadas
- [DMS.4] Las instancias de replicación de DMS deben estar etiquetadas
- [DMS.5] Los grupos de subredes de replicación del DMS deben estar etiquetados

- [DMS.6] Las instancias de replicación de DMS deben tener habilitada la actualización automática de las versiones secundarias
- [DMS.7] Las tareas de replicación del DMS para la base de datos de destino deben tener el registro habilitado
- [DMS.8] Las tareas de replicación del DMS para la base de datos de origen deben tener el registro activado
- [DMS.9] Los puntos finales del DMS deben usar SSL
- [DMS.10] Los puntos finales de DMS para las bases de datos de Neptune deben tener habilitada la autorización de IAM
- [DMS.11] Los puntos finales de DMS para MongoDB deben tener un mecanismo de autenticación habilitado
- [DMS.12] Los puntos finales de DMS para Redis OSS deben tener el TLS habilitado
- [DMS.13] Las instancias de replicación de DMS deben configurarse para usar varias zonas de disponibilidad
- [DocumentDB.1] Los clústeres de Amazon DocumentDB deben cifrarse en reposo
- [DocumentDB.2] Los clústeres de Amazon DocumentDB deben tener un período de retención de copias de seguridad adecuado
- [DocumentDB.3] Las instantáneas de clústeres manuales de Amazon DocumentDB no deben ser públicas
- [DocumentDB.4] Los clústeres de Amazon DocumentDB deben publicar los registros de auditoría en Logs CloudWatch
- [DocumentDB.5] Los clústeres de Amazon DocumentDB deben tener habilitada la protección contra eliminaciones
- [DocumentDB.6] Los clústeres de Amazon DocumentDB deben cifrarse en tránsito
- [DynamoDB.3] Los clústeres de DynamoDB Accelerator (DAX) deben cifrarse en reposo
- [DynamoDB.7] Los clústeres de DynamoDB Accelerator deben cifrarse en tránsito
- [EC2.4] Las instancias EC2 detenidas deben eliminarse después de un período de tiempo específico
- [EC2.14] Los grupos de seguridad no deberían permitir la entrada desde la versión 0.0.0. 0/0 o: :/0 al puerto 3389
- [EC2.22] Deben eliminarse los grupos de seguridad de Amazon EC2 no utilizados

- [EC2.23] Amazon EC2 Transit Gateways no debe aceptar automáticamente las solicitudes de adjuntos de VPC
- [EC2.24] No se deben utilizar los tipos de instancias paravirtuales de Amazon EC2
- [EC2.25] Las plantillas de lanzamiento de Amazon EC2 no deben asignar direcciones IP públicas a las interfaces de red
- [EC2.34] Las tablas de rutas de la pasarela de tránsito EC2 deben estar etiquetadas
- [EC2.40] Las pasarelas NAT EC2 deben estar etiquetadas
- [EC2.58] Las VPC deben configurarse con un punto final de interfaz para los contactos de Systems Manager Incident Manager
- [EC2.60] Las VPC deben configurarse con un punto final de interfaz para Systems Manager Incident Manager
- [EC2.170] Las plantillas de lanzamiento de EC2 deben utilizar la versión 2 del servicio de metadatos de instancias (IMDSv2)
- [EC2.173] Las solicitudes de EC2 Spot Fleet con parámetros de lanzamiento deberían permitir el cifrado de los volúmenes de EBS adjuntos
- [EC2.175] Las plantillas de lanzamiento de EC2 deben estar etiquetadas
- [EC2.181] Las plantillas de lanzamiento de EC2 deberían permitir el cifrado de los volúmenes de EBS adjuntos
- [ECR.4] Los repositorios públicos de ECR deben etiquetarse
- [EFS.1] Elastic File System debe configurarse para cifrar los datos de los archivos en reposo mediante AWS KMS
- [EFS.2] Los volúmenes de Amazon EFS deben figurar en los planes de copia de seguridad
- [ELB.14] El balanceador de carga clásico debe configurarse con el modo defensivo o de mitigación de desincronización más estricto
- [ELB.17] Los balanceadores de cargas de aplicaciones y redes con oyentes deben usar las políticas de seguridad recomendadas
- [ELB.18] Los oyentes del balanceador de cargas de red y aplicaciones deben usar protocolos seguros para cifrar los datos en tránsito
- [ElastiCache.1] ElastiCache (Redis OSS) los clústeres deben tener habilitadas las copias de seguridad automáticas
- [ElastiCache.2] ElastiCache los clústeres deberían tener habilitadas las actualizaciones automáticas de las versiones secundarias

- [ElastiCache.3] los grupos de ElastiCache replicación deberían tener habilitada la conmutación por error automática
- [ElastiCache.4] los grupos de ElastiCache replicación deben cifrarse en reposo
- [ElastiCache.5] los grupos de ElastiCache replicación deben cifrarse en tránsito
- [ElastiCache.6] ElastiCache (Redis OSS) Los grupos de replicación de versiones anteriores deberían tener habilitada la autenticación de Redis OSS
- [ElastiCache.7] los ElastiCache clústeres no deben usar el grupo de subredes predeterminado
- [ElasticBeanstalk.1] Los entornos de Elastic Beanstalk deberían tener habilitados los informes de estado mejorados
- [ElasticBeanstalk.2] Las actualizaciones de la plataforma gestionada de Elastic Beanstalk deben estar habilitadas
- [ElasticBeanstalk.3] Elastic Beanstalk debería transmitir los registros a CloudWatch
- [EMR.1] Los nodos principales del clúster de Amazon EMR no deben tener direcciones IP públicas
- [ES.4] Debería estar habilitado el registro de errores de dominio de Elasticsearch en Logs CloudWatch
- [EventBridge.4] los puntos finales EventBridge globales deberían tener habilitada la replicación de eventos
- [FraudDetector.1] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.2] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas
- [FraudDetector.3] Los resultados de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.4] Las variables de Amazon Fraud Detector deben estar etiquetadas
- [FSx.1] FSx para sistemas de archivos OpenZFS debe configurarse para copiar etiquetas en copias de seguridad y volúmenes
- [FSx.3] FSx para sistemas de archivos OpenZFS debe configurarse para su implementación Multi-AZ
- [GlobalAccelerator.1] Los aceleradores de Global Accelerator deben estar etiquetados
- [Glue.4]AWS GlueLos trabajos de Spark deberían ejecutarse en versiones compatibles deAWS Glue
- GuardDuty Los filtros [GuardDuty.2] deben estar etiquetados
- [IAM.1] Las políticas de IAM no deberían permitir todos los privilegios administrativos «*»
- [IAM.2] Los usuarios de IAM no deberían tener políticas de IAM adjuntas

- [IAM.3] Las claves de acceso de los usuarios de IAM deben rotarse cada 90 días o menos
- [IAM.5] La MFA debe estar habilitada para todos los usuarios de IAM que tengan una contraseña de consola
- [IAM.6] La MFA de hardware debe estar habilitada para el usuario root
- [IAM.8] Se deben eliminar las credenciales de usuario de IAM no utilizadas
- [IAM.10] Las políticas de contraseñas para los usuarios de IAM deben tener configuraciones sólidas
- [IAM.11] Asegúrese de que la política de contraseñas de IAM requiera al menos una letra mayúscula
- [IAM.12] Asegúrese de que la política de contraseñas de IAM requiera al menos una letra minúscula
- [IAM.13] Asegúrese de que la política de contraseñas de IAM requiera al menos un símbolo
- [IAM.14] Asegúrese de que la política de contraseñas de IAM requiera al menos un número
- [IAM.15] Asegúrese de que la política de contraseñas de IAM exija una longitud de contraseña mínima de 14 o más
- [IAM.16] Asegúrese de que la política de contraseñas de IAM impida la reutilización de contraseñas
- [IAM.17] Asegúrese de que la política de contraseñas de IAM haga caducar las contraseñas en un plazo de 90 días o menos
- [IAM.18] Asegúrese de que se haya creado una función de soporte para gestionar los incidentes conAWS Support
- [IAM.19] La MFA debe estar habilitada para todos los usuarios de IAM
- [IAM.21] Las políticas de IAM gestionadas por el cliente que cree no deberían permitir acciones comodín en los servicios
- [IAM.22] Se deben eliminar las credenciales de usuario de IAM que no se hayan utilizado durante 45 días
- [IAM.24] Las funciones de IAM deben estar etiquetadas
- [IAM.25] Los usuarios de IAM deben estar etiquetados
- [IAM.26] SSL/TLS Los certificados caducados gestionados en IAM deben eliminarse
- [IAM.27] Las identidades de IAM no deberían tener la AWSCloudShellFullAccess política adjunta
- [Inspector.1] El escaneo EC2 de Amazon Inspector debe estar activado

- [Inspector.2] El escaneo ECR de Amazon Inspector debe estar activado
- [Inspector.3] El escaneo de código Lambda de Amazon Inspector Lambda debe estar activado
- [Inspector.4] El escaneo estándar de Amazon Inspector Lambda debe estar activado
- [IoT.1]AWS IoT Device Defenderlos perfiles de seguridad deben estar etiquetados
- [IoT.2]AWS IoT Corelas acciones de mitigación deben estar etiquetadas
- [IoT.3]AWS IoT Corelas dimensiones deben estar etiquetadas
- [IoT.4]AWS IoT Corelos autorizadores deben estar etiquetados
- [IoT.5]AWS IoT CoreLos alias de los roles deben estar etiquetados
- [IoT.6]AWS IoT Corelas políticas deben estar etiquetadas
- [IoTSiteWise.1]AWSLos modelos SiteWise de activos de IoT deben estar etiquetados
- [IoTSiteWise.2]AWS SiteWise Los paneles de IoT deben estar etiquetados
- [IoTSiteWise.3]AWS SiteWise Las pasarelas de IoT deben estar etiquetadas
- [IoTSiteWise.4]AWS SiteWise Los portales de IoT deben estar etiquetados
- [IoTSiteWise.5]AWS SiteWise Los proyectos de IoT deben estar etiquetados
- [IoTTwinMaker.1]AWSLos trabajos de TwinMaker sincronización de IoT deben estar etiquetados
- [IoTTwinMaker.2]AWS TwinMaker Los espacios de trabajo de IoT deben estar etiquetados
- [IoTTwinMaker.3]AWS TwinMaker Las escenas de IoT deben estar etiquetadas
- [IoTTwinMaker.4]AWS TwinMaker Las entidades de IoT deben estar etiquetadas
- [IoTWireless.1]AWSLos grupos de multidifusión de IoT Wireless deben estar etiquetados
- [IoTWireless.2]AWSLos perfiles de servicio de IoT Wireless deben estar etiquetados
- [IoTWireless.3]AWSLas tareas de IoT FUOTA deben estar etiquetadas
- [IVS.1] Los pares de teclas de reproducción IVS deben estar etiquetados
- [IVS.2] Las configuraciones de grabación de IVS deben estar etiquetadas
- [IVS.3] Los canales IVS deben estar etiquetados
- [Keyspaces.1] Los espacios clave de Amazon Keyspaces deben estar etiquetados
- [Kinesis.1] Las transmisiones de Kinesis deben cifrarse en reposo
- [KMS.1] Las políticas gestionadas por los clientes de IAM no deberían permitir acciones de descifrado en todas las claves de KMS
- [KMS.2] Los directores de IAM no deberían tener políticas integradas de IAM que permitan realizar acciones de descifrado en todas las claves de KMS

- [Macie.1] Amazon Macie debería estar activado
- [Macie.2] La detección automática de datos confidenciales por parte de Macie debería estar habilitada
- [MQ.6] Los corredores de RabbitMQ deberían usar el modo de despliegue de clústeres
- [MSK.3] Los conectores MSK Connect deben estar cifrados en tránsito
- [MSK.5] Los conectores MSK deben tener el registro activado
- [Neptune.1] Los clústeres de bases de datos de Neptune deben cifrarse en reposo
- [Neptune.2] Los clústeres de bases de datos de Neptune deberían publicar registros de auditoría en Logs CloudWatch
- [Neptune.3] Las instantáneas del clúster de base de datos de Neptune no deben ser públicas
- [Neptune.4] Los clústeres de base de datos de Neptune deben tener habilitada la protección contra eliminación
- [Neptune.5] Los clústeres de Neptune DB deberían tener habilitadas las copias de seguridad automatizadas
- [Neptune.6] Las instantáneas del clúster de base de datos de Neptune deben cifrarse en reposo
- [Neptune.7] Los clústeres de base de datos de Neptune deben tener habilitada la autenticación de bases de datos de IAM
- [Neptune.8] Los clústeres de bases de datos de Neptune deben configurarse para copiar etiquetas a las instantáneas
- [Neptune.9] Los clústeres de base de datos Neptune deben implementarse en varias zonas de disponibilidad
- [Opensearch.1] OpenSearch los dominios deben tener activado el cifrado en reposo
- [Opensearch.2] OpenSearch los dominios no deben ser de acceso público
- [Opensearch.3] OpenSearch los dominios deben cifrar los datos enviados entre nodos
- [Opensearch.4] El registro de errores de OpenSearch dominio en Logs debe estar habilitado CloudWatch
- [Opensearch.5] OpenSearch los dominios deben tener activado el registro de auditoría
- [Opensearch.6] OpenSearch los dominios deben tener al menos tres nodos de datos
- [Opensearch.7] OpenSearch los dominios deben tener habilitado un control de acceso detallado
- [Opensearch.8] Las conexiones a los OpenSearch dominios deben cifrarse con la última política de seguridad de TLS

- [Opensearch.9] OpenSearch los dominios deben estar etiquetados
- [Opensearch.10] OpenSearch los dominios deben tener instalada la última actualización de software
- [Opensearch.11] OpenSearch los dominios deben tener al menos tres nodos principales dedicados
- [RDS.1] La instantánea de RDS debe ser privada
- [RDS.14] Los clústeres de Amazon Aurora deben tener habilitado el retroceso
- [RDS.31] Los grupos de seguridad de la base de datos de RDS deben etiquetarse
- [RDS.35] Los clústeres de bases de datos de RDS deben tener habilitada la actualización automática de versiones secundarias
- [RDS.37] Los clústeres de bases de datos de Aurora PostgreSQL deben publicar los registros en Logs CloudWatch
- [RedshiftServerless.1] Los grupos de trabajo sin servidor de Amazon Redshift deberían utilizar un enrutamiento de VPC mejorado
- [RedshiftServerless.2] Las conexiones a los grupos de trabajo sin servidor de Redshift deberían ser obligatorias para usar SSL
- [RedshiftServerless.3] Los grupos de trabajo sin servidor de Redshift deberían prohibir el acceso público
- [RedshiftServerless.4] Los espacios de nombres de Redshift Serverless deben cifrarse y administrarse por el clienteAWS KMS keys
- [RedshiftServerless.5] Los espacios de nombres Redshift Serverless no deben usar el nombre de usuario de administrador predeterminado
- [RedshiftServerless.6] Los espacios de nombres Redshift Serverless deberían exportar los registros a los registros CloudWatch
- [Route53.1] Los controles de salud de Route 53 deben estar etiquetados
- [Route53.2] Las zonas alojadas públicas de Route 53 deberían registrar las consultas de DNS
- [S3.24] Los puntos de Multi-Region acceso S3 deben tener habilitada la configuración de bloqueo del acceso público
- [S3.25] Los buckets de directorio de S3 deben tener configuraciones de ciclo de vida
- [SageMaker.1] Las instancias de Amazon SageMaker Notebook no deberían tener acceso directo a Internet
- [SageMaker.2] las instancias de SageMaker cuadernos deben lanzarse en una VPC personalizada

- [SageMaker.3] Los usuarios no deben tener acceso root a las instancias de los SageMaker cuadernos
- SageMaker Los modelos [SageMaker.5] deben tener habilitado el aislamiento de red
- [SageMaker.6] las configuraciones de imagen de la SageMaker aplicación deben estar etiquetadas
- [SageMaker.7] SageMaker las imágenes deben estar etiquetadas
- [SageMaker.8] las instancias de SageMaker notebooks deben ejecutarse en plataformas compatibles
- [SageMaker.9] las definiciones de trabajos de calidad de los SageMaker datos deben tener habilitado el cifrado del tráfico entre contenedores
- [SageMaker.10] Las definiciones de trabajos de explicabilidad del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores
- [SageMaker.11] las definiciones de trabajos SageMaker de calidad de los datos deben tener habilitado el aislamiento de red
- [SageMaker.12] las definiciones de trabajo basadas en el sesgo del SageMaker modelo deben tener habilitado el aislamiento de red
- [SageMaker.13] las definiciones de trabajos de calidad del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores
- [SageMaker.14] los programas SageMaker de monitoreo deben tener habilitado el aislamiento de la red
- [SageMaker.15] Las definiciones de trabajo basadas en el sesgo del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores
- SageMaker Los modelos [SageMaker.16] deben usar un registro privado en la VPC para los contenedores principales
- [SageMaker.17] SageMaker Las tiendas offline de los grupos de funciones deben cifrarse con AWS KMS claves
- [SageMaker.18] las tiendas en línea de grupos de SageMaker funciones con almacenamiento estándar deben cifrarse con AWS KMS claves
- [SageMaker.19] SageMaker los modelos deben usar un registro privado en la VPC para las canalizaciones de inferencia de varios contenedores
- [SES.1] Las listas de contactos de SES deben estar etiquetadas
- [SES.2] Los conjuntos de configuración de SES deben estar etiquetados
- [SES.3] Los conjuntos de configuración de SES deben tener el TLS habilitado para enviar correos electrónicos

- [SQS.1] Las colas de Amazon SQS deben cifrarse en reposo
- [SQS.2] Las colas de SQS deben estar etiquetadas
- [SQS.3] Las políticas de acceso a las colas de SQS no deberían permitir el acceso público
- [SSM.4] Los documentos SSM no deben ser públicos
- [SSM.7] Los documentos SSM deben tener habilitada la configuración de bloqueo para compartir en público
- [StepFunctions.1] Step Functions indica que las máquinas deben tener el registro activado
- [Transfer.3] Los conectores Transfer Family deben tener habilitado el registro
- [Transfer.4] Los acuerdos Transfer Family deben estar etiquetados
- [WAF.1]AWS WAFEl registro de ACL web global clásico debe estar habilitado
- [WAF.6]AWS WAFLas reglas globales clásicas deben tener al menos una condición
- [WAF.7]AWS WAFLos grupos de reglas globales clásicos deben tener al menos una regla
- [WAF.8]AWS WAFLas ACL web globales clásicas deben tener al menos una regla o grupo de reglas
- [WorkSpaces.1] los volúmenes de WorkSpaces usuarios deben cifrarse en reposo
- [WorkSpaces.2] los volúmenes WorkSpaces raíz deben cifrarse en reposo

Asia-Pacífico (Mumbai)

Los siguientes controles no se admiten en la región Asia-Pacífico (Bombay).

- [AppSync.1]AWS AppSyncLas cachés de las API deben estar cifradas en reposo
- [AppSync.6]AWS AppSyncLas cachés de las API deben cifrarse en tránsito
- [CloudFront.1] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado
- [CloudFront.3] CloudFront las distribuciones deben requerir el cifrado durante el tránsito
- [CloudFront.4] CloudFront las distribuciones deben tener configurada la conmutación por error de origen
- [CloudFront.5] CloudFront las distribuciones deben tener habilitado el registro
- [CloudFront.6] CloudFront las distribuciones deben tener WAF activado
- [CloudFront.7] CloudFront las distribuciones deben usar certificados personalizados SSL/TLS

- [CloudFront.8] CloudFront las distribuciones deben usar el SNI para atender las solicitudes HTTPS
- [CloudFront.9] CloudFront las distribuciones deben cifrar el tráfico para convertirlo en orígenes personalizados
- [CloudFront.10] CloudFront las distribuciones no deben usar protocolos SSL obsoletos entre ubicaciones de borde y orígenes personalizados
- [CloudFront.12] CloudFront las distribuciones no deben apuntar a orígenes de S3 inexistentes
- [CloudFront.13] CloudFront las distribuciones deben usar el control de acceso al origen
- [CloudFront.14] CloudFront las distribuciones deben estar etiquetadas
- [CloudFront.15] CloudFront las distribuciones deben usar la política de seguridad TLS recomendada
- [CloudFront.16] CloudFront las distribuciones deben usar el control de acceso de origen para los orígenes de las URL de las funciones de Lambda
- [CloudFront.17] CloudFront las distribuciones deben usar grupos de claves confiables para las URL y cookies firmadas
- [CodeGuruProfiler.1] Los grupos CodeGuru de creación de perfiles de Profiler deben estar etiquetados
- [CodeGuruReviewer.1] Las asociaciones de repositorios de CodeGuru Reviewer deben estar etiquetadas
- [Connect.1] Los tipos de objetos de los perfiles de clientes de Amazon Connect deben estar etiquetados
- [Connect.2] Las instancias de Connect Customer deben tener el CloudWatch registro habilitado
- [EC2.24] No se deben utilizar los tipos de instancias paravirtuales de Amazon EC2
- [EC2.173] Las solicitudes de EC2 Spot Fleet con parámetros de lanzamiento deberían permitir el cifrado de los volúmenes de EBS adjuntos
- [ECR.4] Los repositorios públicos de ECR deben etiquetarse
- [FraudDetector.1] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.2] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas
- [FraudDetector.3] Los resultados de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.4] Las variables de Amazon Fraud Detector deben estar etiquetadas
- [GlobalAccelerator.1] Los aceleradores de Global Accelerator deben estar etiquetados
- [IAM.26] SSL/TLS Los certificados caducados gestionados en IAM deben eliminarse

- [Inspector.3] El escaneo de código Lambda de Amazon Inspector Lambda debe estar activado
- [IoTTwinMaker.4]AWS TwinMaker Las entidades de IoT deben estar etiquetadas
- [IoTWireless.1]AWSLos grupos de multidifusión de IoT Wireless deben estar etiquetados
- [IoTWireless.2]AWSLos perfiles de servicio de IoT Wireless deben estar etiquetados
- [IoTWireless.3]AWSLas tareas de IoT FUOTA deben estar etiquetadas
- [RDS.31] Los grupos de seguridad de la base de datos de RDS deben etiquetarse
- [Route53.1] Los controles de salud de Route 53 deben estar etiquetados
- [Route53.2] Las zonas alojadas públicas de Route 53 deberían registrar las consultas de DNS
- [S3.24] Los puntos de Multi-Region acceso S3 deben tener habilitada la configuración de bloqueo del acceso público
- [WAF.1]AWS WAFEl registro de ACL web global clásico debe estar habilitado
- [WAF.6]AWS WAFLas reglas globales clásicas deben tener al menos una condición
- [WAF.7]AWS WAFLos grupos de reglas globales clásicos deben tener al menos una regla
- [WAF.8]AWS WAFLas ACL web globales clásicas deben tener al menos una regla o grupo de reglas

Asia-Pacífico (Nueva Zelanda)

Los siguientes controles no se admiten en la región Asia-Pacífico (Nueva Zelanda).

- [ACM.1] ACM-issued Los certificados importados y renovados deben renovarse después de un período de tiempo específico
- [ACM.2] Los certificados RSA gestionados por ACM deben utilizar una longitud de clave de al menos 2048 bits
- [Account.1] La información de contacto de seguridad debe proporcionarse para unCuenta de AWS
- [Account.2]Cuentas de AWSdebe formar parte de unAWS Organizationsorganización
- [APIGateway.1] El registro de ejecución de API y REST de WebSocket API Gateway deben estar habilitados.
- [APIGateway.2] Las etapas de la API REST de API Gateway deben configurarse para usar certificados SSL para la autenticación de backend
- [APIGateway.3] Las etapas de la API REST de API Gateway deben tener AWS X-Ray rastreo habilitado

- [APIGateway.4] API Gateway debe estar asociada a una ACL web de WAF
- [APIGateway.5] Los datos de la caché de la API REST de API Gateway deben cifrarse en reposo
- [APIGateway.8] Las rutas de API Gateway deben especificar un tipo de autorización
- [APIGateway.9] El registro de acceso debe configurarse para las etapas V2 de API Gateway
- [APIGateway.10] Las integraciones de API Gateway V2 deben usar HTTPS para las conexiones privadas
- [APIGateway.11] Los nombres de dominio de API Gateway deben usar las políticas de seguridad recomendadas
- [Amplify.1] Las aplicaciones Amplify deben estar etiquetadas
- [Amplify.2] Amplify branches debe estar etiquetado
- [AppConfig.1]AWS AppConfiglas aplicaciones deben estar etiquetadas
- [AppConfig.2]AWS AppConfiglos perfiles de configuración deben estar etiquetados
- [AppConfig.3]AWS AppConfiglos entornos deben estar etiquetados
- [AppConfig.4]AWS AppConfiglas asociaciones de extensiones deben estar etiquetadas
- [AppFlow.1] AppFlow Los flujos de Amazon deben estar etiquetados
- [AppRunner.1] Los servicios de App Runner deben estar etiquetados
- [AppRunner.2] Los conectores VPC de App Runner deben estar etiquetados
- [AppSync.1]AWS AppSyncLas cachés de las API deben estar cifradas en reposo
- [AppSync.2]AWS AppSyncdebe tener habilitado el registro a nivel de campo
- [AppSync.4]AWS AppSyncLas API de GraphQL deben estar etiquetadas
- [AppSync.5]AWS AppSyncLas API de GraphQL no deben autenticarse con claves de API
- [AppSync.6]AWS AppSyncLas cachés de las API deben cifrarse en tránsito
- [Athena.2] Los catálogos de datos de Athena deben estar etiquetados
- [Athena.3] Los grupos de trabajo de Athena deben estar etiquetados
- [Athena.4] Los grupos de trabajo de Athena deberían tener habilitado el registro
- [AutoScaling.2] El grupo Amazon EC2 Auto Scaling debe cubrir varias zonas de disponibilidad
- [AutoScaling.3] Las configuraciones de lanzamiento grupal de Auto Scaling deberían configurar las instancias EC2 para que requieran la versión 2 del Servicio de Metadatos de Instancia (IMDSv2)
- [AutoScaling.6] Los grupos de Auto Scaling deben usar varios tipos de instancias en múltiples zonas de disponibilidad

- [AutoScaling.9] Los grupos de Amazon EC2 Auto Scaling deben utilizar las plantillas de lanzamiento de Amazon EC2
- [Backup.1]AWS Backuplos puntos de recuperación deben estar cifrados en reposo
- [Backup.2]AWS Backuplos puntos de recuperación deben estar etiquetados
- [Backup.4]AWS Backuplos planes de informes deben estar etiquetados
- [Batch.1] Las colas de trabajos por lotes deben estar etiquetadas
- [Batch.2] Las políticas de programación de lotes deben estar etiquetadas
- [Batch.3] Los entornos de procesamiento por lotes deben etiquetarse
- [Batch.4] Las propiedades de los recursos de cómputo en los entornos de cómputo por lotes gestionados deben estar etiquetadas
- [BedrockAgentCore.1] Los AgentCore tiempos de ejecución de Bedrock deben configurarse con el modo de red VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways debería requerir autorización para las solicitudes entrantes
- [BedrockAgentCore.3] Bedrock AgentCore Memory debe estar cifrada y gestionada por el clienteAWS KMSclaves
- [BedrockAgentCore.4] Bedrock AgentCore Gateway debe cifrarse de forma que sea gestionada por el clienteAWS KMSclaves
- [BedrockAgentCore.5] Los navegadores AgentCore personalizados de Bedrock no deberían usar el modo de red pública
- [BedrockAgentCore.6] Los navegadores AgentCore personalizados de Bedrock deberían tener habilitada la grabación de sesiones
- [CloudFormation.3] las CloudFormation pilas deben tener habilitada la protección de terminación
- [CloudFormation.4] las CloudFormation pilas deben tener funciones de servicio asociadas
- [CloudFront.1] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado
- [CloudFront.3] CloudFront las distribuciones deben requerir el cifrado durante el tránsito
- [CloudFront.4] CloudFront las distribuciones deben tener configurada la conmutación por error de origen
- [CloudFront.5] CloudFront las distribuciones deben tener habilitado el registro
- [CloudFront.6] CloudFront las distribuciones deben tener WAF activado

- [CloudFront.7] CloudFront las distribuciones deben usar certificados personalizados SSL/TLS
- [CloudFront.8] CloudFront las distribuciones deben usar el SNI para atender las solicitudes HTTPS
- [CloudFront.9] CloudFront las distribuciones deben cifrar el tráfico para convertirlo en orígenes personalizados
- [CloudFront.10] CloudFront las distribuciones no deben usar protocolos SSL obsoletos entre ubicaciones de borde y orígenes personalizados
- [CloudFront.12] CloudFront las distribuciones no deben apuntar a orígenes de S3 inexistentes
- [CloudFront.13] CloudFront las distribuciones deben usar el control de acceso al origen
- [CloudFront.14] CloudFront las distribuciones deben estar etiquetadas
- [CloudFront.15] CloudFront las distribuciones deben usar la política de seguridad TLS recomendada
- [CloudFront.16] CloudFront las distribuciones deben usar el control de acceso de origen para los orígenes de las URL de las funciones de Lambda
- [CloudFront.17] CloudFront las distribuciones deben usar grupos de claves confiables para las URL y cookies firmadas
- [CloudTrail.6] Asegúrese de que el depósito de S3 que se utiliza para almacenar CloudTrail los registros no sea de acceso público
- [CloudTrail.7] Asegúrese de que el registro de acceso al bucket de S3 esté habilitado en el CloudTrail bucket de S3
- [CloudTrail.10] Los almacenes de datos de eventos de CloudTrail Lake deben estar cifrados y gestionados por el clienteAWS KMS keys
- [CloudWatch.17] las acciones CloudWatch de alarma deben estar activadas
- [CodeArtifact.1] CodeArtifact los repositorios deben estar etiquetados
- [CodeBuild.1] Las URL del repositorio fuente de CodeBuild Bitbucket no deben contener credenciales confidenciales
- [CodeBuild.2] las variables de entorno CodeBuild del proyecto no deben contener credenciales de texto claro
- [CodeBuild.3] Los registros de CodeBuild S3 deben estar cifrados
- [CodeBuild.4] los entornos de CodeBuild proyectos deben tener un registroAWS ConfigDuración
- [CodeBuild.7] las exportaciones de grupos de CodeBuild informes deben cifrarse en reposo
- [CodeGuruProfiler.1] Los grupos CodeGuru de creación de perfiles de Profiler deben estar etiquetados

- [CodeGuruReviewer.1] Las asociaciones de repositorios de CodeGuru Reviewer deben estar etiquetadas
- [Cognito.1] Los grupos de usuarios de Cognito deben tener activada la protección contra amenazas y el modo de aplicación con todas las funciones para la autenticación estándar
- [Cognito.2] Los grupos de identidades de Cognito no deben permitir identidades no autenticadas
- [Cognito.3] Las políticas de contraseñas para los grupos de usuarios de Cognito deben tener configuraciones sólidas
- [Cognito.4] Los grupos de usuarios de Cognito deben tener activada la protección contra amenazas y el modo de aplicación con todas las funciones para la autenticación personalizada
- [Cognito.5] La MFA debe estar habilitada para los grupos de usuarios de Cognito
- [Cognito.6] Los grupos de usuarios de Cognito deben tener habilitada la protección contra la eliminación
- [Connect.1] Los tipos de objetos de los perfiles de clientes de Amazon Connect deben estar etiquetados
- [Connect.2] Las instancias de Connect Customer deben tener el CloudWatch registro habilitado
- [DataFirehose.1] Los flujos de entrega de Firehose deben cifrarse en reposo
- [DataSync.1] DataSync las tareas deberían tener el registro activado
- [DataSync.2] DataSync las tareas deben estar etiquetadas
- [Detective.1] Los gráficos de comportamiento de los detectives deben estar etiquetados
- [DMS.2] Los certificados DMS deben estar etiquetados
- [DMS.3] Las suscripciones a eventos de DMS deben estar etiquetadas
- [DMS.4] Las instancias de replicación de DMS deben estar etiquetadas
- [DMS.5] Los grupos de subredes de replicación del DMS deben estar etiquetados
- [DMS.6] Las instancias de replicación de DMS deben tener habilitada la actualización automática de las versiones secundarias
- [DMS.7] Las tareas de replicación del DMS para la base de datos de destino deben tener el registro habilitado
- [DMS.8] Las tareas de replicación del DMS para la base de datos de origen deben tener el registro activado
- [DMS.9] Los puntos finales del DMS deben usar SSL
- [DMS.10] Los puntos finales de DMS para las bases de datos de Neptune deben tener habilitada la autorización de IAM

- [DMS.11] Los puntos finales de DMS para MongoDB deben tener un mecanismo de autenticación habilitado
- [DMS.12] Los puntos finales de DMS para Redis OSS deben tener el TLS habilitado
- [DMS.13] Las instancias de replicación de DMS deben configurarse para usar varias zonas de disponibilidad
- [DocumentDB.1] Los clústeres de Amazon DocumentDB deben cifrarse en reposo
- [DocumentDB.2] Los clústeres de Amazon DocumentDB deben tener un período de retención de copias de seguridad adecuado
- [DocumentDB.3] Las instantáneas de clústeres manuales de Amazon DocumentDB no deben ser públicas
- [DocumentDB.4] Los clústeres de Amazon DocumentDB deben publicar los registros de auditoría en Logs CloudWatch
- [DocumentDB.5] Los clústeres de Amazon DocumentDB deben tener habilitada la protección contra eliminaciones
- [DocumentDB.6] Los clústeres de Amazon DocumentDB deben cifrarse en tránsito
- [DynamoDB.3] Los clústeres de DynamoDB Accelerator (DAX) deben cifrarse en reposo
- [DynamoDB.4] Las tablas de DynamoDB deben estar presentes en un plan de respaldo
- [DynamoDB.6] Las tablas de DynamoDB deben tener habilitada la protección de eliminación
- [DynamoDB.7] Los clústeres de DynamoDB Accelerator deben cifrarse en tránsito
- [EC2.4] Las instancias EC2 detenidas deben eliminarse después de un período de tiempo específico
- [EC2.21] Las ACL de red no deberían permitir la entrada desde la versión 0.0.0. 0/0 al puerto 22 o al puerto 3389
- [EC2.22] Deben eliminarse los grupos de seguridad de Amazon EC2 no utilizados
- [EC2.23] Amazon EC2 Transit Gateways no debe aceptar automáticamente las solicitudes de adjuntos de VPC
- [EC2.24] No se deben utilizar los tipos de instancias paravirtuales de Amazon EC2
- [EC2.25] Las plantillas de lanzamiento de Amazon EC2 no deben asignar direcciones IP públicas a las interfaces de red
- [EC2.28] Los volúmenes de EBS deben estar cubiertos por un plan de respaldo
- [EC2.34] Las tablas de rutas de la pasarela de tránsito EC2 deben estar etiquetadas

- [EC2.40] Las pasarelas NAT EC2 deben estar etiquetadas
- [EC2.51] Los puntos finales EC2 Client VPN deben tener habilitado el registro de conexiones de clientes
- [EC2.53] Los grupos de seguridad de EC2 no deberían permitir la entrada desde la versión 0.0.0.0/0 a los puertos de administración remota del servidor
- [EC2.54] Los grupos de seguridad de EC2 no deberían permitir la entrada desde: :/0 a los puertos de administración remota del servidor
- [EC2.55] Las VPC deben configurarse con un punto final de interfaz para la API de ECR
- [EC2.56] Las VPC deben configurarse con un punto final de interfaz para Docker Registry
- [EC2.57] Las VPC deben configurarse con un punto final de interfaz para Systems Manager
- [EC2.58] Las VPC deben configurarse con un punto final de interfaz para los contactos de Systems Manager Incident Manager
- [EC2.60] Las VPC deben configurarse con un punto final de interfaz para Systems Manager Incident Manager
- [EC2.170] Las plantillas de lanzamiento de EC2 deben utilizar la versión 2 del servicio de metadatos de instancias (IMDSv2)
- [EC2.171] Las conexiones VPN de EC2 deberían tener el registro habilitado
- [EC2.172] La configuración de acceso público del bloque de VPC de EC2 debería bloquear el tráfico de la puerta de enlace de Internet
- [EC2.173] Las solicitudes de EC2 Spot Fleet con parámetros de lanzamiento deberían permitir el cifrado de los volúmenes de EBS adjuntos
- [EC2.174] Los conjuntos de opciones DHCP de EC2 deben estar etiquetados
- [EC2.175] Las plantillas de lanzamiento de EC2 deben estar etiquetadas
- [EC2.176] Las listas de prefijos de EC2 deben estar etiquetadas
- [EC2.177] Las sesiones de réplica de tráfico de EC2 deben etiquetarse
- [EC2.178] Los filtros espejo de tráfico EC2 deben estar etiquetados
- [EC2.179] Los objetivos del espejo de tráfico de EC2 deben estar etiquetados
- [EC2.180] Las interfaces de red EC2 deberían tener habilitada source/destination la verificación
- [EC2.181] Las plantillas de lanzamiento de EC2 deberían permitir el cifrado de los volúmenes de EBS adjuntos
- [EC2.182] La configuración de bloqueo de acceso público debe estar habilitada para las instantáneas de Amazon EBS

- [EC2.183] Las conexiones VPN de EC2 deben utilizar el protocolo IKEv2
- [ECR.1] Los repositorios privados de ECR deben tener configurado el escaneo de imágenes
- [ECR.2] Los repositorios privados de ECR deben tener configurada la inmutabilidad de etiquetas
- [ECR.3] Los repositorios de ECR deben tener configurada al menos una política de ciclo de vida
- [ECR.4] Los repositorios públicos de ECR deben etiquetarse
- [ECR.5] Los repositorios de ECR deben estar cifrados y ser gestionados por el cliente AWS KMS keys
- [ECS.3] Las definiciones de tareas de ECS no deben compartir el espacio de nombres del proceso del host
- [ECS.4] Los contenedores ECS deben ejecutarse sin privilegios
- [ECS.5] Las definiciones de tareas de ECS deben configurar los contenedores para que se limiten al acceso de solo lectura a los sistemas de archivos raíz
- [ECS.8] Los secretos no deben transmitirse como variables de entorno de contenedores
- [ECS.9] Las definiciones de tareas de ECS deben tener una configuración de registro
- [ECS.10] Los servicios Fargate de ECS deberían ejecutarse en la última versión de la plataforma Fargate
- [ECS.12] Los clústeres de ECS deben usar Container Insights
- [ECS.16] Los conjuntos de tareas de ECS no deben asignar automáticamente direcciones IP públicas
- [ECS.17] Las definiciones de tareas de ECS no deben usar el modo de red host
- [ECS.18] Las definiciones de tareas de ECS deben utilizar el cifrado en tránsito para los volúmenes de EFS
- [ECS.19] Los proveedores de capacidad de ECS deberían tener habilitada la protección de terminación gestionada
- [ECS.20] Las definiciones de tareas de ECS deben configurar a los usuarios no root en las definiciones de contenedores de Linux
- [ECS.21] Las definiciones de tareas de ECS deberían configurar a los usuarios no administradores en las definiciones de contenedores de Windows
- [EFS.1] Elastic File System debe configurarse para cifrar los datos de los archivos en reposo mediante AWS KMS
- [EFS.2] Los volúmenes de Amazon EFS deben figurar en los planes de copia de seguridad

- [EFS.3] Los puntos de acceso EFS deben exigir un directorio raíz
- [EFS.4] Los puntos de acceso EFS deben exigir la identidad del usuario
- [EFS.6] Los destinos de montaje de EFS no deben asociarse a subredes que asignan direcciones IP públicas en el momento del lanzamiento
- [] Los sistemas de archivos EFS deben tener habilitadas las copias de seguridad automáticas EFS.7
- [EFS.8] Los sistemas de archivos EFS deben cifrarse en reposo
- [EKS.2] Los clústeres de EKS deben ejecutarse en una versión de Kubernetes compatible
- [EKS.3] Los clústeres de EKS deben usar secretos de Kubernetes cifrados
- [EKS.7] Las configuraciones del proveedor de identidad de EKS deben etiquetarse
- [EKS.8] Los clústeres de EKS deben tener habilitado el registro de auditoría
- [EKS.9] Los grupos de nodos de EKS deben ejecutarse en una versión de Kubernetes compatible
- [ELB.2] Los balanceadores de carga clásicos con SSL/HTTPS oyentes deben usar un certificado proporcionado por AWS Gestor de certificados
- [ELB.10] El balanceador de carga clásico debe abarcar varias zonas de disponibilidad
- [ELB.12] El balanceador de carga de aplicaciones debe configurarse con el modo defensivo o de mitigación de desincronización más estricto
- [ELB.13] Los balanceadores de carga de aplicaciones, redes y puertas de enlace deben abarcar varias zonas de disponibilidad
- [ELB.14] El balanceador de carga clásico debe configurarse con el modo defensivo o de mitigación de desincronización más estricto
- [ELB.16] Los balanceadores de carga de aplicaciones deben estar asociados a un AWS WAF ACL web
- [ELB.17] Los balanceadores de cargas de aplicaciones y redes con oyentes deben usar las políticas de seguridad recomendadas
- [ELB.18] Los oyentes del balanceador de cargas de red y aplicaciones deben usar protocolos seguros para cifrar los datos en tránsito
- [ELB.21] Los grupos destinatarios de Application and Network Load Balancer deben utilizar protocolos de control de estado cifrados
- [ELB.22] Los grupos objetivo del ELB deben usar protocolos de transporte cifrados
- [ElastiCache.1] ElastiCache (Redis OSS) los clústeres deben tener habilitadas las copias de seguridad automáticas

- [ElastiCache.2] ElastiCache los clústeres deberían tener habilitadas las actualizaciones automáticas de las versiones secundarias
- [ElastiCache.3] los grupos de ElastiCache replicación deberían tener habilitada la conmutación por error automática
- [ElastiCache.4] los grupos de ElastiCache replicación deben cifrarse en reposo
- [ElastiCache.5] los grupos de ElastiCache replicación deben cifrarse en tránsito
- [ElastiCache.6] ElastiCache (Redis OSS) Los grupos de replicación de versiones anteriores deberían tener habilitada la autenticación de Redis OSS
- [ElastiCache.7] los ElastiCache clústeres no deben usar el grupo de subredes predeterminado
- [ElasticBeanstalk.1] Los entornos de Elastic Beanstalk deberían tener habilitados los informes de estado mejorados
- [ElasticBeanstalk.2] Las actualizaciones de la plataforma gestionada de Elastic Beanstalk deben estar habilitadas
- [ElasticBeanstalk.3] Elastic Beanstalk debería transmitir los registros a CloudWatch
- [EMR.1] Los nodos principales del clúster de Amazon EMR no deben tener direcciones IP públicas
- [EMR.2] La configuración de acceso público del bloque Amazon EMR debe estar habilitada
- [EMR.3] Las configuraciones de seguridad de Amazon EMR deben cifrarse en reposo
- [EMR.4] Las configuraciones de seguridad de Amazon EMR deben cifrarse en tránsito
- [ES.3] Los dominios de Elasticsearch deben cifrar los datos enviados entre nodos
- [ES.4] Debería estar habilitado el registro de errores de dominio de Elasticsearch en Logs CloudWatch
- [ES.9] Los dominios de Elasticsearch deben etiquetarse
- [EventBridge.3] los autobuses de eventos EventBridge personalizados deben tener adjunta una política basada en los recursos
- [EventBridge.4] los puntos finales EventBridge globales deberían tener habilitada la replicación de eventos
- [FraudDetector.1] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.2] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas
- [FraudDetector.3] Los resultados de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.4] Las variables de Amazon Fraud Detector deben estar etiquetadas

- [FSx.1] FSx para sistemas de archivos OpenZFS debe configurarse para copiar etiquetas en copias de seguridad y volúmenes
- [FSx.2] Los sistemas de archivos FSx for Lustre deben configurarse para copiar etiquetas a las copias de seguridad
- [FSx.3] FSx para sistemas de archivos OpenZFS debe configurarse para su implementación Multi-AZ
- [FSx.4] FSx para sistemas de archivos NetApp ONTAP debe configurarse para su implementación Multi-AZ
- [FSx.5] Los sistemas de archivos FSx for Windows File Server deben configurarse para Multi-AZ su implementación
- [GlobalAccelerator.1] Los aceleradores de Global Accelerator deben estar etiquetados
- [Glue.1]AWS Gluelos trabajos deben estar etiquetados
- [Glue.3]AWS GlueLas transformaciones de aprendizaje automático deben cifrarse en reposo
- [Glue.4]AWS GlueLos trabajos de Spark deberían ejecutarse en versiones compatibles deAWS Glue
- [GuardDuty.1] GuardDuty debería estar activado
- GuardDuty Los filtros [GuardDuty.2] deben estar etiquetados
- [GuardDuty.3] Los GuardDuty IPSets deben estar etiquetados
- [GuardDuty.4] GuardDuty los detectores deben estar etiquetados
- [GuardDuty.5] La monitorización del registro de auditoría de GuardDuty EKS debe estar habilitada
- [GuardDuty.6] GuardDuty La protección Lambda debe estar habilitada
- [GuardDuty.7] La monitorización del tiempo de ejecución de GuardDuty EKS debe estar habilitada
- [GuardDuty.8] La protección contra GuardDuty malware para EC2 debe estar habilitada
- [GuardDuty.9] La protección GuardDuty RDS debe estar habilitada
- [GuardDuty.10] La protección GuardDuty S3 debe estar habilitada
- [GuardDuty.11] La monitorización del GuardDuty tiempo de ejecución debe estar habilitada
- [GuardDuty.12] La monitorización del tiempo de ejecución de GuardDuty ECS debe estar habilitada
- [GuardDuty.13] La monitorización del tiempo de ejecución de GuardDuty EC2 debe estar habilitada
- [IAM.1] Las políticas de IAM no deberían permitir todos los privilegios administrativos «*»

- [IAM.2] Los usuarios de IAM no deberían tener políticas de IAM adjuntas
- [IAM.3] Las claves de acceso de los usuarios de IAM deben rotarse cada 90 días o menos
- [IAM.4] La clave de acceso del usuario raíz de IAM no debería existir
- [IAM.5] La MFA debe estar habilitada para todos los usuarios de IAM que tengan una contraseña de consola
- [IAM.6] La MFA de hardware debe estar habilitada para el usuario root
- [IAM.7] Las políticas de contraseñas para los usuarios de IAM deben tener configuraciones sólidas
- [IAM.8] Se deben eliminar las credenciales de usuario de IAM no utilizadas
- [IAM.9] La MFA debe estar habilitada para el usuario root
- [IAM.10] Las políticas de contraseñas para los usuarios de IAM deben tener configuraciones sólidas
- [IAM.11] Asegúrese de que la política de contraseñas de IAM requiera al menos una letra mayúscula
- [IAM.12] Asegúrese de que la política de contraseñas de IAM requiera al menos una letra minúscula
- [IAM.13] Asegúrese de que la política de contraseñas de IAM requiera al menos un símbolo
- [IAM.14] Asegúrese de que la política de contraseñas de IAM requiera al menos un número
- [IAM.15] Asegúrese de que la política de contraseñas de IAM exija una longitud de contraseña mínima de 14 o más
- [IAM.16] Asegúrese de que la política de contraseñas de IAM impida la reutilización de contraseñas
- [IAM.17] Asegúrese de que la política de contraseñas de IAM haga caducar las contraseñas en un plazo de 90 días o menos
- [IAM.18] Asegúrese de que se haya creado una función de soporte para gestionar los incidentes conAWS Support
- [IAM.19] La MFA debe estar habilitada para todos los usuarios de IAM
- [IAM.21] Las políticas de IAM gestionadas por el cliente que cree no deberían permitir acciones comodín en los servicios
- [IAM.22] Se deben eliminar las credenciales de usuario de IAM que no se hayan utilizado durante 45 días
- [IAM.24] Las funciones de IAM deben estar etiquetadas

- [IAM.25] Los usuarios de IAM deben estar etiquetados
- [IAM.26] SSL/TLS Los certificados caducados gestionados en IAM deben eliminarse
- [IAM.27] Las identidades de IAM no deberían tener la AWSCloudShellFullAccess política adjunta
- [IAM.28] El analizador de acceso externo de IAM Access Analyzer debe estar habilitado
- [Inspector.1] El escaneo EC2 de Amazon Inspector debe estar activado
- [Inspector.2] El escaneo ECR de Amazon Inspector debe estar activado
- [Inspector.3] El escaneo de código Lambda de Amazon Inspector Lambda debe estar activado
- [Inspector.4] El escaneo estándar de Amazon Inspector Lambda debe estar activado
- [IoT.1]AWS IoT Device Defenderlos perfiles de seguridad deben estar etiquetados
- [IoT.2]AWS IoT Corelas acciones de mitigación deben estar etiquetadas
- [IoT.3]AWS IoT Corelas dimensiones deben estar etiquetadas
- [IoT.4]AWS IoT Corelos autorizadores deben estar etiquetados
- [IoT.5]AWS IoT CoreLos alias de los roles deben estar etiquetados
- [IoT.6]AWS IoT Corelas políticas deben estar etiquetadas
- [IoTSiteWise.1]AWSLos modelos SiteWise de activos de IoT deben estar etiquetados
- [IoTSiteWise.2]AWS SiteWise Los paneles de IoT deben estar etiquetados
- [IoTSiteWise.3]AWS SiteWise Las pasarelas de IoT deben estar etiquetadas
- [IoTSiteWise.4]AWS SiteWise Los portales de IoT deben estar etiquetados
- [IoTSiteWise.5]AWS SiteWise Los proyectos de IoT deben estar etiquetados
- [IoTTwinMaker.1]AWSLos trabajos de TwinMaker sincronización de IoT deben estar etiquetados
- [IoTTwinMaker.2]AWS TwinMaker Los espacios de trabajo de IoT deben estar etiquetados
- [IoTTwinMaker.3]AWS TwinMaker Las escenas de IoT deben estar etiquetadas
- [IoTTwinMaker.4]AWS TwinMaker Las entidades de IoT deben estar etiquetadas
- [IoTWireless.1]AWSLos grupos de multidifusión de IoT Wireless deben estar etiquetados
- [IoTWireless.2]AWSLos perfiles de servicio de IoT Wireless deben estar etiquetados
- [IoTWireless.3]AWSLas tareas de IoT FUOTA deben estar etiquetadas
- [IVS.1] Los pares de teclas de reproducción IVS deben estar etiquetados
- [IVS.2] Las configuraciones de grabación de IVS deben estar etiquetadas

- [IVS.3] Los canales IVS deben estar etiquetados
- [Keyspaces.1] Los espacios clave de Amazon Keyspaces deben estar etiquetados
- [Kinesis.1] Las transmisiones de Kinesis deben cifrarse en reposo
- [Kinesis.3] Las transmisiones de Kinesis deben tener un período de retención de datos adecuado
- [KMS.1] Las políticas gestionadas por los clientes de IAM no deberían permitir acciones de descifrado en todas las claves de KMS
- [KMS.2] Los directores de IAM no deberían tener políticas integradas de IAM que permitan realizar acciones de descifrado en todas las claves de KMS
- [KMS.5] Las claves KMS no deben ser de acceso público
- [Lambda.5] Las funciones de VPC Lambda deben funcionar en varias zonas de disponibilidad
- [Lambda.7] Las funciones de Lambda deberían tener AWS X-Ray el rastreo activo está habilitado
- [Macie.1] Amazon Macie debería estar activado
- [Macie.2] La detección automática de datos confidenciales por parte de Macie debería estar habilitada
- [MQ.2] Los corredores de ActiveMQ deben transmitir los registros de auditoría a CloudWatch
- [MQ.4] Los corredores de Amazon MQ deben estar etiquetados
- [MQ.5] Los corredores de ActiveMQ deberían usar el modo de implementación active/standby
- [MQ.6] Los corredores de RabbitMQ deberían usar el modo de despliegue de clústeres
- [MSK.1] Los clústeres de MSK deben cifrarse en tránsito entre los nodos de intermediación
- [MSK.2] Los clústeres de MSK deberían tener configurada una supervisión mejorada
- [MSK.3] Los conectores MSK Connect deben estar cifrados en tránsito
- [MSK.4] Los clústeres de MSK deben tener el acceso público deshabilitado
- [MSK.5] Los conectores MSK deben tener el registro activado
- [MSK.6] Los clústeres de MSK deberían deshabilitar el acceso no autenticado
- [Neptune.1] Los clústeres de bases de datos de Neptune deben cifrarse en reposo
- [Neptune.2] Los clústeres de bases de datos de Neptune deberían publicar registros de auditoría en Logs CloudWatch
- [Neptune.3] Las instantáneas del clúster de base de datos de Neptune no deben ser públicas
- [Neptune.4] Los clústeres de base de datos de Neptune deben tener habilitada la protección contra eliminación

- [Neptune.5] Los clústeres de Neptune DB deberían tener habilitadas las copias de seguridad automatizadas
- [Neptune.6] Las instantáneas del clúster de base de datos de Neptune deben cifrarse en reposo
- [Neptune.7] Los clústeres de base de datos de Neptune deben tener habilitada la autenticación de bases de datos de IAM
- [Neptune.8] Los clústeres de bases de datos de Neptune deben configurarse para copiar etiquetas a las instantáneas
- [Neptune.9] Los clústeres de base de datos Neptune deben implementarse en varias zonas de disponibilidad
- [NetworkFirewall.1] Los firewalls de Network Firewall deben implementarse en varias zonas de disponibilidad
- [NetworkFirewall.2] El registro de Network Firewall debe estar habilitado
- [NetworkFirewall.3] Las políticas de Network Firewall deben tener asociado al menos un grupo de reglas
- [NetworkFirewall.4] La acción sin estado predeterminada para las políticas de Network Firewall debe ser eliminar o reenviar paquetes completos
- [NetworkFirewall.5] La acción sin estado predeterminada para las políticas de Network Firewall debe ser eliminar o reenviar paquetes fragmentados
- [NetworkFirewall.6] El grupo de reglas de Stateless Network Firewall no debe estar vacío
- [NetworkFirewall.9] Los firewalls de Network Firewall deben tener habilitada la protección de eliminación
- [NetworkFirewall.10] Los firewalls de Network Firewall deben tener habilitada la protección contra cambios de subred
- [Opensearch.1] OpenSearch los dominios deben tener activado el cifrado en reposo
- [Opensearch.2] OpenSearch los dominios no deben ser de acceso público
- [Opensearch.3] OpenSearch los dominios deben cifrar los datos enviados entre nodos
- [Opensearch.4] El registro de errores de OpenSearch dominio en Logs debe estar habilitado CloudWatch
- [Opensearch.5] OpenSearch los dominios deben tener activado el registro de auditoría
- [Opensearch.6] OpenSearch los dominios deben tener al menos tres nodos de datos
- [Opensearch.7] OpenSearch los dominios deben tener habilitado un control de acceso detallado

- [Opensearch.8] Las conexiones a los OpenSearch dominios deben cifrarse con la última política de seguridad de TLS
- [Opensearch.9] OpenSearch los dominios deben estar etiquetados
- [Opensearch.10] OpenSearch los dominios deben tener instalada la última actualización de software
- [Opensearch.11] OpenSearch los dominios deben tener al menos tres nodos principales dedicados
- [PCA.1]AWS Privada CALa autoridad emisora de certificados raíz debe estar deshabilitada
- [PCA.2]AWSLas autoridades de certificación de CA privadas deben estar etiquetadas
- [RDS.14] Los clústeres de Amazon Aurora deben tener habilitado el retroceso
- [RDS.24] Los clústeres de bases de datos de RDS deben usar un nombre de usuario de administrador personalizado
- [RDS.25] Las instancias de bases de datos de RDS deben usar un nombre de usuario de administrador personalizado
- [RDS.26] Las instancias de base de datos de RDS deben protegerse mediante un plan de respaldo
- [RDS.27] Los clústeres de bases de datos de RDS deben cifrarse en reposo
- [RDS.31] Los grupos de seguridad de la base de datos de RDS deben etiquetarse
- [RDS.34] Los clústeres de bases de datos Aurora MySQL deben publicar los registros de auditoría en Logs CloudWatch
- [RDS.35] Los clústeres de bases de datos de RDS deben tener habilitada la actualización automática de versiones secundarias
- [RDS.36] Las instancias de base de datos de RDS para PostgreSQL deben publicar los registros en Logs CloudWatch
- [RDS.37] Los clústeres de bases de datos de Aurora PostgreSQL deben publicar los registros en Logs CloudWatch
- [RDS.38] Las instancias de base de datos de RDS para PostgreSQL deben cifrarse en tránsito
- [RDS.39] Las instancias de base de datos de RDS para MySQL deben cifrarse en tránsito
- [RDS.40] Las instancias de base de datos de RDS para SQL Server deben publicar los registros en Logs CloudWatch
- [RDS.41] Las instancias de base de datos de RDS para SQL Server deben cifrarse en tránsito
- [RDS.42] Las instancias de base de datos de RDS para MariaDB deben publicar los registros en Logs CloudWatch

- [RDS.43] Los proxies de bases de datos de RDS deben requerir el cifrado TLS para las conexiones
- [RDS.44] Las instancias de base de datos de RDS para MariaDB deben cifrarse durante el tránsito
- [RDS.45] Los clústeres de bases de datos Aurora MySQL deben tener habilitado el registro de auditoría
- [RDS.46] Las instancias de base de datos de RDS no deben implementarse en subredes públicas con rutas a pasarelas de Internet
- [RDS.47] Los clústeres de bases de datos de RDS para PostgreSQL deben configurarse para copiar las etiquetas a las instantáneas de bases de datos
- [RDS.48] Los clústeres de bases de datos de RDS para MySQL deben configurarse para copiar etiquetas a las instantáneas de bases de datos
- [RDS.50] Los clústeres de bases de datos de RDS deben tener un período de retención de copias de seguridad suficiente
- [RDS.51] Los clústeres globales de RDS deben ejecutarse en una versión compatible de Aurora MySQL
- [Redshift.1] Los clústeres de Amazon Redshift deberían prohibir el acceso público
- [Redshift.3] Los clústeres de Amazon Redshift deben tener habilitadas las instantáneas automáticas
- [Redshift.4] Los clústeres de Amazon Redshift deben tener habilitado el registro de auditoría
- [Redshift.6] Amazon Redshift debería tener habilitadas las actualizaciones automáticas a las versiones principales
- [Redshift.7] Los clústeres de Redshift deberían utilizar un enrutamiento de VPC mejorado
- [Redshift.8] Los clústeres de Amazon Redshift no deben usar el nombre de usuario de administrador predeterminado
- [Redshift.10] Los clústeres de Redshift deben cifrarse en reposo
- [Redshift.11] Los clústeres de Redshift deben estar etiquetados
- [Redshift.13] Las instantáneas del clúster de Redshift deben estar etiquetadas
- [Redshift.15] Los grupos de seguridad de Redshift deberían permitir la entrada en el puerto del clúster solo desde orígenes restringidos
- [Redshift.16] Los grupos de subredes de clústeres de Redshift deben tener subredes de varias zonas de disponibilidad

- [Redshift.17] Los grupos de parámetros del clúster de Redshift deben estar etiquetados
- [Redshift.18] Los clústeres de Redshift deberían tener Multi-AZ las implementaciones habilitadas
- [RedshiftServerless.1] Los grupos de trabajo sin servidor de Amazon Redshift deberían utilizar un enrutamiento de VPC mejorado
- [RedshiftServerless.2] Las conexiones a los grupos de trabajo sin servidor de Redshift deberían ser obligatorias para usar SSL
- [RedshiftServerless.3] Los grupos de trabajo sin servidor de Redshift deberían prohibir el acceso público
- [RedshiftServerless.4] Los espacios de nombres de Redshift Serverless deben cifrarse y administrarse por el clienteAWS KMS keys
- [RedshiftServerless.5] Los espacios de nombres Redshift Serverless no deben usar el nombre de usuario de administrador predeterminado
- [RedshiftServerless.6] Los espacios de nombres Redshift Serverless deberían exportar los registros a los registros CloudWatch
- [Route53.1] Los controles de salud de Route 53 deben estar etiquetados
- [Route53.2] Las zonas alojadas públicas de Route 53 deberían registrar las consultas de DNS
- [S3.7] Los cubos de uso general de S3 deben utilizar la replicación entre regiones
- [S3.10] Los cubos de uso general de S3 con el control de versiones habilitado deben tener configuraciones de ciclo de vida
- [S3.11] Los cubos de uso general de S3 deben tener habilitadas las notificaciones de eventos
- [S3.12] Las ACL no deben usarse para administrar el acceso de los usuarios a los cubos de uso general de S3
- [S3.13] Los cubos de uso general de S3 deben tener configuraciones de ciclo de vida
- [S3.19] Los puntos de acceso S3 deben tener habilitada la configuración de bloqueo de acceso público
- [S3.20] Los cubos de uso general de S3 deben tener habilitada la eliminación de MFA
- [S3.22] Los cubos de uso general de S3 deben registrar los eventos de escritura a nivel de objeto
- [S3.23] Los cubos de uso general de S3 deben registrar los eventos de lectura a nivel de objeto
- [S3.24] Los puntos de Multi-Region acceso S3 deben tener habilitada la configuración de bloqueo del acceso público
- [S3.25] Los buckets de directorio de S3 deben tener configuraciones de ciclo de vida

- [SageMaker.1] Las instancias de Amazon SageMaker Notebook no deberían tener acceso directo a Internet
- [SageMaker.2] las instancias de SageMaker cuadernos deben lanzarse en una VPC personalizada
- [SageMaker.3] Los usuarios no deben tener acceso root a las instancias de los SageMaker cuadernos
- [SageMaker.4] Las variantes de producción de SageMaker terminales deben tener un recuento inicial de instancias superior a 1
- SageMaker Los modelos [SageMaker.5] deben tener habilitado el aislamiento de red
- [SageMaker.6] las configuraciones de imagen de la SageMaker aplicación deben estar etiquetadas
- [SageMaker.7] SageMaker las imágenes deben estar etiquetadas
- [SageMaker.8] las instancias de SageMaker notebooks deben ejecutarse en plataformas compatibles
- [SageMaker.9] las definiciones de trabajos de calidad de los SageMaker datos deben tener habilitado el cifrado del tráfico entre contenedores
- [SageMaker.10] Las definiciones de trabajos de explicabilidad del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores
- [SageMaker.11] las definiciones de trabajos SageMaker de calidad de los datos deben tener habilitado el aislamiento de red
- [SageMaker.12] las definiciones de trabajo basadas en el sesgo del SageMaker modelo deben tener habilitado el aislamiento de red
- [SageMaker.13] las definiciones de trabajos de calidad del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores
- [SageMaker.14] los programas SageMaker de monitoreo deben tener habilitado el aislamiento de la red
- [SageMaker.15] Las definiciones de trabajo basadas en el sesgo del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores
- SageMaker Los modelos [SageMaker.16] deben usar un registro privado en la VPC para los contenedores principales
- [SageMaker.17] SageMaker Las tiendas offline de los grupos de funciones deben cifrarse con AWS KMS claves
- [SageMaker.18] las tiendas en línea de grupos de SageMaker funciones con almacenamiento estándar deben cifrarse con AWS KMS claves

- [SageMaker.19] SageMaker los modelos deben usar un registro privado en la VPC para las canalizaciones de inferencia de varios contenedores
- [SES.1] Las listas de contactos de SES deben estar etiquetadas
- [SES.2] Los conjuntos de configuración de SES deben estar etiquetados
- [SES.3] Los conjuntos de configuración de SES deben tener el TLS habilitado para enviar correos electrónicos
- [ServiceCatalog.1] Las carteras de Service Catalog deben compartirse dentro de unAWSsolo una organización
- [SNS.4] Las políticas de acceso a los temas de SNS no deberían permitir el acceso público
- [SQS.1] Las colas de Amazon SQS deben cifrarse en reposo
- [SQS.2] Las colas de SQS deben estar etiquetadas
- [SQS.3] Las políticas de acceso a las colas de SQS no deberían permitir el acceso público
- [SSM.1] Las instancias de Amazon EC2 deben administrarse medianteAWS Systems Manager
- [SSM.2] Las instancias de Amazon EC2 administradas por Systems Manager deben tener el estado de conformidad con los parches de CONFORMIDAD CON LOS PARCHES tras la instalación de un parche
- [SSM.3] Las instancias de Amazon EC2 administradas por Systems Manager deben tener el estado de conformidad de la asociación de COMPLIANT
- [SSM.4] Los documentos SSM no deben ser públicos
- [SSM.5] Los documentos SSM deben estar etiquetados
- [SSM.6] SSM Automation debería tener el registro habilitado CloudWatch
- [SSM.7] Los documentos SSM deben tener habilitada la configuración de bloqueo para compartir en público
- [StepFunctions.1] Step Functions indica que las máquinas deben tener el registro activado
- [Transfer.1]AWS Transfer Familylos flujos de trabajo deben estar etiquetados
- [Transfer.2] Los servidores Transfer Family no deben usar el protocolo FTP para la conexión de puntos finales
- [Transfer.3] Los conectores Transfer Family deben tener habilitado el registro
- [Transfer.4] Los acuerdos Transfer Family deben estar etiquetados
- [Transfer.5] Los certificados Transfer Family deben estar etiquetados

- [Transfer.6] Los conectores Transfer Family deben estar etiquetados
- [Transfer.7] Los perfiles de Transfer Family deben estar etiquetados
- [WAF.1]AWS WAFEl registro de ACL web global clásico debe estar habilitado
- [WAF.2]AWS WAFLas reglas regionales clásicas deben tener al menos una condición
- [WAF.3]AWS WAFLos grupos de reglas regionales clásicos deben tener al menos una regla
- [WAF.4]AWS WAFLas ACL web regionales clásicas deben tener al menos una regla o grupo de reglas
- [WAF.6]AWS WAFLas reglas globales clásicas deben tener al menos una condición
- [WAF.7]AWS WAFLos grupos de reglas globales clásicos deben tener al menos una regla
- [WAF.8]AWS WAFLas ACL web globales clásicas deben tener al menos una regla o grupo de reglas
- [WAF.10]AWS WAFLas ACL web deben tener al menos una regla o grupo de reglas
- [WAF.11]AWS WAFEl registro de ACL web debe estar habilitado
- [WAF.12]AWS WAFlas reglas deben tener CloudWatch las métricas habilitadas
- [WorkSpaces.1] los volúmenes de WorkSpaces usuarios deben cifrarse en reposo
- [WorkSpaces.2] los volúmenes WorkSpaces raíz deben cifrarse en reposo

Asia-Pacífico (Osaka)

Los siguientes controles no se admiten en la región Asia-Pacífico (Osaka).

- [AppFlow.1] AppFlow Los flujos de Amazon deben estar etiquetados
- [AppRunner.1] Los servicios de App Runner deben estar etiquetados
- [AppRunner.2] Los conectores VPC de App Runner deben estar etiquetados
- [AppSync.1]AWS AppSyncLas cachés de las API deben estar cifradas en reposo
- [AppSync.6]AWS AppSyncLas cachés de las API deben cifrarse en tránsito
- [Backup.1]AWS Backuplos puntos de recuperación deben estar cifrados en reposo
- [BedrockAgentCore.1] Los AgentCore tiempos de ejecución de Bedrock deben configurarse con el modo de red VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways debería requerir autorización para las solicitudes entrantes

- [BedrockAgentCore.3] Bedrock AgentCore Memory debe estar cifrada y gestionada por el clienteAWS KMSclaves
- [BedrockAgentCore.4] Bedrock AgentCore Gateway debe cifrarse de forma que sea gestionada por el clienteAWS KMSclaves
- [BedrockAgentCore.5] Los navegadores AgentCore personalizados de Bedrock no deberían usar el modo de red pública
- [BedrockAgentCore.6] Los navegadores AgentCore personalizados de Bedrock deberían tener habilitada la grabación de sesiones
- [CloudFront.1] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado
- [CloudFront.3] CloudFront las distribuciones deben requerir el cifrado durante el tránsito
- [CloudFront.4] CloudFront las distribuciones deben tener configurada la conmutación por error de origen
- [CloudFront.5] CloudFront las distribuciones deben tener habilitado el registro
- [CloudFront.6] CloudFront las distribuciones deben tener WAF activado
- [CloudFront.7] CloudFront las distribuciones deben usar certificados personalizados SSL/TLS
- [CloudFront.8] CloudFront las distribuciones deben usar el SNI para atender las solicitudes HTTPS
- [CloudFront.9] CloudFront las distribuciones deben cifrar el tráfico para convertirlo en orígenes personalizados
- [CloudFront.10] CloudFront las distribuciones no deben usar protocolos SSL obsoletos entre ubicaciones de borde y orígenes personalizados
- [CloudFront.12] CloudFront las distribuciones no deben apuntar a orígenes de S3 inexistentes
- [CloudFront.13] CloudFront las distribuciones deben usar el control de acceso al origen
- [CloudFront.14] CloudFront las distribuciones deben estar etiquetadas
- [CloudFront.15] CloudFront las distribuciones deben usar la política de seguridad TLS recomendada
- [CloudFront.16] CloudFront las distribuciones deben usar el control de acceso de origen para los orígenes de las URL de las funciones de Lambda
- [CloudFront.17] CloudFront las distribuciones deben usar grupos de claves confiables para las URL y cookies firmadas
- [CodeArtifact.1] CodeArtifact los repositorios deben estar etiquetados

- [CodeGuruProfiler.1] Los grupos CodeGuru de creación de perfiles de Profiler deben estar etiquetados
- [CodeGuruReviewer.1] Las asociaciones de repositorios de CodeGuru Reviewer deben estar etiquetadas
- [Connect.1] Los tipos de objetos de los perfiles de clientes de Amazon Connect deben estar etiquetados
- [Connect.2] Las instancias de Connect Customer deben tener el CloudWatch registro habilitado
- [Detective.1] Los gráficos de comportamiento de los detectives deben estar etiquetados
- [DMS.7] Las tareas de replicación del DMS para la base de datos de destino deben tener el registro habilitado
- [DMS.8] Las tareas de replicación del DMS para la base de datos de origen deben tener el registro activado
- [DMS.10] Los puntos finales de DMS para las bases de datos de Neptune deben tener habilitada la autorización de IAM
- [DocumentDB.1] Los clústeres de Amazon DocumentDB deben cifrarse en reposo
- [DocumentDB.2] Los clústeres de Amazon DocumentDB deben tener un período de retención de copias de seguridad adecuado
- [DocumentDB.3] Las instantáneas de clústeres manuales de Amazon DocumentDB no deben ser públicas
- [DocumentDB.4] Los clústeres de Amazon DocumentDB deben publicar los registros de auditoría en Logs CloudWatch
- [DocumentDB.5] Los clústeres de Amazon DocumentDB deben tener habilitada la protección contra eliminaciones
- [DocumentDB.6] Los clústeres de Amazon DocumentDB deben cifrarse en tránsito
- [DynamoDB.3] Los clústeres de DynamoDB Accelerator (DAX) deben cifrarse en reposo
- [DynamoDB.7] Los clústeres de DynamoDB Accelerator deben cifrarse en tránsito
- [EC2.4] Las instancias EC2 detenidas deben eliminarse después de un período de tiempo específico
- [EC2.14] Los grupos de seguridad no deberían permitir la entrada desde la versión 0.0.0. 0/0 o: :/0 al puerto 3389
- [EC2.22] Deben eliminarse los grupos de seguridad de Amazon EC2 no utilizados

- [EC2.23] Amazon EC2 Transit Gateways no debe aceptar automáticamente las solicitudes de adjuntos de VPC
- [EC2.24] No se deben utilizar los tipos de instancias paravirtuales de Amazon EC2
- [EC2.55] Las VPC deben configurarse con un punto final de interfaz para la API de ECR
- [EC2.56] Las VPC deben configurarse con un punto final de interfaz para Docker Registry
- [EC2.57] Las VPC deben configurarse con un punto final de interfaz para Systems Manager
- [EC2.58] Las VPC deben configurarse con un punto final de interfaz para los contactos de Systems Manager Incident Manager
- [EC2.60] Las VPC deben configurarse con un punto final de interfaz para Systems Manager Incident Manager
- [EC2.173] Las solicitudes de EC2 Spot Fleet con parámetros de lanzamiento deberían permitir el cifrado de los volúmenes de EBS adjuntos
- [ECR.4] Los repositorios públicos de ECR deben etiquetarse
- [ELB.2] Los balanceadores de carga clásicos con SSL/HTTPS oyentes deben usar un certificado proporcionado por AWS Gestor de certificados
- [ElastiCache.1] ElastiCache (Redis OSS) los clústeres deben tener habilitadas las copias de seguridad automáticas
- [ElastiCache.7] los ElastiCache clústeres no deben usar el grupo de subredes predeterminado
- [ElasticBeanstalk.1] Los entornos de Elastic Beanstalk deberían tener habilitados los informes de estado mejorados
- [FraudDetector.1] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.2] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas
- [FraudDetector.3] Los resultados de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.4] Las variables de Amazon Fraud Detector deben estar etiquetadas
- [GlobalAccelerator.1] Los aceleradores de Global Accelerator deben estar etiquetados
- [IAM.26] SSL/TLS Los certificados caducados gestionados en IAM deben eliminarse
- [Inspector.3] El escaneo de código Lambda de Amazon Inspector Lambda debe estar activado
- [IoT.1]AWS IoT Device Defenderlos perfiles de seguridad deben estar etiquetados
- [IoT.2]AWS IoT Corelas acciones de mitigación deben estar etiquetadas
- [IoT.3]AWS IoT Corelas dimensiones deben estar etiquetadas

- [IoT.4]AWS IoT Corelos autorizadores deben estar etiquetados
- [IoT.5]AWS IoT CoreLos alias de los roles deben estar etiquetados
- [IoT.6]AWS IoT Corelas políticas deben estar etiquetadas
- [IoTSiteWise.1]AWSLos modelos SiteWise de activos de IoT deben estar etiquetados
- [IoTSiteWise.2]AWS SiteWise Los paneles de IoT deben estar etiquetados
- [IoTSiteWise.3]AWS SiteWise Las pasarelas de IoT deben estar etiquetadas
- [IoTSiteWise.4]AWS SiteWise Los portales de IoT deben estar etiquetados
- [IoTSiteWise.5]AWS SiteWise Los proyectos de IoT deben estar etiquetados
- [IoTTwinMaker.1]AWSLos trabajos de TwinMaker sincronización de IoT deben estar etiquetados
- [IoTTwinMaker.2]AWS TwinMaker Los espacios de trabajo de IoT deben estar etiquetados
- [IoTTwinMaker.3]AWS TwinMaker Las escenas de IoT deben estar etiquetadas
- [IoTTwinMaker.4]AWS TwinMaker Las entidades de IoT deben estar etiquetadas
- [IoTWireless.1]AWSLos grupos de multidifusión de IoT Wireless deben estar etiquetados
- [IoTWireless.2]AWSLos perfiles de servicio de IoT Wireless deben estar etiquetados
- [IoTWireless.3]AWSLas tareas de IoT FUOTA deben estar etiquetadas
- [IVS.1] Los pares de teclas de reproducción IVS deben estar etiquetados
- [IVS.2] Las configuraciones de grabación de IVS deben estar etiquetadas
- [IVS.3] Los canales IVS deben estar etiquetados
- [Keyspaces.1] Los espacios clave de Amazon Keyspaces deben estar etiquetados
- [MSK.3] Los conectores MSK Connect deben estar cifrados en tránsito
- [MSK.5] Los conectores MSK deben tener el registro activado
- [RDS.31] Los grupos de seguridad de la base de datos de RDS deben etiquetarse
- [RedshiftServerless.1] Los grupos de trabajo sin servidor de Amazon Redshift deberían utilizar un enrutamiento de VPC mejorado
- [RedshiftServerless.2] Las conexiones a los grupos de trabajo sin servidor de Redshift deberían ser obligatorias para usar SSL
- [RedshiftServerless.3] Los grupos de trabajo sin servidor de Redshift deberían prohibir el acceso público
- [RedshiftServerless.4] Los espacios de nombres de Redshift Serverless deben cifrarse y administrarse por el clienteAWS KMS keys

- [RedshiftServerless.5] Los espacios de nombres Redshift Serverless no deben usar el nombre de usuario de administrador predeterminado
- [RedshiftServerless.6] Los espacios de nombres Redshift Serverless deberían exportar los registros a los registros CloudWatch
- [Route53.1] Los controles de salud de Route 53 deben estar etiquetados
- [Route53.2] Las zonas alojadas públicas de Route 53 deberían registrar las consultas de DNS
- [S3.24] Los puntos de Multi-Region acceso S3 deben tener habilitada la configuración de bloqueo del acceso público
- [S3.25] Los buckets de directorio de S3 deben tener configuraciones de ciclo de vida
- SageMaker Los modelos [SageMaker.16] deben usar un registro privado en la VPC para los contenedores principales
- [SageMaker.19] SageMaker los modelos deben usar un registro privado en la VPC para las canalizaciones de inferencia de varios contenedores
- [SSM.2] Las instancias de Amazon EC2 administradas por Systems Manager deben tener el estado de conformidad con los parches de CONFORMIDAD CON LOS PARCHES tras la instalación de un parche
- [SSM.3] Las instancias de Amazon EC2 administradas por Systems Manager deben tener el estado de conformidad de la asociación de COMPLIANT
- [WAF.1]AWS WAFEl registro de ACL web global clásico debe estar habilitado
- [WAF.3]AWS WAFLos grupos de reglas regionales clásicos deben tener al menos una regla
- [WAF.6]AWS WAFLas reglas globales clásicas deben tener al menos una condición
- [WAF.7]AWS WAFLos grupos de reglas globales clásicos deben tener al menos una regla
- [WAF.8]AWS WAFLas ACL web globales clásicas deben tener al menos una regla o grupo de reglas
- [WAF.10]AWS WAFLas ACL web deben tener al menos una regla o grupo de reglas
- [WorkSpaces.1] los volúmenes de WorkSpaces usuarios deben cifrarse en reposo
- [WorkSpaces.2] los volúmenes WorkSpaces raíz deben cifrarse en reposo

Asia-Pacífico (Seúl)

Los siguientes controles no se admiten en la región Asia-Pacífico (Seúl).

- [AppRunner.1] Los servicios de App Runner deben estar etiquetados
- [AppRunner.2] Los conectores VPC de App Runner deben estar etiquetados
- [AppSync.1]AWS AppSyncLas cachés de las API deben estar cifradas en reposo
- [AppSync.6]AWS AppSyncLas cachés de las API deben cifrarse en tránsito
- [BedrockAgentCore.3] Bedrock AgentCore Memory debe estar cifrada y gestionada por el clienteAWS KMSclaves
- [CloudFront.1] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado
- [CloudFront.3] CloudFront las distribuciones deben requerir el cifrado durante el tránsito
- [CloudFront.4] CloudFront las distribuciones deben tener configurada la conmutación por error de origen
- [CloudFront.5] CloudFront las distribuciones deben tener habilitado el registro
- [CloudFront.6] CloudFront las distribuciones deben tener WAF activado
- [CloudFront.7] CloudFront las distribuciones deben usar certificados personalizados SSL/TLS
- [CloudFront.8] CloudFront las distribuciones deben usar el SNI para atender las solicitudes HTTPS
- [CloudFront.9] CloudFront las distribuciones deben cifrar el tráfico para convertirlo en orígenes personalizados
- [CloudFront.10] CloudFront las distribuciones no deben usar protocolos SSL obsoletos entre ubicaciones de borde y orígenes personalizados
- [CloudFront.12] CloudFront las distribuciones no deben apuntar a orígenes de S3 inexistentes
- [CloudFront.13] CloudFront las distribuciones deben usar el control de acceso al origen
- [CloudFront.14] CloudFront las distribuciones deben estar etiquetadas
- [CloudFront.15] CloudFront las distribuciones deben usar la política de seguridad TLS recomendada
- [CloudFront.16] CloudFront las distribuciones deben usar el control de acceso de origen para los orígenes de las URL de las funciones de Lambda
- [CloudFront.17] CloudFront las distribuciones deben usar grupos de claves confiables para las URL y cookies firmadas
- [CodeArtifact.1] CodeArtifact los repositorios deben estar etiquetados
- [CodeGuruProfiler.1] Los grupos CodeGuru de creación de perfiles de Profiler deben estar etiquetados

- [CodeGuruReviewer.1] Las asociaciones de repositorios de CodeGuru Reviewer deben estar etiquetadas
- [Cognito.2] Los grupos de identidades de Cognito no deben permitir identidades no autenticadas
- [DynamoDB.3] Los clústeres de DynamoDB Accelerator (DAX) deben cifrarse en reposo
- [DynamoDB.7] Los clústeres de DynamoDB Accelerator deben cifrarse en tránsito
- [EC2.24] No se deben utilizar los tipos de instancias paravirtuales de Amazon EC2
- [EC2.173] Las solicitudes de EC2 Spot Fleet con parámetros de lanzamiento deberían permitir el cifrado de los volúmenes de EBS adjuntos
- [EC2.180] Las interfaces de red EC2 deberían tener habilitada source/destination la verificación
- [ECR.4] Los repositorios públicos de ECR deben etiquetarse
- [ELB.18] Los oyentes del balanceador de cargas de red y aplicaciones deben usar protocolos seguros para cifrar los datos en tránsito
- [FraudDetector.1] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.2] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas
- [FraudDetector.3] Los resultados de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.4] Las variables de Amazon Fraud Detector deben estar etiquetadas
- [GlobalAccelerator.1] Los aceleradores de Global Accelerator deben estar etiquetados
- [Glue.4]AWS GlueLos trabajos de Spark deberían ejecutarse en versiones compatibles deAWS Glue
- [IAM.26] SSL/TLS Los certificados caducados gestionados en IAM deben eliminarse
- [Inspector.3] El escaneo de código Lambda de Amazon Inspector Lambda debe estar activado
- [IoTTwinMaker.4]AWS TwinMaker Las entidades de IoT deben estar etiquetadas
- [IoTWireless.1]AWSLos grupos de multidifusión de IoT Wireless deben estar etiquetados
- [IoTWireless.2]AWSLos perfiles de servicio de IoT Wireless deben estar etiquetados
- [IoTWireless.3]AWSLas tareas de IoT FUOTA deben estar etiquetadas
- [Lambda.7] Las funciones de Lambda deberían tener AWS X-Ray el rastreo activo está habilitado
- [RDS.31] Los grupos de seguridad de la base de datos de RDS deben etiquetarse
- [Redshift.18] Los clústeres de Redshift deberían tener Multi-AZ las implementaciones habilitadas
- [Route53.1] Los controles de salud de Route 53 deben estar etiquetados

- [Route53.2] Las zonas alojadas públicas de Route 53 deberían registrar las consultas de DNS
- [S3.24] Los puntos de Multi-Region acceso S3 deben tener habilitada la configuración de bloqueo del acceso público
- [S3.25] Los buckets de directorio de S3 deben tener configuraciones de ciclo de vida
- [SageMaker.19] SageMaker los modelos deben usar un registro privado en la VPC para las canalizaciones de inferencia de varios contenedores
- [SSM.6] SSM Automation debería tener el registro habilitado CloudWatch
- [SSM.7] Los documentos SSM deben tener habilitada la configuración de bloqueo para compartir en público
- [WAF.1]AWS WAFEl registro de ACL web global clásico debe estar habilitado
- [WAF.6]AWS WAFLas reglas globales clásicas deben tener al menos una condición
- [WAF.7]AWS WAFLos grupos de reglas globales clásicos deben tener al menos una regla
- [WAF.8]AWS WAFLas ACL web globales clásicas deben tener al menos una regla o grupo de reglas

Asia-Pacífico (Singapur)

Los siguientes controles no se admiten en la región Asia-Pacífico (Singapur).

- [AppSync.1]AWS AppSyncLas cachés de las API deben estar cifradas en reposo
- [AppSync.6]AWS AppSyncLas cachés de las API deben cifrarse en tránsito
- [CloudFront.1] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado
- [CloudFront.3] CloudFront las distribuciones deben requerir el cifrado durante el tránsito
- [CloudFront.4] CloudFront las distribuciones deben tener configurada la conmutación por error de origen
- [CloudFront.5] CloudFront las distribuciones deben tener habilitado el registro
- [CloudFront.6] CloudFront las distribuciones deben tener WAF activado
- [CloudFront.7] CloudFront las distribuciones deben usar certificados personalizados SSL/TLS
- [CloudFront.8] CloudFront las distribuciones deben usar el SNI para atender las solicitudes HTTPS
- [CloudFront.9] CloudFront las distribuciones deben cifrar el tráfico para convertirlo en orígenes personalizados

- [CloudFront.10] CloudFront las distribuciones no deben usar protocolos SSL obsoletos entre ubicaciones de borde y orígenes personalizados
- [CloudFront.12] CloudFront las distribuciones no deben apuntar a orígenes de S3 inexistentes
- [CloudFront.13] CloudFront las distribuciones deben usar el control de acceso al origen
- [CloudFront.14] CloudFront las distribuciones deben estar etiquetadas
- [CloudFront.15] CloudFront las distribuciones deben usar la política de seguridad TLS recomendada
- [CloudFront.16] CloudFront las distribuciones deben usar el control de acceso de origen para los orígenes de las URL de las funciones de Lambda
- [CloudFront.17] CloudFront las distribuciones deben usar grupos de claves confiables para las URL y cookies firmadas
- [EC2.173] Las solicitudes de EC2 Spot Fleet con parámetros de lanzamiento deberían permitir el cifrado de los volúmenes de EBS adjuntos
- [ECR.4] Los repositorios públicos de ECR deben etiquetarse
- [GlobalAccelerator.1] Los aceleradores de Global Accelerator deben estar etiquetados
- [IAM.26] SSL/TLS Los certificados caducados gestionados en IAM deben eliminarse
- [IoTWireless.1]AWSLos grupos de multidifusión de IoT Wireless deben estar etiquetados
- [IoTWireless.2]AWSLos perfiles de servicio de IoT Wireless deben estar etiquetados
- [IoTWireless.3]AWSLas tareas de IoT FUOTA deben estar etiquetadas
- [IVS.1] Los pares de teclas de reproducción IVS deben estar etiquetados
- [IVS.2] Las configuraciones de grabación de IVS deben estar etiquetadas
- [IVS.3] Los canales IVS deben estar etiquetados
- [Route53.1] Los controles de salud de Route 53 deben estar etiquetados
- [Route53.2] Las zonas alojadas públicas de Route 53 deberían registrar las consultas de DNS
- [S3.24] Los puntos de Multi-Region acceso S3 deben tener habilitada la configuración de bloqueo del acceso público
- [S3.25] Los buckets de directorio de S3 deben tener configuraciones de ciclo de vida
- [WAF.1]AWS WAFEl registro de ACL web global clásico debe estar habilitado
- [WAF.6]AWS WAFLas reglas globales clásicas deben tener al menos una condición
- [WAF.7]AWS WAFLos grupos de reglas globales clásicos deben tener al menos una regla

- [WAF.8]AWS WAFLas ACL web globales clásicas deben tener al menos una regla o grupo de reglas

Asia-Pacífico (Sídney)

Los siguientes controles no se admiten en la región Asia-Pacífico (Sídney).

- [AppSync.1]AWS AppSyncLas cachés de las API deben estar cifradas en reposo
- [AppSync.6]AWS AppSyncLas cachés de las API deben cifrarse en tránsito
- [CloudFront.1] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado
- [CloudFront.3] CloudFront las distribuciones deben requerir el cifrado durante el tránsito
- [CloudFront.4] CloudFront las distribuciones deben tener configurada la conmutación por error de origen
- [CloudFront.5] CloudFront las distribuciones deben tener habilitado el registro
- [CloudFront.6] CloudFront las distribuciones deben tener WAF activado
- [CloudFront.7] CloudFront las distribuciones deben usar certificados personalizados SSL/TLS
- [CloudFront.8] CloudFront las distribuciones deben usar el SNI para atender las solicitudes HTTPS
- [CloudFront.9] CloudFront las distribuciones deben cifrar el tráfico para convertirlo en orígenes personalizados
- [CloudFront.10] CloudFront las distribuciones no deben usar protocolos SSL obsoletos entre ubicaciones de borde y orígenes personalizados
- [CloudFront.12] CloudFront las distribuciones no deben apuntar a orígenes de S3 inexistentes
- [CloudFront.13] CloudFront las distribuciones deben usar el control de acceso al origen
- [CloudFront.14] CloudFront las distribuciones deben estar etiquetadas
- [CloudFront.15] CloudFront las distribuciones deben usar la política de seguridad TLS recomendada
- [CloudFront.16] CloudFront las distribuciones deben usar el control de acceso de origen para los orígenes de las URL de las funciones de Lambda
- [CloudFront.17] CloudFront las distribuciones deben usar grupos de claves confiables para las URL y cookies firmadas
- [EC2.173] Las solicitudes de EC2 Spot Fleet con parámetros de lanzamiento deberían permitir el cifrado de los volúmenes de EBS adjuntos

- [ECR.4] Los repositorios públicos de ECR deben etiquetarse
- [GlobalAccelerator.1] Los aceleradores de Global Accelerator deben estar etiquetados
- [IAM.26] SSL/TLS Los certificados caducados gestionados en IAM deben eliminarse
- [IVS.1] Los pares de teclas de reproducción IVS deben estar etiquetados
- [IVS.2] Las configuraciones de grabación de IVS deben estar etiquetadas
- [IVS.3] Los canales IVS deben estar etiquetados
- [Route53.1] Los controles de salud de Route 53 deben estar etiquetados
- [Route53.2] Las zonas alojadas públicas de Route 53 deberían registrar las consultas de DNS
- [S3.24] Los puntos de Multi-Region acceso S3 deben tener habilitada la configuración de bloqueo del acceso público
- [S3.25] Los buckets de directorio de S3 deben tener configuraciones de ciclo de vida
- [WAF.1]AWS WAFEl registro de ACL web global clásico debe estar habilitado
- [WAF.6]AWS WAFLas reglas globales clásicas deben tener al menos una condición
- [WAF.7]AWS WAFLos grupos de reglas globales clásicos deben tener al menos una regla
- [WAF.8]AWS WAFLas ACL web globales clásicas deben tener al menos una regla o grupo de reglas

Asia-Pacífico (Taipéi)

Los siguientes controles no se admiten en la región Asia-Pacífico (Taipéi).

- [ACM.1] ACM-issued Los certificados importados y renovados deben renovarse después de un período de tiempo específico
- [ACM.2] Los certificados RSA gestionados por ACM deben utilizar una longitud de clave de al menos 2048 bits
- [ACM.3] Los certificados ACM deben estar etiquetados
- [Account.1] La información de contacto de seguridad debe proporcionarse para unCuenta de AWS
- [Account.2]Cuentas de AWSdebe formar parte de unAWS Organizationsorganización
- [APIGateway.1] El registro de ejecución de API y REST de WebSocket API Gateway deben estar habilitados.
- [APIGateway.2] Las etapas de la API REST de API Gateway deben configurarse para usar certificados SSL para la autenticación de backend

- [APIGateway.3] Las etapas de la API REST de API Gateway deben tener AWS X-Ray rastreo habilitado
- [APIGateway.4] API Gateway debe estar asociada a una ACL web de WAF
- [APIGateway.5] Los datos de la caché de la API REST de API Gateway deben cifrarse en reposo
- [APIGateway.8] Las rutas de API Gateway deben especificar un tipo de autorización
- [APIGateway.9] El registro de acceso debe configurarse para las etapas V2 de API Gateway
- [APIGateway.10] Las integraciones de API Gateway V2 deben usar HTTPS para las conexiones privadas
- [APIGateway.11] Los nombres de dominio de API Gateway deben usar las políticas de seguridad recomendadas
- [Amplify.1] Las aplicaciones Amplify deben estar etiquetadas
- [Amplify.2] Amplify branches debe estar etiquetado
- [AppConfig.1]AWS AppConfiglas aplicaciones deben estar etiquetadas
- [AppConfig.2]AWS AppConfiglos perfiles de configuración deben estar etiquetados
- [AppConfig.3]AWS AppConfiglos entornos deben estar etiquetados
- [AppConfig.4]AWS AppConfiglas asociaciones de extensiones deben estar etiquetadas
- [AppFlow.1] AppFlow Los flujos de Amazon deben estar etiquetados
- [AppRunner.1] Los servicios de App Runner deben estar etiquetados
- [AppRunner.2] Los conectores VPC de App Runner deben estar etiquetados
- [AppSync.1]AWS AppSyncLas cachés de las API deben estar cifradas en reposo
- [AppSync.2]AWS AppSyncdebe tener habilitado el registro a nivel de campo
- [AppSync.4]AWS AppSyncLas API de GraphQL deben estar etiquetadas
- [AppSync.5]AWS AppSyncLas API de GraphQL no deben autenticarse con claves de API
- [AppSync.6]AWS AppSyncLas cachés de las API deben cifrarse en tránsito
- [Athena.2] Los catálogos de datos de Athena deben estar etiquetados
- [Athena.3] Los grupos de trabajo de Athena deben estar etiquetados
- [Athena.4] Los grupos de trabajo de Athena deberían tener habilitado el registro
- [AutoScaling.1] Los grupos de Auto Scaling asociados a un balanceador de cargas deben usar comprobaciones de estado del ELB
- [AutoScaling.2] El grupo Amazon EC2 Auto Scaling debe cubrir varias zonas de disponibilidad

- [AutoScaling.3] Las configuraciones de lanzamiento grupal de Auto Scaling deberían configurar las instancias EC2 para que requieran la versión 2 del Servicio de Metadatos de Instancia (IMDSv2)
- [AutoScaling.6] Los grupos de Auto Scaling deben usar varios tipos de instancias en múltiples zonas de disponibilidad
- [AutoScaling.9] Los grupos de Amazon EC2 Auto Scaling deben utilizar las plantillas de lanzamiento de Amazon EC2
- [AutoScaling.10] Los grupos de Auto Scaling de EC2 deben estar etiquetados
- [Autoscaling.5] Las instancias de Amazon EC2 lanzadas mediante configuraciones de lanzamiento grupal de Auto Scaling no deben tener direcciones IP públicas
- [Backup.1]AWS Backuplos puntos de recuperación deben estar cifrados en reposo
- [Backup.2]AWS Backuplos puntos de recuperación deben estar etiquetados
- [Backup.3]AWS Backuplas bóvedas deben estar etiquetadas
- [Backup.4]AWS Backuplos planes de informes deben estar etiquetados
- [Backup.5]AWS Backuplos planes de respaldo deben estar etiquetados
- [Batch.1] Las colas de trabajos por lotes deben estar etiquetadas
- [Batch.2] Las políticas de programación de lotes deben estar etiquetadas
- [Batch.3] Los entornos de procesamiento por lotes deben etiquetarse
- [Batch.4] Las propiedades de los recursos de cómputo en los entornos de cómputo por lotes gestionados deben estar etiquetadas
- [BedrockAgentCore.1] Los AgentCore tiempos de ejecución de Bedrock deben configurarse con el modo de red VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways debería requerir autorización para las solicitudes entrantes
- [BedrockAgentCore.3] Bedrock AgentCore Memory debe estar cifrada y gestionada por el clienteAWS KMSclaves
- [BedrockAgentCore.4] Bedrock AgentCore Gateway debe cifrarse de forma que sea gestionada por el clienteAWS KMSclaves
- [BedrockAgentCore.5] Los navegadores AgentCore personalizados de Bedrock no deberían usar el modo de red pública
- [BedrockAgentCore.6] Los navegadores AgentCore personalizados de Bedrock deberían tener habilitada la grabación de sesiones
- [CloudFormation.2] las CloudFormation pilas deben estar etiquetadas

- [CloudFormation.3] las CloudFormation pilas deben tener habilitada la protección de terminación
- [CloudFormation.4] las CloudFormation pilas deben tener funciones de servicio asociadas
- [CloudFront.1] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado
- [CloudFront.3] CloudFront las distribuciones deben requerir el cifrado durante el tránsito
- [CloudFront.4] CloudFront las distribuciones deben tener configurada la conmutación por error de origen
- [CloudFront.5] CloudFront las distribuciones deben tener habilitado el registro
- [CloudFront.6] CloudFront las distribuciones deben tener WAF activado
- [CloudFront.7] CloudFront las distribuciones deben usar certificados personalizados SSL/TLS
- [CloudFront.8] CloudFront las distribuciones deben usar el SNI para atender las solicitudes HTTPS
- [CloudFront.9] CloudFront las distribuciones deben cifrar el tráfico para convertirlo en orígenes personalizados
- [CloudFront.10] CloudFront las distribuciones no deben usar protocolos SSL obsoletos entre ubicaciones de borde y orígenes personalizados
- [CloudFront.12] CloudFront las distribuciones no deben apuntar a orígenes de S3 inexistentes
- [CloudFront.13] CloudFront las distribuciones deben usar el control de acceso al origen
- [CloudFront.14] CloudFront las distribuciones deben estar etiquetadas
- [CloudFront.15] CloudFront las distribuciones deben usar la política de seguridad TLS recomendada
- [CloudFront.16] CloudFront las distribuciones deben usar el control de acceso de origen para los orígenes de las URL de las funciones de Lambda
- [CloudFront.17] CloudFront las distribuciones deben usar grupos de claves confiables para las URL y cookies firmadas
- [CloudTrail.6] Asegúrese de que el depósito de S3 que se utiliza para almacenar CloudTrail los registros no sea de acceso público
- [CloudTrail.7] Asegúrese de que el registro de acceso al bucket de S3 esté habilitado en el CloudTrail bucket de S3
- [CloudTrail.9] las CloudTrail rutas deben estar etiquetadas
- [CloudTrail.10] Los almacenes de datos de eventos de CloudTrail Lake deben estar cifrados y gestionados por el clienteAWS KMS keys

- [CloudWatch.17] las acciones CloudWatch de alarma deben estar activadas
- [CodeArtifact.1] CodeArtifact los repositorios deben estar etiquetados
- [CodeBuild.1] Las URL del repositorio fuente de CodeBuild Bitbucket no deben contener credenciales confidenciales
- [CodeBuild.2] las variables de entorno CodeBuild del proyecto no deben contener credenciales de texto claro
- [CodeBuild.3] Los registros de CodeBuild S3 deben estar cifrados
- [CodeBuild.4] los entornos de CodeBuild proyectos deben tener un registroAWS ConfigDuración
- [CodeBuild.7] las exportaciones de grupos de CodeBuild informes deben cifrarse en reposo
- [CodeGuruProfiler.1] Los grupos CodeGuru de creación de perfiles de Profiler deben estar etiquetados
- [CodeGuruReviewer.1] Las asociaciones de repositorios de CodeGuru Reviewer deben estar etiquetadas
- [Cognito.1] Los grupos de usuarios de Cognito deben tener activada la protección contra amenazas y el modo de aplicación con todas las funciones para la autenticación estándar
- [Cognito.2] Los grupos de identidades de Cognito no deben permitir identidades no autenticadas
- [Cognito.3] Las políticas de contraseñas para los grupos de usuarios de Cognito deben tener configuraciones sólidas
- [Cognito.4] Los grupos de usuarios de Cognito deben tener activada la protección contra amenazas y el modo de aplicación con todas las funciones para la autenticación personalizada
- [Cognito.5] La MFA debe estar habilitada para los grupos de usuarios de Cognito
- [Cognito.6] Los grupos de usuarios de Cognito deben tener habilitada la protección contra la eliminación
- [Connect.1] Los tipos de objetos de los perfiles de clientes de Amazon Connect deben estar etiquetados
- [Connect.2] Las instancias de Connect Customer deben tener el CloudWatch registro habilitado
- [DataFirehose.1] Los flujos de entrega de Firehose deben cifrarse en reposo
- [DataSync.1] DataSync las tareas deberían tener el registro activado
- [DataSync.2] DataSync las tareas deben estar etiquetadas
- [Detective.1] Los gráficos de comportamiento de los detectives deben estar etiquetados
- [DMS.1] Las instancias de replicación de Database Migration Service no deben ser públicas

- [DMS.2] Los certificados DMS deben estar etiquetados
- [DMS.3] Las suscripciones a eventos de DMS deben estar etiquetadas
- [DMS.4] Las instancias de replicación de DMS deben estar etiquetadas
- [DMS.5] Los grupos de subredes de replicación del DMS deben estar etiquetados
- [DMS.6] Las instancias de replicación de DMS deben tener habilitada la actualización automática de las versiones secundarias
- [DMS.7] Las tareas de replicación del DMS para la base de datos de destino deben tener el registro habilitado
- [DMS.8] Las tareas de replicación del DMS para la base de datos de origen deben tener el registro activado
- [DMS.9] Los puntos finales del DMS deben usar SSL
- [DMS.10] Los puntos finales de DMS para las bases de datos de Neptune deben tener habilitada la autorización de IAM
- [DMS.11] Los puntos finales de DMS para MongoDB deben tener un mecanismo de autenticación habilitado
- [DMS.12] Los puntos finales de DMS para Redis OSS deben tener el TLS habilitado
- [DMS.13] Las instancias de replicación de DMS deben configurarse para usar varias zonas de disponibilidad
- [DocumentDB.1] Los clústeres de Amazon DocumentDB deben cifrarse en reposo
- [DocumentDB.2] Los clústeres de Amazon DocumentDB deben tener un período de retención de copias de seguridad adecuado
- [DocumentDB.3] Las instantáneas de clústeres manuales de Amazon DocumentDB no deben ser públicas
- [DocumentDB.4] Los clústeres de Amazon DocumentDB deben publicar los registros de auditoría en Logs CloudWatch
- [DocumentDB.5] Los clústeres de Amazon DocumentDB deben tener habilitada la protección contra eliminaciones
- [DocumentDB.6] Los clústeres de Amazon DocumentDB deben cifrarse en tránsito
- [DynamoDB.3] Los clústeres de DynamoDB Accelerator (DAX) deben cifrarse en reposo
- [DynamoDB.4] Las tablas de DynamoDB deben estar presentes en un plan de respaldo
- [DynamoDB.5] Las tablas de DynamoDB deben estar etiquetadas

- [DynamoDB.6] Las tablas de DynamoDB deben tener habilitada la protección de eliminación
- [DynamoDB.7] Los clústeres de DynamoDB Accelerator deben cifrarse en tránsito
- [EC2.4] Las instancias EC2 detenidas deben eliminarse después de un período de tiempo específico
- [EC2.10] Amazon EC2 debe configurarse para utilizar los puntos de enlace de VPC que se crean para el servicio Amazon EC2
- [EC2.19] Los grupos de seguridad no deben permitir el acceso irrestricto a los puertos de alto riesgo
- [EC2.21] Las ACL de red no deberían permitir la entrada desde la versión 0.0.0. 0/0 al puerto 22 o al puerto 3389
- [EC2.22] Deben eliminarse los grupos de seguridad de Amazon EC2 no utilizados
- [EC2.23] Amazon EC2 Transit Gateways no debe aceptar automáticamente las solicitudes de adjuntos de VPC
- [EC2.24] No se deben utilizar los tipos de instancias paravirtuales de Amazon EC2
- [EC2.25] Las plantillas de lanzamiento de Amazon EC2 no deben asignar direcciones IP públicas a las interfaces de red
- [EC2.28] Los volúmenes de EBS deben estar cubiertos por un plan de respaldo
- [EC2.33] Los archivos adjuntos de la pasarela de tránsito EC2 deben estar etiquetados
- [EC2.34] Las tablas de rutas de la pasarela de tránsito EC2 deben estar etiquetadas
- [EC2.35] Las interfaces de red EC2 deben estar etiquetadas
- [EC2.36] Las pasarelas de clientes de EC2 deben estar etiquetadas
- [EC2.37] Las direcciones IP elásticas de EC2 deben estar etiquetadas
- [EC2.38] Las instancias EC2 deben estar etiquetadas
- [EC2.39] Las pasarelas de Internet EC2 deben estar etiquetadas
- [EC2.40] Las pasarelas NAT EC2 deben estar etiquetadas
- [EC2.41] Las ACL de la red EC2 deben estar etiquetadas
- [EC2.42] Las tablas de rutas de EC2 deben estar etiquetadas
- [EC2.43] Los grupos de seguridad de EC2 deben estar etiquetados
- [EC2.44] Las subredes EC2 deben estar etiquetadas
- [EC2.45] Los volúmenes EC2 deben estar etiquetados

- [EC2.46] Las Amazon VPC deben estar etiquetadas
- [EC2.47] Los servicios de punto final de Amazon VPC deben estar etiquetados
- [EC2.48] Los registros de flujo de Amazon VPC deben estar etiquetados
- [EC2.49] Las conexiones de emparejamiento de Amazon VPC deben estar etiquetadas
- [EC2.50] Las pasarelas VPN de EC2 deben estar etiquetadas
- [EC2.51] Los puntos finales EC2 Client VPN deben tener habilitado el registro de conexiones de clientes
- [EC2.52] Las pasarelas de tránsito EC2 deben estar etiquetadas
- [EC2.53] Los grupos de seguridad de EC2 no deberían permitir la entrada desde la versión 0.0.0.0/0 a los puertos de administración remota del servidor
- [EC2.54] Los grupos de seguridad de EC2 no deberían permitir la entrada desde: :/0 a los puertos de administración remota del servidor
- [EC2.55] Las VPC deben configurarse con un punto final de interfaz para la API de ECR
- [EC2.56] Las VPC deben configurarse con un punto final de interfaz para Docker Registry
- [EC2.57] Las VPC deben configurarse con un punto final de interfaz para Systems Manager
- [EC2.58] Las VPC deben configurarse con un punto final de interfaz para los contactos de Systems Manager Incident Manager
- [EC2.60] Las VPC deben configurarse con un punto final de interfaz para Systems Manager Incident Manager
- [EC2.170] Las plantillas de lanzamiento de EC2 deben utilizar la versión 2 del servicio de metadatos de instancias (IMDSv2)
- [EC2.171] Las conexiones VPN de EC2 deberían tener el registro habilitado
- [EC2.172] La configuración de acceso público del bloque de VPC de EC2 debería bloquear el tráfico de la puerta de enlace de Internet
- [EC2.173] Las solicitudes de EC2 Spot Fleet con parámetros de lanzamiento deberían permitir el cifrado de los volúmenes de EBS adjuntos
- [EC2.174] Los conjuntos de opciones DHCP de EC2 deben estar etiquetados
- [EC2.175] Las plantillas de lanzamiento de EC2 deben estar etiquetadas
- [EC2.176] Las listas de prefijos de EC2 deben estar etiquetadas
- [EC2.177] Las sesiones de réplica de tráfico de EC2 deben etiquetarse
- [EC2.178] Los filtros espejo de tráfico EC2 deben estar etiquetados

- [EC2.179] Los objetivos del espejo de tráfico de EC2 deben estar etiquetados
- [EC2.180] Las interfaces de red EC2 deberían tener habilitada source/destination la verificación
- [EC2.181] Las plantillas de lanzamiento de EC2 deberían permitir el cifrado de los volúmenes de EBS adjuntos
- [EC2.182] La configuración de bloqueo de acceso público debe estar habilitada para las instantáneas de Amazon EBS
- [EC2.183] Las conexiones VPN de EC2 deben utilizar el protocolo IKEv2
- [ECR.1] Los repositorios privados de ECR deben tener configurado el escaneo de imágenes
- [ECR.2] Los repositorios privados de ECR deben tener configurada la inmutabilidad de etiquetas
- [ECR.3] Los repositorios de ECR deben tener configurada al menos una política de ciclo de vida
- [ECR.4] Los repositorios públicos de ECR deben etiquetarse
- [ECR.5] Los repositorios de ECR deben estar cifrados y ser gestionados por el cliente AWS KMS keys
- [ECS.2] Los servicios de ECS no deberían tener direcciones IP públicas asignadas automáticamente
- [ECS.3] Las definiciones de tareas de ECS no deben compartir el espacio de nombres del proceso del host
- [ECS.4] Los contenedores ECS deben ejecutarse sin privilegios
- [ECS.5] Las definiciones de tareas de ECS deben configurar los contenedores para que se limiten al acceso de solo lectura a los sistemas de archivos raíz
- [ECS.8] Los secretos no deben transmitirse como variables de entorno de contenedores
- [ECS.9] Las definiciones de tareas de ECS deben tener una configuración de registro
- [ECS.10] Los servicios Fargate de ECS deberían ejecutarse en la última versión de la plataforma Fargate
- [ECS.12] Los clústeres de ECS deben usar Container Insights
- [ECS.13] Los servicios de ECS deben estar etiquetados
- [ECS.14] Los clústeres de ECS deben etiquetarse
- [ECS.15] Las definiciones de las tareas de ECS deben estar etiquetadas
- [ECS.16] Los conjuntos de tareas de ECS no deben asignar automáticamente direcciones IP públicas
- [ECS.17] Las definiciones de tareas de ECS no deben usar el modo de red host

- [ECS.18] Las definiciones de tareas de ECS deben utilizar el cifrado en tránsito para los volúmenes de EFS
- [ECS.19] Los proveedores de capacidad de ECS deberían tener habilitada la protección de terminación gestionada
- [ECS.20] Las definiciones de tareas de ECS deben configurar a los usuarios no root en las definiciones de contenedores de Linux
- [ECS.21] Las definiciones de tareas de ECS deberían configurar a los usuarios no administradores en las definiciones de contenedores de Windows
- [EFS.1] Elastic File System debe configurarse para cifrar los datos de los archivos en reposo mediante AWS KMS
- [EFS.2] Los volúmenes de Amazon EFS deben figurar en los planes de copia de seguridad
- [EFS.3] Los puntos de acceso EFS deben exigir un directorio raíz
- [EFS.4] Los puntos de acceso EFS deben exigir la identidad del usuario
- [EFS.5] Los puntos de acceso EFS deben estar etiquetados
- [EFS.6] Los destinos de montaje de EFS no deben asociarse a subredes que asignan direcciones IP públicas en el momento del lanzamiento
- [] Los sistemas de archivos EFS deben tener habilitadas las copias de seguridad automáticas EFS.7
- [EFS.8] Los sistemas de archivos EFS deben cifrarse en reposo
- [EKS.1] Los puntos finales del clúster EKS no deben ser de acceso público
- [EKS.2] Los clústeres de EKS deben ejecutarse en una versión de Kubernetes compatible
- [EKS.3] Los clústeres de EKS deben usar secretos de Kubernetes cifrados
- [] Los clústeres de EKS deben etiquetarse EKS.6
- [EKS.7] Las configuraciones del proveedor de identidad de EKS deben etiquetarse
- [EKS.8] Los clústeres de EKS deben tener habilitado el registro de auditoría
- [EKS.9] Los grupos de nodos de EKS deben ejecutarse en una versión de Kubernetes compatible
- [ELB.2] Los balanceadores de carga clásicos con SSL/HTTPS oyentes deben usar un certificado proporcionado por AWS Gestor de certificados
- [ELB.3] Los oyentes de Classic Load Balancer deben configurarse con terminación HTTPS o TLS
- [ELB.7] Los balanceadores de carga clásicos deben tener activado el drenaje de conexiones
- [ELB.8] Los balanceadores de carga clásicos con receptores SSL deben usar una política de seguridad predefinida que sea sólida AWS Config Duración

- [ELB.10] El balanceador de carga clásico debe abarcar varias zonas de disponibilidad
- [ELB.12] El balanceador de carga de aplicaciones debe configurarse con el modo defensivo o de mitigación de desincronización más estricto
- [ELB.13] Los balanceadores de carga de aplicaciones, redes y puertas de enlace deben abarcar varias zonas de disponibilidad
- [ELB.14] El balanceador de carga clásico debe configurarse con el modo defensivo o de mitigación de desincronización más estricto
- [ELB.16] Los balanceadores de carga de aplicaciones deben estar asociados a un AWS WAF ACL web
- [ELB.17] Los balanceadores de cargas de aplicaciones y redes con oyentes deben usar las políticas de seguridad recomendadas
- [ELB.18] Los oyentes del balanceador de cargas de red y aplicaciones deben usar protocolos seguros para cifrar los datos en tránsito
- [ELB.21] Los grupos destinatarios de Application and Network Load Balancer deben utilizar protocolos de control de estado cifrados
- [ELB.22] Los grupos objetivo del ELB deben usar protocolos de transporte cifrados
- [ElastiCache.1] ElastiCache (Redis OSS) los clústeres deben tener habilitadas las copias de seguridad automáticas
- [ElastiCache.2] ElastiCache los clústeres deberían tener habilitadas las actualizaciones automáticas de las versiones secundarias
- [ElastiCache.3] los grupos de ElastiCache replicación deberían tener habilitada la conmutación por error automática
- [ElastiCache.4] los grupos de ElastiCache replicación deben cifrarse en reposo
- [ElastiCache.5] los grupos de ElastiCache replicación deben cifrarse en tránsito
- [ElastiCache.6] ElastiCache (Redis OSS) Los grupos de replicación de versiones anteriores deberían tener habilitada la autenticación de Redis OSS
- [ElastiCache.7] los ElastiCache clústeres no deben usar el grupo de subredes predeterminado
- [ElasticBeanstalk.1] Los entornos de Elastic Beanstalk deberían tener habilitados los informes de estado mejorados
- [ElasticBeanstalk.2] Las actualizaciones de la plataforma gestionada de Elastic Beanstalk deben estar habilitadas
- [ElasticBeanstalk.3] Elastic Beanstalk debería transmitir los registros a CloudWatch

- [EMR.1] Los nodos principales del clúster de Amazon EMR no deben tener direcciones IP públicas
- [EMR.2] La configuración de acceso público del bloque Amazon EMR debe estar habilitada
- [EMR.3] Las configuraciones de seguridad de Amazon EMR deben cifrarse en reposo
- [EMR.4] Las configuraciones de seguridad de Amazon EMR deben cifrarse en tránsito
- [ES.1] Los dominios de Elasticsearch deben tener habilitado el cifrado en reposo
- [ES.2] Los dominios de Elasticsearch no deben ser de acceso público
- [ES.3] Los dominios de Elasticsearch deben cifrar los datos enviados entre nodos
- [ES.4] Debería estar habilitado el registro de errores de dominio de Elasticsearch en Logs CloudWatch
- [ES.5] Los dominios de Elasticsearch deben tener habilitado el registro de auditoría
- [ES.6] Los dominios de Elasticsearch deben tener al menos tres nodos de datos
- [ES.7] Los dominios de Elasticsearch deben configurarse con al menos tres nodos maestros dedicados
- [ES.8] Las conexiones a los dominios de Elasticsearch deben cifrarse con la política de seguridad TLS más reciente
- [ES.9] Los dominios de Elasticsearch deben etiquetarse
- [EventBridge.2] los autobuses de EventBridge eventos deben estar etiquetados
- [EventBridge.3] los autobuses de eventos EventBridge personalizados deben tener adjunta una política basada en los recursos
- [EventBridge.4] los puntos finales EventBridge globales deberían tener habilitada la replicación de eventos
- [FraudDetector.1] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.2] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas
- [FraudDetector.3] Los resultados de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.4] Las variables de Amazon Fraud Detector deben estar etiquetadas
- [FSx.1] FSx para sistemas de archivos OpenZFS debe configurarse para copiar etiquetas en copias de seguridad y volúmenes
- [FSx.2] Los sistemas de archivos FSx for Lustre deben configurarse para copiar etiquetas a las copias de seguridad
- [FSx.3] FSx para sistemas de archivos OpenZFS debe configurarse para su implementación Multi-AZ

- [FSx.4] FSx para sistemas de archivos NetApp ONTAP debe configurarse para su implementación Multi-AZ
- [FSx.5] Los sistemas de archivos FSx for Windows File Server deben configurarse para Multi-AZ su implementación
- [GlobalAccelerator.1] Los aceleradores de Global Accelerator deben estar etiquetados
- [Glue.1]AWS Gluelos trabajos deben estar etiquetados
- [Glue.3]AWS GlueLas transformaciones de aprendizaje automático deben cifrarse en reposo
- [Glue.4]AWS GlueLos trabajos de Spark deberían ejecutarse en versiones compatibles deAWS Glue
- [GuardDuty.1] GuardDuty debería estar activado
- GuardDuty Los filtros [GuardDuty.2] deben estar etiquetados
- [GuardDuty.3] Los GuardDuty IPSets deben estar etiquetados
- [GuardDuty.4] GuardDuty los detectores deben estar etiquetados
- [GuardDuty.5] La monitorización del registro de auditoría de GuardDuty EKS debe estar habilitada
- [GuardDuty.6] GuardDuty La protección Lambda debe estar habilitada
- [GuardDuty.7] La monitorización del tiempo de ejecución de GuardDuty EKS debe estar habilitada
- [GuardDuty.8] La protección contra GuardDuty malware para EC2 debe estar habilitada
- [GuardDuty.9] La protección GuardDuty RDS debe estar habilitada
- [GuardDuty.10] La protección GuardDuty S3 debe estar habilitada
- [GuardDuty.11] La monitorización del GuardDuty tiempo de ejecución debe estar habilitada
- [GuardDuty.12] La monitorización del tiempo de ejecución de GuardDuty ECS debe estar habilitada
- [GuardDuty.13] La monitorización del tiempo de ejecución de GuardDuty EC2 debe estar habilitada
- [IAM.1] Las políticas de IAM no deberían permitir todos los privilegios administrativos «*»
- [IAM.2] Los usuarios de IAM no deberían tener políticas de IAM adjuntas
- [IAM.3] Las claves de acceso de los usuarios de IAM deben rotarse cada 90 días o menos
- [IAM.4] La clave de acceso del usuario raíz de IAM no debería existir
- [IAM.5] La MFA debe estar habilitada para todos los usuarios de IAM que tengan una contraseña de consola
- [IAM.6] La MFA de hardware debe estar habilitada para el usuario root

- [IAM.7] Las políticas de contraseñas para los usuarios de IAM deben tener configuraciones sólidas
- [IAM.8] Se deben eliminar las credenciales de usuario de IAM no utilizadas
- [IAM.9] La MFA debe estar habilitada para el usuario root
- [IAM.10] Las políticas de contraseñas para los usuarios de IAM deben tener configuraciones sólidas
- [IAM.11] Asegúrese de que la política de contraseñas de IAM requiera al menos una letra mayúscula
- [IAM.12] Asegúrese de que la política de contraseñas de IAM requiera al menos una letra minúscula
- [IAM.13] Asegúrese de que la política de contraseñas de IAM requiera al menos un símbolo
- [IAM.14] Asegúrese de que la política de contraseñas de IAM requiera al menos un número
- [IAM.15] Asegúrese de que la política de contraseñas de IAM exija una longitud de contraseña mínima de 14 o más
- [IAM.16] Asegúrese de que la política de contraseñas de IAM impida la reutilización de contraseñas
- [IAM.17] Asegúrese de que la política de contraseñas de IAM haga caducar las contraseñas en un plazo de 90 días o menos
- [IAM.18] Asegúrese de que se haya creado una función de soporte para gestionar los incidentes conAWS Support
- [IAM.19] La MFA debe estar habilitada para todos los usuarios de IAM
- [IAM.21] Las políticas de IAM gestionadas por el cliente que cree no deberían permitir acciones comodín en los servicios
- [IAM.22] Se deben eliminar las credenciales de usuario de IAM que no se hayan utilizado durante 45 días
- [IAM.23] Los analizadores de IAM Access Analyzer deben estar etiquetados
- [IAM.24] Las funciones de IAM deben estar etiquetadas
- [IAM.25] Los usuarios de IAM deben estar etiquetados
- [IAM.26] SSL/TLS Los certificados caducados gestionados en IAM deben eliminarse
- [IAM.27] Las identidades de IAM no deberían tener la AWSCloudShellFullAccess política adjunta
- [IAM.28] El analizador de acceso externo de IAM Access Analyzer debe estar habilitado
- [Inspector.1] El escaneo EC2 de Amazon Inspector debe estar activado

- [Inspector.2] El escaneo ECR de Amazon Inspector debe estar activado
- [Inspector.3] El escaneo de código Lambda de Amazon Inspector Lambda debe estar activado
- [Inspector.4] El escaneo estándar de Amazon Inspector Lambda debe estar activado
- [IoT.1]AWS IoT Device Defenderlos perfiles de seguridad deben estar etiquetados
- [IoT.2]AWS IoT Corelas acciones de mitigación deben estar etiquetadas
- [IoT.3]AWS IoT Corelas dimensiones deben estar etiquetadas
- [IoT.4]AWS IoT Corelos autorizadores deben estar etiquetados
- [IoT.5]AWS IoT CoreLos alias de los roles deben estar etiquetados
- [IoT.6]AWS IoT Corelas políticas deben estar etiquetadas
- [IoTSiteWise.1]AWSLos modelos SiteWise de activos de IoT deben estar etiquetados
- [IoTSiteWise.2]AWS SiteWise Los paneles de IoT deben estar etiquetados
- [IoTSiteWise.3]AWS SiteWise Las pasarelas de IoT deben estar etiquetadas
- [IoTSiteWise.4]AWS SiteWise Los portales de IoT deben estar etiquetados
- [IoTSiteWise.5]AWS SiteWise Los proyectos de IoT deben estar etiquetados
- [IoTTwinMaker.1]AWSLos trabajos de TwinMaker sincronización de IoT deben estar etiquetados
- [IoTTwinMaker.2]AWS TwinMaker Los espacios de trabajo de IoT deben estar etiquetados
- [IoTTwinMaker.3]AWS TwinMaker Las escenas de IoT deben estar etiquetadas
- [IoTTwinMaker.4]AWS TwinMaker Las entidades de IoT deben estar etiquetadas
- [IoTWireless.1]AWSLos grupos de multidifusión de IoT Wireless deben estar etiquetados
- [IoTWireless.2]AWSLos perfiles de servicio de IoT Wireless deben estar etiquetados
- [IoTWireless.3]AWSLas tareas de IoT FUOTA deben estar etiquetadas
- [IVS.1] Los pares de teclas de reproducción IVS deben estar etiquetados
- [IVS.2] Las configuraciones de grabación de IVS deben estar etiquetadas
- [IVS.3] Los canales IVS deben estar etiquetados
- [Keyspaces.1] Los espacios clave de Amazon Keyspaces deben estar etiquetados
- [Kinesis.1] Las transmisiones de Kinesis deben cifrarse en reposo
- [Kinesis.2] Las transmisiones de Kinesis deben estar etiquetadas
- [Kinesis.3] Las transmisiones de Kinesis deben tener un período de retención de datos adecuado

- [KMS.1] Las políticas gestionadas por los clientes de IAM no deberían permitir acciones de descifrado en todas las claves de KMS
- [KMS.2] Los directores de IAM no deberían tener políticas integradas de IAM que permitan realizar acciones de descifrado en todas las claves de KMS
- [KMS.3]AWS KMS keysno se debe eliminar involuntariamente
- [KMS.5] Las claves KMS no deben ser de acceso público
- [Lambda.5] Las funciones de VPC Lambda deben funcionar en varias zonas de disponibilidad
- [Lambda.6] Las funciones de Lambda deben estar etiquetadas
- [Lambda.7] Las funciones de Lambda deberían tener AWS X-Ray el rastreo activo está habilitado
- [Macie.1] Amazon Macie debería estar activado
- [Macie.2] La detección automática de datos confidenciales por parte de Macie debería estar habilitada
- [MQ.2] Los corredores de ActiveMQ deben transmitir los registros de auditoría a CloudWatch
- [MQ.4] Los corredores de Amazon MQ deben estar etiquetados
- [MQ.5] Los corredores de ActiveMQ deberían usar el modo de implementación active/standby
- [MQ.6] Los corredores de RabbitMQ deberían usar el modo de despliegue de clústeres
- [MSK.1] Los clústeres de MSK deben cifrarse en tránsito entre los nodos de intermediación
- [MSK.2] Los clústeres de MSK deberían tener configurada una supervisión mejorada
- [MSK.3] Los conectores MSK Connect deben estar cifrados en tránsito
- [MSK.4] Los clústeres de MSK deben tener el acceso público deshabilitado
- [MSK.5] Los conectores MSK deben tener el registro activado
- [MSK.6] Los clústeres de MSK deberían deshabilitar el acceso no autenticado
- [Neptune.1] Los clústeres de bases de datos de Neptune deben cifrarse en reposo
- [Neptune.2] Los clústeres de bases de datos de Neptune deberían publicar registros de auditoría en Logs CloudWatch
- [Neptune.3] Las instantáneas del clúster de base de datos de Neptune no deben ser públicas
- [Neptune.4] Los clústeres de base de datos de Neptune deben tener habilitada la protección contra eliminación
- [Neptune.5] Los clústeres de Neptune DB deberían tener habilitadas las copias de seguridad automatizadas

- [Neptune.6] Las instantáneas del clúster de base de datos de Neptune deben cifrarse en reposo
- [Neptune.7] Los clústeres de base de datos de Neptune deben tener habilitada la autenticación de bases de datos de IAM
- [Neptune.8] Los clústeres de bases de datos de Neptune deben configurarse para copiar etiquetas a las instantáneas
- [Neptune.9] Los clústeres de base de datos Neptune deben implementarse en varias zonas de disponibilidad
- [NetworkFirewall.1] Los firewalls de Network Firewall deben implementarse en varias zonas de disponibilidad
- [NetworkFirewall.2] El registro de Network Firewall debe estar habilitado
- [NetworkFirewall.3] Las políticas de Network Firewall deben tener asociado al menos un grupo de reglas
- [NetworkFirewall.4] La acción sin estado predeterminada para las políticas de Network Firewall debe ser eliminar o reenviar paquetes completos
- [NetworkFirewall.5] La acción sin estado predeterminada para las políticas de Network Firewall debe ser eliminar o reenviar paquetes fragmentados
- [NetworkFirewall.6] El grupo de reglas de Stateless Network Firewall no debe estar vacío
- [NetworkFirewall.7] Los firewalls de Network Firewall deben estar etiquetados
- [NetworkFirewall.8] Las políticas de firewall de Network Firewall deben estar etiquetadas
- [NetworkFirewall.9] Los firewalls de Network Firewall deben tener habilitada la protección de eliminación
- [NetworkFirewall.10] Los firewalls de Network Firewall deben tener habilitada la protección contra cambios de subred
- [Opensearch.1] OpenSearch los dominios deben tener activado el cifrado en reposo
- [Opensearch.2] OpenSearch los dominios no deben ser de acceso público
- [Opensearch.3] OpenSearch los dominios deben cifrar los datos enviados entre nodos
- [Opensearch.4] El registro de errores de OpenSearch dominio en Logs debe estar habilitado CloudWatch
- [Opensearch.5] OpenSearch los dominios deben tener activado el registro de auditoría
- [Opensearch.6] OpenSearch los dominios deben tener al menos tres nodos de datos
- [Opensearch.7] OpenSearch los dominios deben tener habilitado un control de acceso detallado

- [Opensearch.8] Las conexiones a los OpenSearch dominios deben cifrarse con la última política de seguridad de TLS
- [Opensearch.9] OpenSearch los dominios deben estar etiquetados
- [Opensearch.10] OpenSearch los dominios deben tener instalada la última actualización de software
- [Opensearch.11] OpenSearch los dominios deben tener al menos tres nodos principales dedicados
- [PCA.1]AWS Privada CALa autoridad emisora de certificados raíz debe estar deshabilitada
- [PCA.2]AWSLas autoridades de certificación de CA privadas deben estar etiquetadas
- [RDS.14] Los clústeres de Amazon Aurora deben tener habilitado el retroceso
- [RDS.16] Los clústeres de bases de datos de Aurora deben configurarse para copiar las etiquetas a las instantáneas de bases de datos
- [RDS.17] Las instancias de base de datos de RDS deben configurarse para copiar las etiquetas de las instantáneas
- [RDS.19] Las suscripciones de notificación de eventos de RDS existentes deben configurarse para los eventos críticos del clúster
- [RDS.20] Las suscripciones de notificación de eventos de RDS existentes deben configurarse para los eventos críticos de las instancias de bases de datos
- [RDS.21] Se debe configurar una suscripción a las notificaciones de eventos de RDS para los eventos de grupos de parámetros de base de datos críticos
- [RDS.22] Se debe configurar una suscripción a las notificaciones de eventos de RDS para los eventos críticos de grupos de seguridad de bases de datos
- [RDS.23] Las instancias de RDS no deben usar el puerto predeterminado de un motor de base de datos
- [RDS.24] Los clústeres de bases de datos de RDS deben usar un nombre de usuario de administrador personalizado
- [RDS.25] Las instancias de bases de datos de RDS deben usar un nombre de usuario de administrador personalizado
- [RDS.26] Las instancias de base de datos de RDS deben protegerse mediante un plan de respaldo
- [RDS.27] Los clústeres de bases de datos de RDS deben cifrarse en reposo
- [RDS.28] Los clústeres de bases de datos de RDS deben etiquetarse
- [RDS.29] Las instantáneas del clúster de bases de datos de RDS deben etiquetarse

- [RDS.30] Las instancias de base de datos de RDS deben etiquetarse
- [RDS.31] Los grupos de seguridad de la base de datos de RDS deben etiquetarse
- [RDS.32] Las instantáneas de la base de datos de RDS deben etiquetarse
- [RDS.33] Los grupos de subredes de bases de datos de RDS deben etiquetarse
- [RDS.34] Los clústeres de bases de datos Aurora MySQL deben publicar los registros de auditoría en Logs CloudWatch
- [RDS.35] Los clústeres de bases de datos de RDS deben tener habilitada la actualización automática de versiones secundarias
- [RDS.36] Las instancias de base de datos de RDS para PostgreSQL deben publicar los registros en Logs CloudWatch
- [RDS.37] Los clústeres de bases de datos de Aurora PostgreSQL deben publicar los registros en Logs CloudWatch
- [RDS.38] Las instancias de base de datos de RDS para PostgreSQL deben cifrarse en tránsito
- [RDS.39] Las instancias de base de datos de RDS para MySQL deben cifrarse en tránsito
- [RDS.40] Las instancias de base de datos de RDS para SQL Server deben publicar los registros en Logs CloudWatch
- [RDS.41] Las instancias de base de datos de RDS para SQL Server deben cifrarse en tránsito
- [RDS.42] Las instancias de base de datos de RDS para MariaDB deben publicar los registros en Logs CloudWatch
- [RDS.43] Los proxies de bases de datos de RDS deben requerir el cifrado TLS para las conexiones
- [RDS.44] Las instancias de base de datos de RDS para MariaDB deben cifrarse durante el tránsito
- [RDS.45] Los clústeres de bases de datos Aurora MySQL deben tener habilitado el registro de auditoría
- [RDS.46] Las instancias de base de datos de RDS no deben implementarse en subredes públicas con rutas a pasarelas de Internet
- [RDS.47] Los clústeres de bases de datos de RDS para PostgreSQL deben configurarse para copiar las etiquetas a las instantáneas de bases de datos
- [RDS.48] Los clústeres de bases de datos de RDS para MySQL deben configurarse para copiar etiquetas a las instantáneas de bases de datos
- [RDS.50] Los clústeres de bases de datos de RDS deben tener un período de retención de copias de seguridad suficiente

- [RDS.51] Los clústeres globales de RDS deben ejecutarse en una versión compatible de Aurora MySQL
- [Redshift.1] Los clústeres de Amazon Redshift deberían prohibir el acceso público
- [Redshift.2] Las conexiones a los clústeres de Amazon Redshift deben cifrarse en tránsito
- [Redshift.3] Los clústeres de Amazon Redshift deben tener habilitadas las instantáneas automáticas
- [Redshift.4] Los clústeres de Amazon Redshift deben tener habilitado el registro de auditoría
- [Redshift.6] Amazon Redshift debería tener habilitadas las actualizaciones automáticas a las versiones principales
- [Redshift.7] Los clústeres de Redshift deberían utilizar un enrutamiento de VPC mejorado
- [Redshift.8] Los clústeres de Amazon Redshift no deben usar el nombre de usuario de administrador predeterminado
- [Redshift.10] Los clústeres de Redshift deben cifrarse en reposo
- [Redshift.11] Los clústeres de Redshift deben estar etiquetados
- [Redshift.12] Las suscripciones a notificaciones de eventos de Redshift deben estar etiquetadas
- [Redshift.13] Las instantáneas del clúster de Redshift deben estar etiquetadas
- [Redshift.14] Los grupos de subredes del clúster de Redshift deben estar etiquetados
- [Redshift.15] Los grupos de seguridad de Redshift deberían permitir la entrada en el puerto del clúster solo desde orígenes restringidos
- [Redshift.16] Los grupos de subredes de clústeres de Redshift deben tener subredes de varias zonas de disponibilidad
- [Redshift.17] Los grupos de parámetros del clúster de Redshift deben estar etiquetados
- [Redshift.18] Los clústeres de Redshift deberían tener Multi-AZ las implementaciones habilitadas
- [RedshiftServerless.1] Los grupos de trabajo sin servidor de Amazon Redshift deberían utilizar un enrutamiento de VPC mejorado
- [RedshiftServerless.2] Las conexiones a los grupos de trabajo sin servidor de Redshift deberían ser obligatorias para usar SSL
- [RedshiftServerless.3] Los grupos de trabajo sin servidor de Redshift deberían prohibir el acceso público
- [RedshiftServerless.4] Los espacios de nombres de Redshift Serverless deben cifrarse y administrarse por el clienteAWS KMS keys

- [RedshiftServerless.5] Los espacios de nombres Redshift Serverless no deben usar el nombre de usuario de administrador predeterminado
- [RedshiftServerless.6] Los espacios de nombres Redshift Serverless deberían exportar los registros a los registros CloudWatch
- [Route53.1] Los controles de salud de Route 53 deben estar etiquetados
- [Route53.2] Las zonas alojadas públicas de Route 53 deberían registrar las consultas de DNS
- [S3.7] Los cubos de uso general de S3 deben utilizar la replicación entre regiones
- [S3.10] Los cubos de uso general de S3 con el control de versiones habilitado deben tener configuraciones de ciclo de vida
- [S3.11] Los cubos de uso general de S3 deben tener habilitadas las notificaciones de eventos
- [S3.12] Las ACL no deben usarse para administrar el acceso de los usuarios a los cubos de uso general de S3
- [S3.13] Los cubos de uso general de S3 deben tener configuraciones de ciclo de vida
- [S3.17] Los cubos de uso general de S3 deben cifrarse en reposo con AWS KMS keys
- [S3.19] Los puntos de acceso S3 deben tener habilitada la configuración de bloqueo de acceso público
- [S3.20] Los cubos de uso general de S3 deben tener habilitada la eliminación de MFA
- [S3.22] Los cubos de uso general de S3 deben registrar los eventos de escritura a nivel de objeto
- [S3.23] Los cubos de uso general de S3 deben registrar los eventos de lectura a nivel de objeto
- [S3.24] Los puntos de Multi-Region acceso S3 deben tener habilitada la configuración de bloqueo del acceso público
- [S3.25] Los buckets de directorio de S3 deben tener configuraciones de ciclo de vida
- [SageMaker.1] Las instancias de Amazon SageMaker Notebook no deberían tener acceso directo a Internet
- [SageMaker.2] las instancias de SageMaker cuadernos deben lanzarse en una VPC personalizada
- [SageMaker.3] Los usuarios no deben tener acceso root a las instancias de los SageMaker cuadernos
- [SageMaker.4] Las variantes de producción de SageMaker terminales deben tener un recuento inicial de instancias superior a 1
- SageMaker Los modelos [SageMaker.5] deben tener habilitado el aislamiento de red
- [SageMaker.6] las configuraciones de imagen de la SageMaker aplicación deben estar etiquetadas

- [SageMaker.7] SageMaker las imágenes deben estar etiquetadas
- [SageMaker.8] las instancias de SageMaker notebooks deben ejecutarse en plataformas compatibles
- [SageMaker.9] las definiciones de trabajos de calidad de los SageMaker datos deben tener habilitado el cifrado del tráfico entre contenedores
- [SageMaker.10] Las definiciones de trabajos de explicabilidad del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores
- [SageMaker.11] las definiciones de trabajos SageMaker de calidad de los datos deben tener habilitado el aislamiento de red
- [SageMaker.12] las definiciones de trabajo basadas en el sesgo del SageMaker modelo deben tener habilitado el aislamiento de red
- [SageMaker.13] las definiciones de trabajos de calidad del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores
- [SageMaker.14] los programas SageMaker de monitoreo deben tener habilitado el aislamiento de la red
- [SageMaker.15] Las definiciones de trabajo basadas en el sesgo del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores
- SageMaker Los modelos [SageMaker.16] deben usar un registro privado en la VPC para los contenedores principales
- [SageMaker.17] SageMaker Las tiendas offline de los grupos de funciones deben cifrarse con AWS KMS claves
- [SageMaker.18] las tiendas en línea de grupos de SageMaker funciones con almacenamiento estándar deben cifrarse con AWS KMS claves
- [SageMaker.19] SageMaker los modelos deben usar un registro privado en la VPC para las canalizaciones de inferencia de varios contenedores
- [SES.1] Las listas de contactos de SES deben estar etiquetadas
- [SES.2] Los conjuntos de configuración de SES deben estar etiquetados
- [SES.3] Los conjuntos de configuración de SES deben tener el TLS habilitado para enviar correos electrónicos
- [SecretsManager.1] Los secretos de Secrets Manager deberían tener habilitada la rotación automática
- [SecretsManager.2] Los secretos de Secrets Manager configurados con rotación automática deberían girar correctamente

- [SecretsManager.3] Eliminar los secretos de Secrets Manager no utilizados
- [SecretsManager.4] Los secretos de Secrets Manager deben rotarse en un número específico de días
- [SecretsManager.5] Los secretos de Secrets Manager deben estar etiquetados
- [ServiceCatalog.1] Las carteras de Service Catalog deben compartirse dentro de unAWSsolo una organización
- [SNS.3] Los temas de SNS deben estar etiquetados
- [SNS.4] Las políticas de acceso a los temas de SNS no deberían permitir el acceso público
- [SQS.1] Las colas de Amazon SQS deben cifrarse en reposo
- [SQS.2] Las colas de SQS deben estar etiquetadas
- [SQS.3] Las políticas de acceso a las colas de SQS no deberían permitir el acceso público
- [SSM.1] Las instancias de Amazon EC2 deben administrarse medianteAWS Systems Manager
- [SSM.2] Las instancias de Amazon EC2 administradas por Systems Manager deben tener el estado de conformidad con los parches de CONFORMIDAD CON LOS PARCHES tras la instalación de un parche
- [SSM.3] Las instancias de Amazon EC2 administradas por Systems Manager deben tener el estado de conformidad de la asociación de COMPLIANT
- [SSM.4] Los documentos SSM no deben ser públicos
- [SSM.5] Los documentos SSM deben estar etiquetados
- [SSM.6] SSM Automation debería tener el registro habilitado CloudWatch
- [SSM.7] Los documentos SSM deben tener habilitada la configuración de bloqueo para compartir en público
- [StepFunctions.1] Step Functions indica que las máquinas deben tener el registro activado
- [StepFunctions.2] Las actividades de Step Functions deben estar etiquetadas
- [Transfer.1]AWS Transfer Familylos flujos de trabajo deben estar etiquetados
- [Transfer.2] Los servidores Transfer Family no deben usar el protocolo FTP para la conexión de puntos finales
- [Transfer.3] Los conectores Transfer Family deben tener habilitado el registro
- [Transfer.4] Los acuerdos Transfer Family deben estar etiquetados
- [Transfer.5] Los certificados Transfer Family deben estar etiquetados

- [Transfer.6] Los conectores Transfer Family deben estar etiquetados
- [Transfer.7] Los perfiles de Transfer Family deben estar etiquetados
- [WAF.1]AWS WAFEl registro de ACL web global clásico debe estar habilitado
- [WAF.2]AWS WAFLas reglas regionales clásicas deben tener al menos una condición
- [WAF.3]AWS WAFLos grupos de reglas regionales clásicos deben tener al menos una regla
- [WAF.4]AWS WAFLas ACL web regionales clásicas deben tener al menos una regla o grupo de reglas
- [WAF.6]AWS WAFLas reglas globales clásicas deben tener al menos una condición
- [WAF.7]AWS WAFLos grupos de reglas globales clásicos deben tener al menos una regla
- [WAF.8]AWS WAFLas ACL web globales clásicas deben tener al menos una regla o grupo de reglas
- [WAF.10]AWS WAFLas ACL web deben tener al menos una regla o grupo de reglas
- [WAF.11]AWS WAFEl registro de ACL web debe estar habilitado
- [WAF.12]AWS WAFlas reglas deben tener CloudWatch las métricas habilitadas
- [WorkSpaces.1] los volúmenes de WorkSpaces usuarios deben cifrarse en reposo
- [WorkSpaces.2] los volúmenes WorkSpaces raíz deben cifrarse en reposo

Asia-Pacífico (Tailandia)

Los siguientes controles no se admiten en la región Asia-Pacífico (Tailandia).

- [ACM.1] ACM-issued Los certificados importados y renovados deben renovarse después de un período de tiempo específico
- [ACM.2] Los certificados RSA gestionados por ACM deben utilizar una longitud de clave de al menos 2048 bits
- [Account.1] La información de contacto de seguridad debe proporcionarse para unCuenta de AWS
- [Account.2]Cuentas de AWSdebe formar parte de unAWS Organizationsorganización
- [APIGateway.8] Las rutas de API Gateway deben especificar un tipo de autorización
- [APIGateway.9] El registro de acceso debe configurarse para las etapas V2 de API Gateway
- [APIGateway.10] Las integraciones de API Gateway V2 deben usar HTTPS para las conexiones privadas

- [Amplify.1] Las aplicaciones Amplify deben estar etiquetadas
- [Amplify.2] Amplify branches debe estar etiquetado
- [AppConfig.1]AWS AppConfiglas aplicaciones deben estar etiquetadas
- [AppConfig.2]AWS AppConfiglos perfiles de configuración deben estar etiquetados
- [AppConfig.3]AWS AppConfiglos entornos deben estar etiquetados
- [AppConfig.4]AWS AppConfiglas asociaciones de extensiones deben estar etiquetadas
- [AppFlow.1] AppFlow Los flujos de Amazon deben estar etiquetados
- [AppRunner.1] Los servicios de App Runner deben estar etiquetados
- [AppRunner.2] Los conectores VPC de App Runner deben estar etiquetados
- [AppSync.1]AWS AppSyncLas cachés de las API deben estar cifradas en reposo
- [AppSync.2]AWS AppSyncdebe tener habilitado el registro a nivel de campo
- [AppSync.5]AWS AppSyncLas API de GraphQL no deben autenticarse con claves de API
- [AppSync.6]AWS AppSyncLas cachés de las API deben cifrarse en tránsito
- [Athena.2] Los catálogos de datos de Athena deben estar etiquetados
- [Athena.3] Los grupos de trabajo de Athena deben estar etiquetados
- [Athena.4] Los grupos de trabajo de Athena deberían tener habilitado el registro
- [AutoScaling.2] El grupo Amazon EC2 Auto Scaling debe cubrir varias zonas de disponibilidad
- [AutoScaling.3] Las configuraciones de lanzamiento grupal de Auto Scaling deberían configurar las instancias EC2 para que requieran la versión 2 del Servicio de Metadatos de Instancia (IMDSv2)
- [AutoScaling.6] Los grupos de Auto Scaling deben usar varios tipos de instancias en múltiples zonas de disponibilidad
- [AutoScaling.9] Los grupos de Amazon EC2 Auto Scaling deben utilizar las plantillas de lanzamiento de Amazon EC2
- [Backup.1]AWS Backuplos puntos de recuperación deben estar cifrados en reposo
- [Backup.2]AWS Backuplos puntos de recuperación deben estar etiquetados
- [Backup.4]AWS Backuplos planes de informes deben estar etiquetados
- [Batch.1] Las colas de trabajos por lotes deben estar etiquetadas
- [Batch.2] Las políticas de programación de lotes deben estar etiquetadas
- [Batch.3] Los entornos de procesamiento por lotes deben etiquetarse

- [Batch.4] Las propiedades de los recursos de cómputo en los entornos de cómputo por lotes gestionados deben estar etiquetadas
- [BedrockAgentCore.1] Los AgentCore tiempos de ejecución de Bedrock deben configurarse con el modo de red VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways debería requerir autorización para las solicitudes entrantes
- [BedrockAgentCore.3] Bedrock AgentCore Memory debe estar cifrada y gestionada por el clienteAWS KMSclaves
- [BedrockAgentCore.4] Bedrock AgentCore Gateway debe cifrarse de forma que sea gestionada por el clienteAWS KMSclaves
- [BedrockAgentCore.5] Los navegadores AgentCore personalizados de Bedrock no deberían usar el modo de red pública
- [BedrockAgentCore.6] Los navegadores AgentCore personalizados de Bedrock deberían tener habilitada la grabación de sesiones
- [CloudFormation.3] las CloudFormation pilas deben tener habilitada la protección de terminación
- [CloudFormation.4] las CloudFormation pilas deben tener funciones de servicio asociadas
- [CloudFront.1] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado
- [CloudFront.3] CloudFront las distribuciones deben requerir el cifrado durante el tránsito
- [CloudFront.4] CloudFront las distribuciones deben tener configurada la conmutación por error de origen
- [CloudFront.5] CloudFront las distribuciones deben tener habilitado el registro
- [CloudFront.6] CloudFront las distribuciones deben tener WAF activado
- [CloudFront.7] CloudFront las distribuciones deben usar certificados personalizados SSL/TLS
- [CloudFront.8] CloudFront las distribuciones deben usar el SNI para atender las solicitudes HTTPS
- [CloudFront.9] CloudFront las distribuciones deben cifrar el tráfico para convertirlo en orígenes personalizados
- [CloudFront.10] CloudFront las distribuciones no deben usar protocolos SSL obsoletos entre ubicaciones de borde y orígenes personalizados
- [CloudFront.12] CloudFront las distribuciones no deben apuntar a orígenes de S3 inexistentes
- [CloudFront.13] CloudFront las distribuciones deben usar el control de acceso al origen
- [CloudFront.14] CloudFront las distribuciones deben estar etiquetadas

- [CloudFront.15] CloudFront las distribuciones deben usar la política de seguridad TLS recomendada
- [CloudFront.16] CloudFront las distribuciones deben usar el control de acceso de origen para los orígenes de las URL de las funciones de Lambda
- [CloudFront.17] CloudFront las distribuciones deben usar grupos de claves confiables para las URL y cookies firmadas
- [CloudTrail.6] Asegúrese de que el depósito de S3 que se utiliza para almacenar CloudTrail los registros no sea de acceso público
- [CloudTrail.7] Asegúrese de que el registro de acceso al bucket de S3 esté habilitado en el CloudTrail bucket de S3
- [CloudTrail.10] Los almacenes de datos de eventos de CloudTrail Lake deben estar cifrados y gestionados por el clienteAWS KMS keys
- [CloudWatch.17] las acciones CloudWatch de alarma deben estar activadas
- [CodeArtifact.1] CodeArtifact los repositorios deben estar etiquetados
- [CodeBuild.1] Las URL del repositorio fuente de CodeBuild Bitbucket no deben contener credenciales confidenciales
- [CodeBuild.2] las variables de entorno CodeBuild del proyecto no deben contener credenciales de texto claro
- [CodeBuild.3] Los registros de CodeBuild S3 deben estar cifrados
- [CodeBuild.4] los entornos de CodeBuild proyectos deben tener un registroAWS ConfigDuración
- [CodeBuild.7] las exportaciones de grupos de CodeBuild informes deben cifrarse en reposo
- [CodeGuruProfiler.1] Los grupos CodeGuru de creación de perfiles de Profiler deben estar etiquetados
- [CodeGuruReviewer.1] Las asociaciones de repositorios de CodeGuru Reviewer deben estar etiquetadas
- [Cognito.1] Los grupos de usuarios de Cognito deben tener activada la protección contra amenazas y el modo de aplicación con todas las funciones para la autenticación estándar
- [Cognito.2] Los grupos de identidades de Cognito no deben permitir identidades no autenticadas
- [Cognito.3] Las políticas de contraseñas para los grupos de usuarios de Cognito deben tener configuraciones sólidas
- [Cognito.4] Los grupos de usuarios de Cognito deben tener activada la protección contra amenazas y el modo de aplicación con todas las funciones para la autenticación personalizada

- [Cognito.5] La MFA debe estar habilitada para los grupos de usuarios de Cognito
- [Cognito.6] Los grupos de usuarios de Cognito deben tener habilitada la protección contra la eliminación
- [Connect.1] Los tipos de objetos de los perfiles de clientes de Amazon Connect deben estar etiquetados
- [Connect.2] Las instancias de Connect Customer deben tener el CloudWatch registro habilitado
- [DataFirehose.1] Los flujos de entrega de Firehose deben cifrarse en reposo
- [DataSync.1] DataSync las tareas deberían tener el registro activado
- [DataSync.2] DataSync las tareas deben estar etiquetadas
- [Detective.1] Los gráficos de comportamiento de los detectives deben estar etiquetados
- [DMS.2] Los certificados DMS deben estar etiquetados
- [DMS.3] Las suscripciones a eventos de DMS deben estar etiquetadas
- [DMS.4] Las instancias de replicación de DMS deben estar etiquetadas
- [DMS.5] Los grupos de subredes de replicación del DMS deben estar etiquetados
- [DMS.6] Las instancias de replicación de DMS deben tener habilitada la actualización automática de las versiones secundarias
- [DMS.7] Las tareas de replicación del DMS para la base de datos de destino deben tener el registro habilitado
- [DMS.8] Las tareas de replicación del DMS para la base de datos de origen deben tener el registro activado
- [DMS.9] Los puntos finales del DMS deben usar SSL
- [DMS.10] Los puntos finales de DMS para las bases de datos de Neptune deben tener habilitada la autorización de IAM
- [DMS.11] Los puntos finales de DMS para MongoDB deben tener un mecanismo de autenticación habilitado
- [DMS.12] Los puntos finales de DMS para Redis OSS deben tener el TLS habilitado
- [DMS.13] Las instancias de replicación de DMS deben configurarse para usar varias zonas de disponibilidad
- [DocumentDB.1] Los clústeres de Amazon DocumentDB deben cifrarse en reposo
- [DocumentDB.2] Los clústeres de Amazon DocumentDB deben tener un período de retención de copias de seguridad adecuado

- [DocumentDB.3] Las instantáneas de clústeres manuales de Amazon DocumentDB no deben ser públicas
- [DocumentDB.4] Los clústeres de Amazon DocumentDB deben publicar los registros de auditoría en Logs CloudWatch
- [DocumentDB.5] Los clústeres de Amazon DocumentDB deben tener habilitada la protección contra eliminaciones
- [DocumentDB.6] Los clústeres de Amazon DocumentDB deben cifrarse en tránsito
- [DynamoDB.3] Los clústeres de DynamoDB Accelerator (DAX) deben cifrarse en reposo
- [DynamoDB.4] Las tablas de DynamoDB deben estar presentes en un plan de respaldo
- [DynamoDB.6] Las tablas de DynamoDB deben tener habilitada la protección de eliminación
- [DynamoDB.7] Los clústeres de DynamoDB Accelerator deben cifrarse en tránsito
- [EC2.4] Las instancias EC2 detenidas deben eliminarse después de un período de tiempo específico
- [EC2.21] Las ACL de red no deberían permitir la entrada desde la versión 0.0.0. 0/0 al puerto 22 o al puerto 3389
- [EC2.22] Deben eliminarse los grupos de seguridad de Amazon EC2 no utilizados
- [EC2.23] Amazon EC2 Transit Gateways no debe aceptar automáticamente las solicitudes de adjuntos de VPC
- [EC2.24] No se deben utilizar los tipos de instancias paravirtuales de Amazon EC2
- [EC2.25] Las plantillas de lanzamiento de Amazon EC2 no deben asignar direcciones IP públicas a las interfaces de red
- [EC2.28] Los volúmenes de EBS deben estar cubiertos por un plan de respaldo
- [EC2.34] Las tablas de rutas de la pasarela de tránsito EC2 deben estar etiquetadas
- [EC2.40] Las pasarelas NAT EC2 deben estar etiquetadas
- [EC2.51] Los puntos finales EC2 Client VPN deben tener habilitado el registro de conexiones de clientes
- [EC2.53] Los grupos de seguridad de EC2 no deberían permitir la entrada desde la versión 0.0.0. 0/0 a los puertos de administración remota del servidor
- [EC2.54] Los grupos de seguridad de EC2 no deberían permitir la entrada desde: :/0 a los puertos de administración remota del servidor
- [EC2.55] Las VPC deben configurarse con un punto final de interfaz para la API de ECR

- [EC2.56] Las VPC deben configurarse con un punto final de interfaz para Docker Registry
- [EC2.57] Las VPC deben configurarse con un punto final de interfaz para Systems Manager
- [EC2.58] Las VPC deben configurarse con un punto final de interfaz para los contactos de Systems Manager Incident Manager
- [EC2.60] Las VPC deben configurarse con un punto final de interfaz para Systems Manager Incident Manager
- [EC2.170] Las plantillas de lanzamiento de EC2 deben utilizar la versión 2 del servicio de metadatos de instancias (IMDSv2)
- [EC2.171] Las conexiones VPN de EC2 deberían tener el registro habilitado
- [EC2.172] La configuración de acceso público del bloque de VPC de EC2 debería bloquear el tráfico de la puerta de enlace de Internet
- [EC2.173] Las solicitudes de EC2 Spot Fleet con parámetros de lanzamiento deberían permitir el cifrado de los volúmenes de EBS adjuntos
- [EC2.174] Los conjuntos de opciones DHCP de EC2 deben estar etiquetados
- [EC2.175] Las plantillas de lanzamiento de EC2 deben estar etiquetadas
- [EC2.176] Las listas de prefijos de EC2 deben estar etiquetadas
- [EC2.177] Las sesiones de réplica de tráfico de EC2 deben etiquetarse
- [EC2.178] Los filtros espejo de tráfico EC2 deben estar etiquetados
- [EC2.179] Los objetivos del espejo de tráfico de EC2 deben estar etiquetados
- [EC2.180] Las interfaces de red EC2 deberían tener habilitada source/destination la verificación
- [EC2.181] Las plantillas de lanzamiento de EC2 deberían permitir el cifrado de los volúmenes de EBS adjuntos
- [EC2.182] La configuración de bloqueo de acceso público debe estar habilitada para las instantáneas de Amazon EBS
- [EC2.183] Las conexiones VPN de EC2 deben utilizar el protocolo IKEv2
- [ECR.1] Los repositorios privados de ECR deben tener configurado el escaneo de imágenes
- [ECR.2] Los repositorios privados de ECR deben tener configurada la inmutabilidad de etiquetas
- [ECR.3] Los repositorios de ECR deben tener configurada al menos una política de ciclo de vida
- [ECR.4] Los repositorios públicos de ECR deben etiquetarse
- [ECR.5] Los repositorios de ECR deben estar cifrados y ser gestionados por el cliente AWS KMS keys

- [ECS.3] Las definiciones de tareas de ECS no deben compartir el espacio de nombres del proceso del host
- [ECS.4] Los contenedores ECS deben ejecutarse sin privilegios
- [ECS.5] Las definiciones de tareas de ECS deben configurar los contenedores para que se limiten al acceso de solo lectura a los sistemas de archivos raíz
- [ECS.8] Los secretos no deben transmitirse como variables de entorno de contenedores
- [ECS.9] Las definiciones de tareas de ECS deben tener una configuración de registro
- [ECS.10] Los servicios Fargate de ECS deberían ejecutarse en la última versión de la plataforma Fargate
- [ECS.12] Los clústeres de ECS deben usar Container Insights
- [ECS.16] Los conjuntos de tareas de ECS no deben asignar automáticamente direcciones IP públicas
- [ECS.17] Las definiciones de tareas de ECS no deben usar el modo de red host
- [ECS.18] Las definiciones de tareas de ECS deben utilizar el cifrado en tránsito para los volúmenes de EFS
- [ECS.19] Los proveedores de capacidad de ECS deberían tener habilitada la protección de terminación gestionada
- [ECS.20] Las definiciones de tareas de ECS deben configurar a los usuarios no root en las definiciones de contenedores de Linux
- [ECS.21] Las definiciones de tareas de ECS deberían configurar a los usuarios no administradores en las definiciones de contenedores de Windows
- [EFS.1] Elastic File System debe configurarse para cifrar los datos de los archivos en reposo mediante AWS KMS
- [EFS.2] Los volúmenes de Amazon EFS deben figurar en los planes de copia de seguridad
- [EFS.3] Los puntos de acceso EFS deben exigir un directorio raíz
- [EFS.4] Los puntos de acceso EFS deben exigir la identidad del usuario
- [EFS.6] Los destinos de montaje de EFS no deben asociarse a subredes que asignan direcciones IP públicas en el momento del lanzamiento
- [] Los sistemas de archivos EFS deben tener habilitadas las copias de seguridad automáticas EFS.7
- [EFS.8] Los sistemas de archivos EFS deben cifrarse en reposo

- [EKS.2] Los clústeres de EKS deben ejecutarse en una versión de Kubernetes compatible
- [EKS.3] Los clústeres de EKS deben usar secretos de Kubernetes cifrados
- [EKS.7] Las configuraciones del proveedor de identidad de EKS deben etiquetarse
- [EKS.8] Los clústeres de EKS deben tener habilitado el registro de auditoría
- [EKS.9] Los grupos de nodos de EKS deben ejecutarse en una versión de Kubernetes compatible
- [ELB.10] El balanceador de carga clásico debe abarcar varias zonas de disponibilidad
- [ELB.12] El balanceador de carga de aplicaciones debe configurarse con el modo defensivo o de mitigación de desincronización más estricto
- [ELB.13] Los balanceadores de carga de aplicaciones, redes y puertas de enlace deben abarcar varias zonas de disponibilidad
- [ELB.14] El balanceador de carga clásico debe configurarse con el modo defensivo o de mitigación de desincronización más estricto
- [ELB.17] Los balanceadores de cargas de aplicaciones y redes con oyentes deben usar las políticas de seguridad recomendadas
- [ELB.18] Los oyentes del balanceador de cargas de red y aplicaciones deben usar protocolos seguros para cifrar los datos en tránsito
- [ElastiCache.1] ElastiCache (Redis OSS) los clústeres deben tener habilitadas las copias de seguridad automáticas
- [ElastiCache.2] ElastiCache los clústeres deberían tener habilitadas las actualizaciones automáticas de las versiones secundarias
- [ElastiCache.3] los grupos de ElastiCache replicación deberían tener habilitada la conmutación por error automática
- [ElastiCache.4] los grupos de ElastiCache replicación deben cifrarse en reposo
- [ElastiCache.5] los grupos de ElastiCache replicación deben cifrarse en tránsito
- [ElastiCache.6] ElastiCache (Redis OSS) Los grupos de replicación de versiones anteriores deberían tener habilitada la autenticación de Redis OSS
- [ElastiCache.7] los ElastiCache clústeres no deben usar el grupo de subredes predeterminado
- [ElasticBeanstalk.1] Los entornos de Elastic Beanstalk deberían tener habilitados los informes de estado mejorados
- [ElasticBeanstalk.2] Las actualizaciones de la plataforma gestionada de Elastic Beanstalk deben estar habilitadas

- [ElasticBeanstalk.3] Elastic Beanstalk debería transmitir los registros a CloudWatch
- [EMR.1] Los nodos principales del clúster de Amazon EMR no deben tener direcciones IP públicas
- [EMR.2] La configuración de acceso público del bloque Amazon EMR debe estar habilitada
- [EMR.3] Las configuraciones de seguridad de Amazon EMR deben cifrarse en reposo
- [EMR.4] Las configuraciones de seguridad de Amazon EMR deben cifrarse en tránsito
- [ES.4] Debería estar habilitado el registro de errores de dominio de Elasticsearch en Logs CloudWatch
- [ES.9] Los dominios de Elasticsearch deben etiquetarse
- [EventBridge.3] los autobuses de eventos EventBridge personalizados deben tener adjunta una política basada en los recursos
- [EventBridge.4] los puntos finales EventBridge globales deberían tener habilitada la replicación de eventos
- [FraudDetector.1] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.2] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas
- [FraudDetector.3] Los resultados de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.4] Las variables de Amazon Fraud Detector deben estar etiquetadas
- [FSx.1] FSx para sistemas de archivos OpenZFS debe configurarse para copiar etiquetas en copias de seguridad y volúmenes
- [FSx.2] Los sistemas de archivos FSx for Lustre deben configurarse para copiar etiquetas a las copias de seguridad
- [FSx.3] FSx para sistemas de archivos OpenZFS debe configurarse para su implementación Multi-AZ
- [FSx.4] FSx para sistemas de archivos NetApp ONTAP debe configurarse para su implementación Multi-AZ
- [FSx.5] Los sistemas de archivos FSx for Windows File Server deben configurarse para Multi-AZ su implementación
- [GlobalAccelerator.1] Los aceleradores de Global Accelerator deben estar etiquetados
- [Glue.1]AWS Gluelos trabajos deben estar etiquetados
- [Glue.3]AWS GlueLas transformaciones de aprendizaje automático deben cifrarse en reposo
- [Glue.4]AWS GlueLos trabajos de Spark deberían ejecutarse en versiones compatibles deAWS Glue

- [GuardDuty.1] GuardDuty debería estar activado
- GuardDuty Los filtros [GuardDuty.2] deben estar etiquetados
- [GuardDuty.5] La monitorización del registro de auditoría de GuardDuty EKS debe estar habilitada
- [GuardDuty.6] GuardDuty La protección Lambda debe estar habilitada
- [GuardDuty.7] La monitorización del tiempo de ejecución de GuardDuty EKS debe estar habilitada
- [GuardDuty.8] La protección contra GuardDuty malware para EC2 debe estar habilitada
- [GuardDuty.9] La protección GuardDuty RDS debe estar habilitada
- [GuardDuty.10] La protección GuardDuty S3 debe estar habilitada
- [GuardDuty.11] La monitorización del GuardDuty tiempo de ejecución debe estar habilitada
- [GuardDuty.12] La monitorización del tiempo de ejecución de GuardDuty ECS debe estar habilitada
- [GuardDuty.13] La monitorización del tiempo de ejecución de GuardDuty EC2 debe estar habilitada
- [IAM.1] Las políticas de IAM no deberían permitir todos los privilegios administrativos «*»
- [IAM.2] Los usuarios de IAM no deberían tener políticas de IAM adjuntas
- [IAM.3] Las claves de acceso de los usuarios de IAM deben rotarse cada 90 días o menos
- [IAM.4] La clave de acceso del usuario raíz de IAM no debería existir
- [IAM.5] La MFA debe estar habilitada para todos los usuarios de IAM que tengan una contraseña de consola
- [IAM.6] La MFA de hardware debe estar habilitada para el usuario root
- [IAM.7] Las políticas de contraseñas para los usuarios de IAM deben tener configuraciones sólidas
- [IAM.8] Se deben eliminar las credenciales de usuario de IAM no utilizadas
- [IAM.9] La MFA debe estar habilitada para el usuario root
- [IAM.10] Las políticas de contraseñas para los usuarios de IAM deben tener configuraciones sólidas
- [IAM.11] Asegúrese de que la política de contraseñas de IAM requiera al menos una letra mayúscula
- [IAM.12] Asegúrese de que la política de contraseñas de IAM requiera al menos una letra minúscula
- [IAM.13] Asegúrese de que la política de contraseñas de IAM requiera al menos un símbolo
- [IAM.14] Asegúrese de que la política de contraseñas de IAM requiera al menos un número

- [IAM.15] Asegúrese de que la política de contraseñas de IAM exija una longitud de contraseña mínima de 14 o más
- [IAM.16] Asegúrese de que la política de contraseñas de IAM impida la reutilización de contraseñas
- [IAM.17] Asegúrese de que la política de contraseñas de IAM haga caducar las contraseñas en un plazo de 90 días o menos
- [IAM.18] Asegúrese de que se haya creado una función de soporte para gestionar los incidentes conAWS Support
- [IAM.19] La MFA debe estar habilitada para todos los usuarios de IAM
- [IAM.21] Las políticas de IAM gestionadas por el cliente que cree no deberían permitir acciones comodín en los servicios
- [IAM.22] Se deben eliminar las credenciales de usuario de IAM que no se hayan utilizado durante 45 días
- [IAM.24] Las funciones de IAM deben estar etiquetadas
- [IAM.25] Los usuarios de IAM deben estar etiquetados
- [IAM.26] SSL/TLS Los certificados caducados gestionados en IAM deben eliminarse
- [IAM.27] Las identidades de IAM no deberían tener la AWSCloudShellFullAccess política adjunta
- [IAM.28] El analizador de acceso externo de IAM Access Analyzer debe estar habilitado
- [Inspector.1] El escaneo EC2 de Amazon Inspector debe estar activado
- [Inspector.2] El escaneo ECR de Amazon Inspector debe estar activado
- [Inspector.3] El escaneo de código Lambda de Amazon Inspector Lambda debe estar activado
- [Inspector.4] El escaneo estándar de Amazon Inspector Lambda debe estar activado
- [IoT.1]AWS IoT Device Defenderlos perfiles de seguridad deben estar etiquetados
- [IoT.2]AWS IoT Corelas acciones de mitigación deben estar etiquetadas
- [IoT.3]AWS IoT Corelas dimensiones deben estar etiquetadas
- [IoT.4]AWS IoT Corelos autorizadores deben estar etiquetados
- [IoT.5]AWS IoT CoreLos alias de los roles deben estar etiquetados
- [IoT.6]AWS IoT Corelas políticas deben estar etiquetadas
- [IoTSiteWise.1]AWSLos modelos SiteWise de activos de IoT deben estar etiquetados
- [IoTSiteWise.2]AWS SiteWise Los paneles de IoT deben estar etiquetados

- [IoTSiteWise.3]AWS SiteWise Las pasarelas de IoT deben estar etiquetadas
- [IoTSiteWise.4]AWS SiteWise Los portales de IoT deben estar etiquetados
- [IoTSiteWise.5]AWS SiteWise Los proyectos de IoT deben estar etiquetados
- [IoTTwinMaker.1]AWSLos trabajos de TwinMaker sincronización de IoT deben estar etiquetados
- [IoTTwinMaker.2]AWS TwinMaker Los espacios de trabajo de IoT deben estar etiquetados
- [IoTTwinMaker.3]AWS TwinMaker Las escenas de IoT deben estar etiquetadas
- [IoTTwinMaker.4]AWS TwinMaker Las entidades de IoT deben estar etiquetadas
- [IoTWireless.1]AWSLos grupos de multidifusión de IoT Wireless deben estar etiquetados
- [IoTWireless.2]AWSLos perfiles de servicio de IoT Wireless deben estar etiquetados
- [IoTWireless.3]AWSLas tareas de IoT FUOTA deben estar etiquetadas
- [IVS.1] Los pares de teclas de reproducción IVS deben estar etiquetados
- [IVS.2] Las configuraciones de grabación de IVS deben estar etiquetadas
- [IVS.3] Los canales IVS deben estar etiquetados
- [Keyspaces.1] Los espacios clave de Amazon Keyspaces deben estar etiquetados
- [Kinesis.1] Las transmisiones de Kinesis deben cifrarse en reposo
- [Kinesis.3] Las transmisiones de Kinesis deben tener un período de retención de datos adecuado
- [KMS.1] Las políticas gestionadas por los clientes de IAM no deberían permitir acciones de descifrado en todas las claves de KMS
- [KMS.2] Los directores de IAM no deberían tener políticas integradas de IAM que permitan realizar acciones de descifrado en todas las claves de KMS
- [KMS.5] Las claves KMS no deben ser de acceso público
- [Lambda.5] Las funciones de VPC Lambda deben funcionar en varias zonas de disponibilidad
- [Lambda.7] Las funciones de Lambda deberían tener AWS X-Ray el rastreo activo está habilitado
- [Macie.1] Amazon Macie debería estar activado
- [Macie.2] La detección automática de datos confidenciales por parte de Macie debería estar habilitada
- [MQ.2] Los corredores de ActiveMQ deben transmitir los registros de auditoría a CloudWatch
- [MQ.4] Los corredores de Amazon MQ deben estar etiquetados
- [MQ.5] Los corredores de ActiveMQ deberían usar el modo de implementación active/standby

- [MQ.6] Los corredores de RabbitMQ deberían usar el modo de despliegue de clústeres
- [MSK.1] Los clústeres de MSK deben cifrarse en tránsito entre los nodos de intermediación
- [MSK.2] Los clústeres de MSK deberían tener configurada una supervisión mejorada
- [MSK.3] Los conectores MSK Connect deben estar cifrados en tránsito
- [MSK.4] Los clústeres de MSK deben tener el acceso público deshabilitado
- [MSK.5] Los conectores MSK deben tener el registro activado
- [MSK.6] Los clústeres de MSK deberían deshabilitar el acceso no autenticado
- [Neptune.1] Los clústeres de bases de datos de Neptune deben cifrarse en reposo
- [Neptune.2] Los clústeres de bases de datos de Neptune deberían publicar registros de auditoría en Logs CloudWatch
- [Neptune.3] Las instantáneas del clúster de base de datos de Neptune no deben ser públicas
- [Neptune.4] Los clústeres de base de datos de Neptune deben tener habilitada la protección contra eliminación
- [Neptune.5] Los clústeres de Neptune DB deberían tener habilitadas las copias de seguridad automatizadas
- [Neptune.6] Las instantáneas del clúster de base de datos de Neptune deben cifrarse en reposo
- [Neptune.7] Los clústeres de base de datos de Neptune deben tener habilitada la autenticación de bases de datos de IAM
- [Neptune.8] Los clústeres de bases de datos de Neptune deben configurarse para copiar etiquetas a las instantáneas
- [Neptune.9] Los clústeres de base de datos Neptune deben implementarse en varias zonas de disponibilidad
- [NetworkFirewall.1] Los firewalls de Network Firewall deben implementarse en varias zonas de disponibilidad
- [NetworkFirewall.2] El registro de Network Firewall debe estar habilitado
- [NetworkFirewall.3] Las políticas de Network Firewall deben tener asociado al menos un grupo de reglas
- [NetworkFirewall.4] La acción sin estado predeterminada para las políticas de Network Firewall debe ser eliminar o reenviar paquetes completos
- [NetworkFirewall.5] La acción sin estado predeterminada para las políticas de Network Firewall debe ser eliminar o reenviar paquetes fragmentados

- [NetworkFirewall.6] El grupo de reglas de Stateless Network Firewall no debe estar vacío
- [NetworkFirewall.9] Los firewalls de Network Firewall deben tener habilitada la protección de eliminación
- [NetworkFirewall.10] Los firewalls de Network Firewall deben tener habilitada la protección contra cambios de subred
- [Opensearch.1] OpenSearch los dominios deben tener activado el cifrado en reposo
- [Opensearch.2] OpenSearch los dominios no deben ser de acceso público
- [Opensearch.3] OpenSearch los dominios deben cifrar los datos enviados entre nodos
- [Opensearch.4] El registro de errores de OpenSearch dominio en Logs debe estar habilitado CloudWatch
- [Opensearch.5] OpenSearch los dominios deben tener activado el registro de auditoría
- [Opensearch.6] OpenSearch los dominios deben tener al menos tres nodos de datos
- [Opensearch.7] OpenSearch los dominios deben tener habilitado un control de acceso detallado
- [Opensearch.8] Las conexiones a los OpenSearch dominios deben cifrarse con la última política de seguridad de TLS
- [Opensearch.9] OpenSearch los dominios deben estar etiquetados
- [Opensearch.10] OpenSearch los dominios deben tener instalada la última actualización de software
- [Opensearch.11] OpenSearch los dominios deben tener al menos tres nodos principales dedicados
- [PCA.1]AWS Privada CALa autoridad emisora de certificados raíz debe estar deshabilitada
- [PCA.2]AWSLas autoridades de certificación de CA privadas deben estar etiquetadas
- [RDS.14] Los clústeres de Amazon Aurora deben tener habilitado el retroceso
- [RDS.24] Los clústeres de bases de datos de RDS deben usar un nombre de usuario de administrador personalizado
- [RDS.25] Las instancias de bases de datos de RDS deben usar un nombre de usuario de administrador personalizado
- [RDS.26] Las instancias de base de datos de RDS deben protegerse mediante un plan de respaldo
- [RDS.27] Los clústeres de bases de datos de RDS deben cifrarse en reposo
- [RDS.31] Los grupos de seguridad de la base de datos de RDS deben etiquetarse
- [RDS.34] Los clústeres de bases de datos Aurora MySQL deben publicar los registros de auditoría en Logs CloudWatch

- [RDS.35] Los clústeres de bases de datos de RDS deben tener habilitada la actualización automática de versiones secundarias
- [RDS.36] Las instancias de base de datos de RDS para PostgreSQL deben publicar los registros en Logs CloudWatch
- [RDS.37] Los clústeres de bases de datos de Aurora PostgreSQL deben publicar los registros en Logs CloudWatch
- [RDS.38] Las instancias de base de datos de RDS para PostgreSQL deben cifrarse en tránsito
- [RDS.39] Las instancias de base de datos de RDS para MySQL deben cifrarse en tránsito
- [RDS.40] Las instancias de base de datos de RDS para SQL Server deben publicar los registros en Logs CloudWatch
- [RDS.41] Las instancias de base de datos de RDS para SQL Server deben cifrarse en tránsito
- [RDS.42] Las instancias de base de datos de RDS para MariaDB deben publicar los registros en Logs CloudWatch
- [RDS.43] Los proxies de bases de datos de RDS deben requerir el cifrado TLS para las conexiones
- [RDS.44] Las instancias de base de datos de RDS para MariaDB deben cifrarse durante el tránsito
- [RDS.45] Los clústeres de bases de datos Aurora MySQL deben tener habilitado el registro de auditoría
- [RDS.46] Las instancias de base de datos de RDS no deben implementarse en subredes públicas con rutas a pasarelas de Internet
- [RDS.47] Los clústeres de bases de datos de RDS para PostgreSQL deben configurarse para copiar las etiquetas a las instantáneas de bases de datos
- [RDS.48] Los clústeres de bases de datos de RDS para MySQL deben configurarse para copiar etiquetas a las instantáneas de bases de datos
- [RDS.51] Los clústeres globales de RDS deben ejecutarse en una versión compatible de Aurora MySQL
- [Redshift.8] Los clústeres de Amazon Redshift no deben usar el nombre de usuario de administrador predeterminado
- [Redshift.10] Los clústeres de Redshift deben cifrarse en reposo
- [Redshift.15] Los grupos de seguridad de Redshift deberían permitir la entrada en el puerto del clúster solo desde orígenes restringidos
- [Redshift.16] Los grupos de subredes de clústeres de Redshift deben tener subredes de varias zonas de disponibilidad

- [Redshift.17] Los grupos de parámetros del clúster de Redshift deben estar etiquetados
- [Redshift.18] Los clústeres de Redshift deberían tener Multi-AZ las implementaciones habilitadas
- [RedshiftServerless.1] Los grupos de trabajo sin servidor de Amazon Redshift deberían utilizar un enrutamiento de VPC mejorado
- [RedshiftServerless.2] Las conexiones a los grupos de trabajo sin servidor de Redshift deberían ser obligatorias para usar SSL
- [RedshiftServerless.3] Los grupos de trabajo sin servidor de Redshift deberían prohibir el acceso público
- [RedshiftServerless.4] Los espacios de nombres de Redshift Serverless deben cifrarse y administrarse por el clienteAWS KMS keys
- [RedshiftServerless.5] Los espacios de nombres Redshift Serverless no deben usar el nombre de usuario de administrador predeterminado
- [RedshiftServerless.6] Los espacios de nombres Redshift Serverless deberían exportar los registros a los registros CloudWatch
- [Route53.1] Los controles de salud de Route 53 deben estar etiquetados
- [Route53.2] Las zonas alojadas públicas de Route 53 deberían registrar las consultas de DNS
- [S3.7] Los cubos de uso general de S3 deben utilizar la replicación entre regiones
- [S3.10] Los cubos de uso general de S3 con el control de versiones habilitado deben tener configuraciones de ciclo de vida
- [S3.11] Los cubos de uso general de S3 deben tener habilitadas las notificaciones de eventos
- [S3.12] Las ACL no deben usarse para administrar el acceso de los usuarios a los cubos de uso general de S3
- [S3.13] Los cubos de uso general de S3 deben tener configuraciones de ciclo de vida
- [S3.19] Los puntos de acceso S3 deben tener habilitada la configuración de bloqueo de acceso público
- [S3.20] Los cubos de uso general de S3 deben tener habilitada la eliminación de MFA
- [S3.22] Los cubos de uso general de S3 deben registrar los eventos de escritura a nivel de objeto
- [S3.23] Los cubos de uso general de S3 deben registrar los eventos de lectura a nivel de objeto
- [S3.24] Los puntos de Multi-Region acceso S3 deben tener habilitada la configuración de bloqueo del acceso público
- [S3.25] Los buckets de directorio de S3 deben tener configuraciones de ciclo de vida

- [SageMaker.1] Las instancias de Amazon SageMaker Notebook no deberían tener acceso directo a Internet
- [SageMaker.2] las instancias de SageMaker cuadernos deben lanzarse en una VPC personalizada
- [SageMaker.3] Los usuarios no deben tener acceso root a las instancias de los SageMaker cuadernos
- [SageMaker.4] Las variantes de producción de SageMaker terminales deben tener un recuento inicial de instancias superior a 1
- SageMaker Los modelos [SageMaker.5] deben tener habilitado el aislamiento de red
- [SageMaker.6] las configuraciones de imagen de la SageMaker aplicación deben estar etiquetadas
- [SageMaker.7] SageMaker las imágenes deben estar etiquetadas
- [SageMaker.8] las instancias de SageMaker notebooks deben ejecutarse en plataformas compatibles
- [SageMaker.9] las definiciones de trabajos de calidad de los SageMaker datos deben tener habilitado el cifrado del tráfico entre contenedores
- [SageMaker.10] Las definiciones de trabajos de explicabilidad del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores
- [SageMaker.11] las definiciones de trabajos SageMaker de calidad de los datos deben tener habilitado el aislamiento de red
- [SageMaker.12] las definiciones de trabajo basadas en el sesgo del SageMaker modelo deben tener habilitado el aislamiento de red
- [SageMaker.13] las definiciones de trabajos de calidad del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores
- [SageMaker.14] los programas SageMaker de monitoreo deben tener habilitado el aislamiento de la red
- [SageMaker.15] Las definiciones de trabajo basadas en el sesgo del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores
- SageMaker Los modelos [SageMaker.16] deben usar un registro privado en la VPC para los contenedores principales
- [SageMaker.17] SageMaker Las tiendas offline de los grupos de funciones deben cifrarse con AWS KMS claves
- [SageMaker.18] las tiendas en línea de grupos de SageMaker funciones con almacenamiento estándar deben cifrarse con AWS KMS claves

- [SageMaker.19] SageMaker los modelos deben usar un registro privado en la VPC para las canalizaciones de inferencia de varios contenedores
- [SES.1] Las listas de contactos de SES deben estar etiquetadas
- [SES.2] Los conjuntos de configuración de SES deben estar etiquetados
- [SES.3] Los conjuntos de configuración de SES deben tener el TLS habilitado para enviar correos electrónicos
- [ServiceCatalog.1] Las carteras de Service Catalog deben compartirse dentro de unAWSsolo una organización
- [SNS.4] Las políticas de acceso a los temas de SNS no deberían permitir el acceso público
- [SQS.1] Las colas de Amazon SQS deben cifrarse en reposo
- [SQS.2] Las colas de SQS deben estar etiquetadas
- [SQS.3] Las políticas de acceso a las colas de SQS no deberían permitir el acceso público
- [SSM.3] Las instancias de Amazon EC2 administradas por Systems Manager deben tener el estado de conformidad de la asociación de COMPLIANT
- [SSM.4] Los documentos SSM no deben ser públicos
- [SSM.5] Los documentos SSM deben estar etiquetados
- [SSM.6] SSM Automation debería tener el registro habilitado CloudWatch
- [SSM.7] Los documentos SSM deben tener habilitada la configuración de bloqueo para compartir en público
- [StepFunctions.1] Step Functions indica que las máquinas deben tener el registro activado
- [Transfer.1]AWS Transfer Familylos flujos de trabajo deben estar etiquetados
- [Transfer.2] Los servidores Transfer Family no deben usar el protocolo FTP para la conexión de puntos finales
- [Transfer.3] Los conectores Transfer Family deben tener habilitado el registro
- [Transfer.4] Los acuerdos Transfer Family deben estar etiquetados
- [Transfer.5] Los certificados Transfer Family deben estar etiquetados
- [Transfer.6] Los conectores Transfer Family deben estar etiquetados
- [Transfer.7] Los perfiles de Transfer Family deben estar etiquetados
- [WAF.1]AWS WAFEl registro de ACL web global clásico debe estar habilitado
- [WAF.2]AWS WAFLas reglas regionales clásicas deben tener al menos una condición

- [WAF.3]AWS WAFLos grupos de reglas regionales clásicos deben tener al menos una regla
- [WAF.4]AWS WAFLas ACL web regionales clásicas deben tener al menos una regla o grupo de reglas
- [WAF.6]AWS WAFLas reglas globales clásicas deben tener al menos una condición
- [WAF.7]AWS WAFLos grupos de reglas globales clásicos deben tener al menos una regla
- [WAF.8]AWS WAFLas ACL web globales clásicas deben tener al menos una regla o grupo de reglas
- [WAF.10]AWS WAFLas ACL web deben tener al menos una regla o grupo de reglas
- [WAF.12]AWS WAFlas reglas deben tener CloudWatch las métricas habilitadas
- [WorkSpaces.1] los volúmenes de WorkSpaces usuarios deben cifrarse en reposo
- [WorkSpaces.2] los volúmenes WorkSpaces raíz deben cifrarse en reposo

Asia-Pacífico (Tokio)

Los siguientes controles no se admiten en la región Asia-Pacífico (Tokio).

- [AppSync.1]AWS AppSyncLas cachés de las API deben estar cifradas en reposo
- [AppSync.6]AWS AppSyncLas cachés de las API deben cifrarse en tránsito
- [CloudFront.1] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado
- [CloudFront.3] CloudFront las distribuciones deben requerir el cifrado durante el tránsito
- [CloudFront.4] CloudFront las distribuciones deben tener configurada la conmutación por error de origen
- [CloudFront.5] CloudFront las distribuciones deben tener habilitado el registro
- [CloudFront.6] CloudFront las distribuciones deben tener WAF activado
- [CloudFront.7] CloudFront las distribuciones deben usar certificados personalizados SSL/TLS
- [CloudFront.8] CloudFront las distribuciones deben usar el SNI para atender las solicitudes HTTPS
- [CloudFront.9] CloudFront las distribuciones deben cifrar el tráfico para convertirlo en orígenes personalizados
- [CloudFront.10] CloudFront las distribuciones no deben usar protocolos SSL obsoletos entre ubicaciones de borde y orígenes personalizados
- [CloudFront.12] CloudFront las distribuciones no deben apuntar a orígenes de S3 inexistentes

- [CloudFront.13] CloudFront las distribuciones deben usar el control de acceso al origen
- [CloudFront.14] CloudFront las distribuciones deben estar etiquetadas
- [CloudFront.15] CloudFront las distribuciones deben usar la política de seguridad TLS recomendada
- [CloudFront.16] CloudFront las distribuciones deben usar el control de acceso de origen para los orígenes de las URL de las funciones de Lambda
- [CloudFront.17] CloudFront las distribuciones deben usar grupos de claves confiables para las URL y cookies firmadas
- [EC2.173] Las solicitudes de EC2 Spot Fleet con parámetros de lanzamiento deberían permitir el cifrado de los volúmenes de EBS adjuntos
- [ECR.4] Los repositorios públicos de ECR deben etiquetarse
- [FraudDetector.1] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.2] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas
- [FraudDetector.3] Los resultados de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.4] Las variables de Amazon Fraud Detector deben estar etiquetadas
- [GlobalAccelerator.1] Los aceleradores de Global Accelerator deben estar etiquetados
- [IAM.26] SSL/TLS Los certificados caducados gestionados en IAM deben eliminarse
- [IoTTwinMaker.4]AWS TwinMaker Las entidades de IoT deben estar etiquetadas
- [Route53.1] Los controles de salud de Route 53 deben estar etiquetados
- [Route53.2] Las zonas alojadas públicas de Route 53 deberían registrar las consultas de DNS
- [S3.24] Los puntos de Multi-Region acceso S3 deben tener habilitada la configuración de bloqueo del acceso público
- [WAF.1]AWS WAFEl registro de ACL web global clásico debe estar habilitado
- [WAF.6]AWS WAFLas reglas globales clásicas deben tener al menos una condición
- [WAF.7]AWS WAFLos grupos de reglas globales clásicos deben tener al menos una regla
- [WAF.8]AWS WAFLas ACL web globales clásicas deben tener al menos una regla o grupo de reglas

Canadá (centro)

Los siguientes controles no se admiten en la región Canadá (centro).

- [AppRunner.1] Los servicios de App Runner deben estar etiquetados
- [AppRunner.2] Los conectores VPC de App Runner deben estar etiquetados
- [AppSync.1]AWS AppSyncLas cachés de las API deben estar cifradas en reposo
- [AppSync.6]AWS AppSyncLas cachés de las API deben cifrarse en tránsito
- [BedrockAgentCore.3] Bedrock AgentCore Memory debe estar cifrada y gestionada por el clienteAWS KMSclaves
- [CloudFront.1] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado
- [CloudFront.3] CloudFront las distribuciones deben requerir el cifrado durante el tránsito
- [CloudFront.4] CloudFront las distribuciones deben tener configurada la conmutación por error de origen
- [CloudFront.5] CloudFront las distribuciones deben tener habilitado el registro
- [CloudFront.6] CloudFront las distribuciones deben tener WAF activado
- [CloudFront.7] CloudFront las distribuciones deben usar certificados personalizados SSL/TLS
- [CloudFront.8] CloudFront las distribuciones deben usar el SNI para atender las solicitudes HTTPS
- [CloudFront.9] CloudFront las distribuciones deben cifrar el tráfico para convertirlo en orígenes personalizados
- [CloudFront.10] CloudFront las distribuciones no deben usar protocolos SSL obsoletos entre ubicaciones de borde y orígenes personalizados
- [CloudFront.12] CloudFront las distribuciones no deben apuntar a orígenes de S3 inexistentes
- [CloudFront.13] CloudFront las distribuciones deben usar el control de acceso al origen
- [CloudFront.14] CloudFront las distribuciones deben estar etiquetadas
- [CloudFront.15] CloudFront las distribuciones deben usar la política de seguridad TLS recomendada
- [CloudFront.16] CloudFront las distribuciones deben usar el control de acceso de origen para los orígenes de las URL de las funciones de Lambda
- [CloudFront.17] CloudFront las distribuciones deben usar grupos de claves confiables para las URL y cookies firmadas
- [CodeArtifact.1] CodeArtifact los repositorios deben estar etiquetados
- [CodeGuruProfiler.1] Los grupos CodeGuru de creación de perfiles de Profiler deben estar etiquetados

- [CodeGuruReviewer.1] Las asociaciones de repositorios de CodeGuru Reviewer deben estar etiquetadas
- [DynamoDB.3] Los clústeres de DynamoDB Accelerator (DAX) deben cifrarse en reposo
- [DynamoDB.7] Los clústeres de DynamoDB Accelerator deben cifrarse en tránsito
- [EC2.24] No se deben utilizar los tipos de instancias paravirtuales de Amazon EC2
- [EC2.173] Las solicitudes de EC2 Spot Fleet con parámetros de lanzamiento deberían permitir el cifrado de los volúmenes de EBS adjuntos
- [ECR.4] Los repositorios públicos de ECR deben etiquetarse
- [FraudDetector.1] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.2] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas
- [FraudDetector.3] Los resultados de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.4] Las variables de Amazon Fraud Detector deben estar etiquetadas
- [GlobalAccelerator.1] Los aceleradores de Global Accelerator deben estar etiquetados
- [IAM.26] SSL/TLS Los certificados caducados gestionados en IAM deben eliminarse
- [Inspector.3] El escaneo de código Lambda de Amazon Inspector Lambda debe estar activado
- [IoTTwinMaker.1]AWSLos trabajos de TwinMaker sincronización de IoT deben estar etiquetados
- [IoTTwinMaker.2]AWS TwinMaker Los espacios de trabajo de IoT deben estar etiquetados
- [IoTTwinMaker.3]AWS TwinMaker Las escenas de IoT deben estar etiquetadas
- [IoTTwinMaker.4]AWS TwinMaker Las entidades de IoT deben estar etiquetadas
- [IoTWireless.1]AWSLos grupos de multidifusión de IoT Wireless deben estar etiquetados
- [IoTWireless.2]AWSLos perfiles de servicio de IoT Wireless deben estar etiquetados
- [IoTWireless.3]AWSLas tareas de IoT FUOTA deben estar etiquetadas
- [IVS.1] Los pares de teclas de reproducción IVS deben estar etiquetados
- [IVS.2] Las configuraciones de grabación de IVS deben estar etiquetadas
- [IVS.3] Los canales IVS deben estar etiquetados
- [Kinesis.3] Las transmisiones de Kinesis deben tener un período de retención de datos adecuado
- [RDS.31] Los grupos de seguridad de la base de datos de RDS deben etiquetarse
- [Route53.1] Los controles de salud de Route 53 deben estar etiquetados
- [Route53.2] Las zonas alojadas públicas de Route 53 deberían registrar las consultas de DNS

- [S3.24] Los puntos de Multi-Region acceso S3 deben tener habilitada la configuración de bloqueo del acceso público
- [S3.25] Los buckets de directorio de S3 deben tener configuraciones de ciclo de vida
- [SageMaker.19] SageMaker los modelos deben usar un registro privado en la VPC para las canalizaciones de inferencia de varios contenedores
- [WAF.1]AWS WAFEl registro de ACL web global clásico debe estar habilitado
- [WAF.6]AWS WAFLas reglas globales clásicas deben tener al menos una condición
- [WAF.7]AWS WAFLos grupos de reglas globales clásicos deben tener al menos una regla
- [WAF.8]AWS WAFLas ACL web globales clásicas deben tener al menos una regla o grupo de reglas

Oeste de Canadá (Calgary)

Los siguientes controles no se admiten en la región Oeste de Canadá (Calgary).

- [ACM.1] ACM-issued Los certificados importados y renovados deben renovarse después de un período de tiempo específico
- [ACM.2] Los certificados RSA gestionados por ACM deben utilizar una longitud de clave de al menos 2048 bits
- [Account.1] La información de contacto de seguridad debe proporcionarse para unCuenta de AWS
- [Account.2]Cuentas de AWSdebe formar parte de unAWS Organizationsorganización
- [APIGateway.8] Las rutas de API Gateway deben especificar un tipo de autorización
- [APIGateway.9] El registro de acceso debe configurarse para las etapas V2 de API Gateway
- [Amplify.1] Las aplicaciones Amplify deben estar etiquetadas
- [Amplify.2] Amplify branches debe estar etiquetado
- [AppConfig.1]AWS AppConfiglas aplicaciones deben estar etiquetadas
- [AppConfig.2]AWS AppConfiglos perfiles de configuración deben estar etiquetados
- [AppConfig.3]AWS AppConfiglos entornos deben estar etiquetados
- [AppConfig.4]AWS AppConfiglas asociaciones de extensiones deben estar etiquetadas
- [AppFlow.1] AppFlow Los flujos de Amazon deben estar etiquetados
- [AppRunner.1] Los servicios de App Runner deben estar etiquetados
- [AppRunner.2] Los conectores VPC de App Runner deben estar etiquetados

- [AppSync.1]AWS AppSyncLas cachés de las API deben estar cifradas en reposo
- [AppSync.2]AWS AppSyncdebe tener habilitado el registro a nivel de campo
- [AppSync.5]AWS AppSyncLas API de GraphQL no deben autenticarse con claves de API
- [AppSync.6]AWS AppSyncLas cachés de las API deben cifrarse en tránsito
- [Athena.4] Los grupos de trabajo de Athena deberían tener habilitado el registro
- [AutoScaling.2] El grupo Amazon EC2 Auto Scaling debe cubrir varias zonas de disponibilidad
- [AutoScaling.3] Las configuraciones de lanzamiento grupal de Auto Scaling deberían configurar las instancias EC2 para que requieran la versión 2 del Servicio de Metadatos de Instancia (IMDSv2)
- [AutoScaling.6] Los grupos de Auto Scaling deben usar varios tipos de instancias en múltiples zonas de disponibilidad
- [AutoScaling.9] Los grupos de Amazon EC2 Auto Scaling deben utilizar las plantillas de lanzamiento de Amazon EC2
- [Backup.1]AWS Backuplos puntos de recuperación deben estar cifrados en reposo
- [Backup.4]AWS Backuplos planes de informes deben estar etiquetados
- [Batch.1] Las colas de trabajos por lotes deben estar etiquetadas
- [Batch.3] Los entornos de procesamiento por lotes deben etiquetarse
- [Batch.4] Las propiedades de los recursos de cómputo en los entornos de cómputo por lotes gestionados deben estar etiquetadas
- [BedrockAgentCore.1] Los AgentCore tiempos de ejecución de Bedrock deben configurarse con el modo de red VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways debería requerir autorización para las solicitudes entrantes
- [BedrockAgentCore.3] Bedrock AgentCore Memory debe estar cifrada y gestionada por el clienteAWS KMSclaves
- [BedrockAgentCore.4] Bedrock AgentCore Gateway debe cifrarse de forma que sea gestionada por el clienteAWS KMSclaves
- [BedrockAgentCore.5] Los navegadores AgentCore personalizados de Bedrock no deberían usar el modo de red pública
- [BedrockAgentCore.6] Los navegadores AgentCore personalizados de Bedrock deberían tener habilitada la grabación de sesiones
- [CloudFormation.3] las CloudFormation pilas deben tener habilitada la protección de terminación

- [CloudFormation.4] las CloudFormation pilas deben tener funciones de servicio asociadas
- [CloudFront.1] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado
- [CloudFront.3] CloudFront las distribuciones deben requerir el cifrado durante el tránsito
- [CloudFront.4] CloudFront las distribuciones deben tener configurada la conmutación por error de origen
- [CloudFront.5] CloudFront las distribuciones deben tener habilitado el registro
- [CloudFront.6] CloudFront las distribuciones deben tener WAF activado
- [CloudFront.7] CloudFront las distribuciones deben usar certificados personalizados SSL/TLS
- [CloudFront.8] CloudFront las distribuciones deben usar el SNI para atender las solicitudes HTTPS
- [CloudFront.9] CloudFront las distribuciones deben cifrar el tráfico para convertirlo en orígenes personalizados
- [CloudFront.10] CloudFront las distribuciones no deben usar protocolos SSL obsoletos entre ubicaciones de borde y orígenes personalizados
- [CloudFront.12] CloudFront las distribuciones no deben apuntar a orígenes de S3 inexistentes
- [CloudFront.13] CloudFront las distribuciones deben usar el control de acceso al origen
- [CloudFront.14] CloudFront las distribuciones deben estar etiquetadas
- [CloudFront.15] CloudFront las distribuciones deben usar la política de seguridad TLS recomendada
- [CloudFront.16] CloudFront las distribuciones deben usar el control de acceso de origen para los orígenes de las URL de las funciones de Lambda
- [CloudFront.17] CloudFront las distribuciones deben usar grupos de claves confiables para las URL y cookies firmadas
- [CloudTrail.6] Asegúrese de que el depósito de S3 que se utiliza para almacenar CloudTrail los registros no sea de acceso público
- [CloudTrail.7] Asegúrese de que el registro de acceso al bucket de S3 esté habilitado en el CloudTrail bucket de S3
- [CloudTrail.10] Los almacenes de datos de eventos de CloudTrail Lake deben estar cifrados y gestionados por el clienteAWS KMS keys
- [CloudWatch.17] las acciones CloudWatch de alarma deben estar activadas
- [CodeArtifact.1] CodeArtifact los repositorios deben estar etiquetados

- [CodeBuild.1] Las URL del repositorio fuente de CodeBuild Bitbucket no deben contener credenciales confidenciales
- [CodeBuild.2] las variables de entorno CodeBuild del proyecto no deben contener credenciales de texto claro
- [CodeBuild.3] Los registros de CodeBuild S3 deben estar cifrados
- [CodeBuild.4] los entornos de CodeBuild proyectos deben tener un registroAWS ConfigDuración
- [CodeBuild.7] las exportaciones de grupos de CodeBuild informes deben cifrarse en reposo
- [CodeGuruProfiler.1] Los grupos CodeGuru de creación de perfiles de Profiler deben estar etiquetados
- [CodeGuruReviewer.1] Las asociaciones de repositorios de CodeGuru Reviewer deben estar etiquetadas
- [Cognito.1] Los grupos de usuarios de Cognito deben tener activada la protección contra amenazas y el modo de aplicación con todas las funciones para la autenticación estándar
- [Cognito.2] Los grupos de identidades de Cognito no deben permitir identidades no autenticadas
- [Connect.1] Los tipos de objetos de los perfiles de clientes de Amazon Connect deben estar etiquetados
- [Connect.2] Las instancias de Connect Customer deben tener el CloudWatch registro habilitado
- [DataFirehose.1] Los flujos de entrega de Firehose deben cifrarse en reposo
- [DataSync.1] DataSync las tareas deberían tener el registro activado
- [Detective.1] Los gráficos de comportamiento de los detectives deben estar etiquetados
- [DMS.2] Los certificados DMS deben estar etiquetados
- [DMS.3] Las suscripciones a eventos de DMS deben estar etiquetadas
- [DMS.4] Las instancias de replicación de DMS deben estar etiquetadas
- [DMS.5] Los grupos de subredes de replicación del DMS deben estar etiquetados
- [DMS.6] Las instancias de replicación de DMS deben tener habilitada la actualización automática de las versiones secundarias
- [DMS.7] Las tareas de replicación del DMS para la base de datos de destino deben tener el registro habilitado
- [DMS.8] Las tareas de replicación del DMS para la base de datos de origen deben tener el registro activado
- [DMS.9] Los puntos finales del DMS deben usar SSL

- [DMS.10] Los puntos finales de DMS para las bases de datos de Neptune deben tener habilitada la autorización de IAM
- [DMS.11] Los puntos finales de DMS para MongoDB deben tener un mecanismo de autenticación habilitado
- [DMS.12] Los puntos finales de DMS para Redis OSS deben tener el TLS habilitado
- [DMS.13] Las instancias de replicación de DMS deben configurarse para usar varias zonas de disponibilidad
- [DocumentDB.1] Los clústeres de Amazon DocumentDB deben cifrarse en reposo
- [DocumentDB.2] Los clústeres de Amazon DocumentDB deben tener un período de retención de copias de seguridad adecuado
- [DocumentDB.3] Las instantáneas de clústeres manuales de Amazon DocumentDB no deben ser públicas
- [DocumentDB.4] Los clústeres de Amazon DocumentDB deben publicar los registros de auditoría en Logs CloudWatch
- [DocumentDB.5] Los clústeres de Amazon DocumentDB deben tener habilitada la protección contra eliminaciones
- [DocumentDB.6] Los clústeres de Amazon DocumentDB deben cifrarse en tránsito
- [DynamoDB.3] Los clústeres de DynamoDB Accelerator (DAX) deben cifrarse en reposo
- [DynamoDB.4] Las tablas de DynamoDB deben estar presentes en un plan de respaldo
- [DynamoDB.6] Las tablas de DynamoDB deben tener habilitada la protección de eliminación
- [DynamoDB.7] Los clústeres de DynamoDB Accelerator deben cifrarse en tránsito
- [EC2.4] Las instancias EC2 detenidas deben eliminarse después de un período de tiempo específico
- [EC2.21] Las ACL de red no deberían permitir la entrada desde la versión 0.0.0. 0/0 al puerto 22 o al puerto 3389
- [EC2.22] Deben eliminarse los grupos de seguridad de Amazon EC2 no utilizados
- [EC2.23] Amazon EC2 Transit Gateways no debe aceptar automáticamente las solicitudes de adjuntos de VPC
- [EC2.24] No se deben utilizar los tipos de instancias paravirtuales de Amazon EC2
- [EC2.25] Las plantillas de lanzamiento de Amazon EC2 no deben asignar direcciones IP públicas a las interfaces de red

- [EC2.28] Los volúmenes de EBS deben estar cubiertos por un plan de respaldo
- [EC2.34] Las tablas de rutas de la pasarela de tránsito EC2 deben estar etiquetadas
- [EC2.40] Las pasarelas NAT EC2 deben estar etiquetadas
- [EC2.51] Los puntos finales EC2 Client VPN deben tener habilitado el registro de conexiones de clientes
- [EC2.53] Los grupos de seguridad de EC2 no deberían permitir la entrada desde la versión 0.0.0.0/0 a los puertos de administración remota del servidor
- [EC2.54] Los grupos de seguridad de EC2 no deberían permitir la entrada desde: :/0 a los puertos de administración remota del servidor
- [EC2.55] Las VPC deben configurarse con un punto final de interfaz para la API de ECR
- [EC2.56] Las VPC deben configurarse con un punto final de interfaz para Docker Registry
- [EC2.57] Las VPC deben configurarse con un punto final de interfaz para Systems Manager
- [EC2.58] Las VPC deben configurarse con un punto final de interfaz para los contactos de Systems Manager Incident Manager
- [EC2.60] Las VPC deben configurarse con un punto final de interfaz para Systems Manager Incident Manager
- [EC2.170] Las plantillas de lanzamiento de EC2 deben utilizar la versión 2 del servicio de metadatos de instancias (IMDSv2)
- [EC2.171] Las conexiones VPN de EC2 deberían tener el registro habilitado
- [EC2.173] Las solicitudes de EC2 Spot Fleet con parámetros de lanzamiento deberían permitir el cifrado de los volúmenes de EBS adjuntos
- [EC2.175] Las plantillas de lanzamiento de EC2 deben estar etiquetadas
- [EC2.177] Las sesiones de réplica de tráfico de EC2 deben etiquetarse
- [EC2.179] Los objetivos del espejo de tráfico de EC2 deben estar etiquetados
- [EC2.180] Las interfaces de red EC2 deberían tener habilitada source/destination la verificación
- [EC2.181] Las plantillas de lanzamiento de EC2 deberían permitir el cifrado de los volúmenes de EBS adjuntos
- [EC2.183] Las conexiones VPN de EC2 deben utilizar el protocolo IKEv2
- [ECR.1] Los repositorios privados de ECR deben tener configurado el escaneo de imágenes
- [ECR.2] Los repositorios privados de ECR deben tener configurada la inmutabilidad de etiquetas

- [ECR.3] Los repositorios de ECR deben tener configurada al menos una política de ciclo de vida
- [ECR.4] Los repositorios públicos de ECR deben etiquetarse
- [ECR.5] Los repositorios de ECR deben estar cifrados y ser gestionados por el cliente AWS KMS keys
- [ECS.3] Las definiciones de tareas de ECS no deben compartir el espacio de nombres del proceso del host
- [ECS.4] Los contenedores ECS deben ejecutarse sin privilegios
- [ECS.5] Las definiciones de tareas de ECS deben configurar los contenedores para que se limiten al acceso de solo lectura a los sistemas de archivos raíz
- [ECS.8] Los secretos no deben transmitirse como variables de entorno de contenedores
- [ECS.9] Las definiciones de tareas de ECS deben tener una configuración de registro
- [ECS.10] Los servicios Fargate de ECS deberían ejecutarse en la última versión de la plataforma Fargate
- [ECS.12] Los clústeres de ECS deben usar Container Insights
- [ECS.16] Los conjuntos de tareas de ECS no deben asignar automáticamente direcciones IP públicas
- [ECS.17] Las definiciones de tareas de ECS no deben usar el modo de red host
- [EFS.1] Elastic File System debe configurarse para cifrar los datos de los archivos en reposo mediante AWS KMS
- [EFS.2] Los volúmenes de Amazon EFS deben figurar en los planes de copia de seguridad
- [EFS.3] Los puntos de acceso EFS deben exigir un directorio raíz
- [EFS.4] Los puntos de acceso EFS deben exigir la identidad del usuario
- [EFS.6] Los destinos de montaje de EFS no deben asociarse a subredes que asignan direcciones IP públicas en el momento del lanzamiento
- [] Los sistemas de archivos EFS deben tener habilitadas las copias de seguridad automáticas EFS.7
- [EFS.8] Los sistemas de archivos EFS deben cifrarse en reposo
- [EKS.2] Los clústeres de EKS deben ejecutarse en una versión de Kubernetes compatible
- [EKS.3] Los clústeres de EKS deben usar secretos de Kubernetes cifrados
- [EKS.7] Las configuraciones del proveedor de identidad de EKS deben etiquetarse

- [EKS.8] Los clústeres de EKS deben tener habilitado el registro de auditoría
- [ELB.2] Los balanceadores de carga clásicos con SSL/HTTPS oyentes deben usar un certificado proporcionado por AWS Gestor de certificados
- [ELB.10] El balanceador de carga clásico debe abarcar varias zonas de disponibilidad
- [ELB.12] El balanceador de carga de aplicaciones debe configurarse con el modo defensivo o de mitigación de desincronización más estricto
- [ELB.13] Los balanceadores de carga de aplicaciones, redes y puertas de enlace deben abarcar varias zonas de disponibilidad
- [ELB.14] El balanceador de carga clásico debe configurarse con el modo defensivo o de mitigación de desincronización más estricto
- [ELB.17] Los balanceadores de cargas de aplicaciones y redes con oyentes deben usar las políticas de seguridad recomendadas
- [ELB.18] Los oyentes del balanceador de cargas de red y aplicaciones deben usar protocolos seguros para cifrar los datos en tránsito
- [ElastiCache.1] ElastiCache (Redis OSS) los clústeres deben tener habilitadas las copias de seguridad automáticas
- [ElastiCache.2] ElastiCache los clústeres deberían tener habilitadas las actualizaciones automáticas de las versiones secundarias
- [ElastiCache.3] los grupos de ElastiCache replicación deberían tener habilitada la conmutación por error automática
- [ElastiCache.4] los grupos de ElastiCache replicación deben cifrarse en reposo
- [ElastiCache.5] los grupos de ElastiCache replicación deben cifrarse en tránsito
- [ElastiCache.6] ElastiCache (Redis OSS) Los grupos de replicación de versiones anteriores deberían tener habilitada la autenticación de Redis OSS
- [ElastiCache.7] los ElastiCache clústeres no deben usar el grupo de subredes predeterminado
- [ElasticBeanstalk.1] Los entornos de Elastic Beanstalk deberían tener habilitados los informes de estado mejorados
- [ElasticBeanstalk.2] Las actualizaciones de la plataforma gestionada de Elastic Beanstalk deben estar habilitadas
- [ElasticBeanstalk.3] Elastic Beanstalk debería transmitir los registros a CloudWatch
- [EMR.1] Los nodos principales del clúster de Amazon EMR no deben tener direcciones IP públicas

- [EMR.2] La configuración de acceso público del bloque Amazon EMR debe estar habilitada
- [ES.4] Debería estar habilitado el registro de errores de dominio de Elasticsearch en Logs CloudWatch
- [EventBridge.3] los autobuses de eventos EventBridge personalizados deben tener adjunta una política basada en los recursos
- [EventBridge.4] los puntos finales EventBridge globales deberían tener habilitada la replicación de eventos
- [FraudDetector.1] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.2] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas
- [FraudDetector.3] Los resultados de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.4] Las variables de Amazon Fraud Detector deben estar etiquetadas
- [FSx.1] FSx para sistemas de archivos OpenZFS debe configurarse para copiar etiquetas en copias de seguridad y volúmenes
- [FSx.2] Los sistemas de archivos FSx for Lustre deben configurarse para copiar etiquetas a las copias de seguridad
- [FSx.3] FSx para sistemas de archivos OpenZFS debe configurarse para su implementación Multi-AZ
- [FSx.4] FSx para sistemas de archivos NetApp ONTAP debe configurarse para su implementación Multi-AZ
- [FSx.5] Los sistemas de archivos FSx for Windows File Server deben configurarse para Multi-AZ su implementación
- [GlobalAccelerator.1] Los aceleradores de Global Accelerator deben estar etiquetados
- [Glue.3]AWS GlueLas transformaciones de aprendizaje automático deben cifrarse en reposo
- [Glue.4]AWS GlueLos trabajos de Spark deberían ejecutarse en versiones compatibles deAWS Glue
- GuardDuty Los filtros [GuardDuty.2] deben estar etiquetados
- [GuardDuty.5] La monitorización del registro de auditoría de GuardDuty EKS debe estar habilitada
- [GuardDuty.6] GuardDuty La protección Lambda debe estar habilitada
- [GuardDuty.7] La monitorización del tiempo de ejecución de GuardDuty EKS debe estar habilitada
- [GuardDuty.8] La protección contra GuardDuty malware para EC2 debe estar habilitada
- [GuardDuty.9] La protección GuardDuty RDS debe estar habilitada

- [GuardDuty.10] La protección GuardDuty S3 debe estar habilitada
- [GuardDuty.11] La monitorización del GuardDuty tiempo de ejecución debe estar habilitada
- [GuardDuty.12] La monitorización del tiempo de ejecución de GuardDuty ECS debe estar habilitada
- [GuardDuty.13] La monitorización del tiempo de ejecución de GuardDuty EC2 debe estar habilitada
- [IAM.1] Las políticas de IAM no deberían permitir todos los privilegios administrativos «*»
- [IAM.2] Los usuarios de IAM no deberían tener políticas de IAM adjuntas
- [IAM.3] Las claves de acceso de los usuarios de IAM deben rotarse cada 90 días o menos
- [IAM.4] La clave de acceso del usuario raíz de IAM no debería existir
- [IAM.5] La MFA debe estar habilitada para todos los usuarios de IAM que tengan una contraseña de consola
- [IAM.6] La MFA de hardware debe estar habilitada para el usuario root
- [IAM.7] Las políticas de contraseñas para los usuarios de IAM deben tener configuraciones sólidas
- [IAM.8] Se deben eliminar las credenciales de usuario de IAM no utilizadas
- [IAM.9] La MFA debe estar habilitada para el usuario root
- [IAM.10] Las políticas de contraseñas para los usuarios de IAM deben tener configuraciones sólidas
- [IAM.11] Asegúrese de que la política de contraseñas de IAM requiera al menos una letra mayúscula
- [IAM.12] Asegúrese de que la política de contraseñas de IAM requiera al menos una letra minúscula
- [IAM.13] Asegúrese de que la política de contraseñas de IAM requiera al menos un símbolo
- [IAM.14] Asegúrese de que la política de contraseñas de IAM requiera al menos un número
- [IAM.15] Asegúrese de que la política de contraseñas de IAM exija una longitud de contraseña mínima de 14 o más
- [IAM.16] Asegúrese de que la política de contraseñas de IAM impida la reutilización de contraseñas
- [IAM.17] Asegúrese de que la política de contraseñas de IAM haga caducar las contraseñas en un plazo de 90 días o menos
- [IAM.18] Asegúrese de que se haya creado una función de soporte para gestionar los incidentes conAWS Support

- [IAM.19] La MFA debe estar habilitada para todos los usuarios de IAM
- [IAM.21] Las políticas de IAM gestionadas por el cliente que cree no deberían permitir acciones comodín en los servicios
- [IAM.22] Se deben eliminar las credenciales de usuario de IAM que no se hayan utilizado durante 45 días
- [IAM.24] Las funciones de IAM deben estar etiquetadas
- [IAM.25] Los usuarios de IAM deben estar etiquetados
- [IAM.26] SSL/TLS Los certificados caducados gestionados en IAM deben eliminarse
- [IAM.27] Las identidades de IAM no deberían tener la AWSCloudShellFullAccess política adjunta
- [IAM.28] El analizador de acceso externo de IAM Access Analyzer debe estar habilitado
- [Inspector.1] El escaneo EC2 de Amazon Inspector debe estar activado
- [Inspector.2] El escaneo ECR de Amazon Inspector debe estar activado
- [Inspector.3] El escaneo de código Lambda de Amazon Inspector Lambda debe estar activado
- [Inspector.4] El escaneo estándar de Amazon Inspector Lambda debe estar activado
- [IoT.1]AWS IoT Device Defenderlos perfiles de seguridad deben estar etiquetados
- [IoT.2]AWS IoT Corelas acciones de mitigación deben estar etiquetadas
- [IoT.3]AWS IoT Corelas dimensiones deben estar etiquetadas
- [IoT.4]AWS IoT Corelos autorizadores deben estar etiquetados
- [IoT.5]AWS IoT CoreLos alias de los roles deben estar etiquetados
- [IoT.6]AWS IoT Corelas políticas deben estar etiquetadas
- [IoTSiteWise.1]AWSLos modelos SiteWise de activos de IoT deben estar etiquetados
- [IoTSiteWise.2]AWS SiteWise Los paneles de IoT deben estar etiquetados
- [IoTSiteWise.3]AWS SiteWise Las pasarelas de IoT deben estar etiquetadas
- [IoTSiteWise.4]AWS SiteWise Los portales de IoT deben estar etiquetados
- [IoTSiteWise.5]AWS SiteWise Los proyectos de IoT deben estar etiquetados
- [IoTTwinMaker.1]AWSLos trabajos de TwinMaker sincronización de IoT deben estar etiquetados
- [IoTTwinMaker.2]AWS TwinMaker Los espacios de trabajo de IoT deben estar etiquetados
- [IoTTwinMaker.3]AWS TwinMaker Las escenas de IoT deben estar etiquetadas
- [IoTTwinMaker.4]AWS TwinMaker Las entidades de IoT deben estar etiquetadas

- [IoTWireless.1]AWSLos grupos de multidifusión de IoT Wireless deben estar etiquetados
- [IoTWireless.2]AWSLos perfiles de servicio de IoT Wireless deben estar etiquetados
- [IoTWireless.3]AWSLas tareas de IoT FUOTA deben estar etiquetadas
- [IVS.1] Los pares de teclas de reproducción IVS deben estar etiquetados
- [IVS.2] Las configuraciones de grabación de IVS deben estar etiquetadas
- [IVS.3] Los canales IVS deben estar etiquetados
- [Keyspaces.1] Los espacios clave de Amazon Keyspaces deben estar etiquetados
- [Kinesis.1] Las transmisiones de Kinesis deben cifrarse en reposo
- [Kinesis.3] Las transmisiones de Kinesis deben tener un período de retención de datos adecuado
- [KMS.1] Las políticas gestionadas por los clientes de IAM no deberían permitir acciones de descifrado en todas las claves de KMS
- [KMS.2] Los directores de IAM no deberían tener políticas integradas de IAM que permitan realizar acciones de descifrado en todas las claves de KMS
- [KMS.5] Las claves KMS no deben ser de acceso público
- [Lambda.5] Las funciones de VPC Lambda deben funcionar en varias zonas de disponibilidad
- [Lambda.7] Las funciones de Lambda deberían tener AWS X-Ray el rastreo activo está habilitado
- [Macie.1] Amazon Macie debería estar activado
- [Macie.2] La detección automática de datos confidenciales por parte de Macie debería estar habilitada
- [MQ.2] Los corredores de ActiveMQ deben transmitir los registros de auditoría a CloudWatch
- [MQ.4] Los corredores de Amazon MQ deben estar etiquetados
- [MQ.5] Los corredores de ActiveMQ deberían usar el modo de implementación active/standby
- [MQ.6] Los corredores de RabbitMQ deberían usar el modo de despliegue de clústeres
- [MSK.1] Los clústeres de MSK deben cifrarse en tránsito entre los nodos de intermediación
- [MSK.2] Los clústeres de MSK deberían tener configurada una supervisión mejorada
- [MSK.3] Los conectores MSK Connect deben estar cifrados en tránsito
- [MSK.4] Los clústeres de MSK deben tener el acceso público deshabilitado
- [MSK.5] Los conectores MSK deben tener el registro activado
- [MSK.6] Los clústeres de MSK deberían deshabilitar el acceso no autenticado

- [Neptune.1] Los clústeres de bases de datos de Neptune deben cifrarse en reposo
- [Neptune.2] Los clústeres de bases de datos de Neptune deberían publicar registros de auditoría en Logs CloudWatch
- [Neptune.3] Las instantáneas del clúster de base de datos de Neptune no deben ser públicas
- [Neptune.4] Los clústeres de base de datos de Neptune deben tener habilitada la protección contra eliminación
- [Neptune.5] Los clústeres de Neptune DB deberían tener habilitadas las copias de seguridad automatizadas
- [Neptune.6] Las instantáneas del clúster de base de datos de Neptune deben cifrarse en reposo
- [Neptune.7] Los clústeres de base de datos de Neptune deben tener habilitada la autenticación de bases de datos de IAM
- [Neptune.8] Los clústeres de bases de datos de Neptune deben configurarse para copiar etiquetas a las instantáneas
- [Neptune.9] Los clústeres de base de datos Neptune deben implementarse en varias zonas de disponibilidad
- [NetworkFirewall.1] Los firewalls de Network Firewall deben implementarse en varias zonas de disponibilidad
- [NetworkFirewall.2] El registro de Network Firewall debe estar habilitado
- [NetworkFirewall.3] Las políticas de Network Firewall deben tener asociado al menos un grupo de reglas
- [NetworkFirewall.4] La acción sin estado predeterminada para las políticas de Network Firewall debe ser eliminar o reenviar paquetes completos
- [NetworkFirewall.5] La acción sin estado predeterminada para las políticas de Network Firewall debe ser eliminar o reenviar paquetes fragmentados
- [NetworkFirewall.6] El grupo de reglas de Stateless Network Firewall no debe estar vacío
- [NetworkFirewall.9] Los firewalls de Network Firewall deben tener habilitada la protección de eliminación
- [NetworkFirewall.10] Los firewalls de Network Firewall deben tener habilitada la protección contra cambios de subred
- [Opensearch.1] OpenSearch los dominios deben tener activado el cifrado en reposo
- [Opensearch.2] OpenSearch los dominios no deben ser de acceso público
- [Opensearch.3] OpenSearch los dominios deben cifrar los datos enviados entre nodos

- [Opensearch.4] El registro de errores de OpenSearch dominio en Logs debe estar habilitado CloudWatch
- [Opensearch.5] OpenSearch los dominios deben tener activado el registro de auditoría
- [Opensearch.6] OpenSearch los dominios deben tener al menos tres nodos de datos
- [Opensearch.7] OpenSearch los dominios deben tener habilitado un control de acceso detallado
- [Opensearch.8] Las conexiones a los OpenSearch dominios deben cifrarse con la última política de seguridad de TLS
- [Opensearch.9] OpenSearch los dominios deben estar etiquetados
- [Opensearch.10] OpenSearch los dominios deben tener instalada la última actualización de software
- [Opensearch.11] OpenSearch los dominios deben tener al menos tres nodos principales dedicados
- [PCA.1]AWS Privada CALa autoridad emisora de certificados raíz debe estar deshabilitada
- [RDS.14] Los clústeres de Amazon Aurora deben tener habilitado el retroceso
- [RDS.24] Los clústeres de bases de datos de RDS deben usar un nombre de usuario de administrador personalizado
- [RDS.25] Las instancias de bases de datos de RDS deben usar un nombre de usuario de administrador personalizado
- [RDS.26] Las instancias de base de datos de RDS deben protegerse mediante un plan de respaldo
- [RDS.27] Los clústeres de bases de datos de RDS deben cifrarse en reposo
- [RDS.31] Los grupos de seguridad de la base de datos de RDS deben etiquetarse
- [RDS.34] Los clústeres de bases de datos Aurora MySQL deben publicar los registros de auditoría en Logs CloudWatch
- [RDS.35] Los clústeres de bases de datos de RDS deben tener habilitada la actualización automática de versiones secundarias
- [RDS.36] Las instancias de base de datos de RDS para PostgreSQL deben publicar los registros en Logs CloudWatch
- [RDS.37] Los clústeres de bases de datos de Aurora PostgreSQL deben publicar los registros en Logs CloudWatch
- [RDS.38] Las instancias de base de datos de RDS para PostgreSQL deben cifrarse en tránsito
- [RDS.39] Las instancias de base de datos de RDS para MySQL deben cifrarse en tránsito
- [RDS.40] Las instancias de base de datos de RDS para SQL Server deben publicar los registros en Logs CloudWatch

- [RDS.41] Las instancias de base de datos de RDS para SQL Server deben cifrarse en tránsito
- [RDS.42] Las instancias de base de datos de RDS para MariaDB deben publicar los registros en Logs CloudWatch
- [RDS.43] Los proxies de bases de datos de RDS deben requerir el cifrado TLS para las conexiones
- [RDS.44] Las instancias de base de datos de RDS para MariaDB deben cifrarse durante el tránsito
- [RDS.45] Los clústeres de bases de datos Aurora MySQL deben tener habilitado el registro de auditoría
- [RDS.46] Las instancias de base de datos de RDS no deben implementarse en subredes públicas con rutas a pasarelas de Internet
- [RDS.51] Los clústeres globales de RDS deben ejecutarse en una versión compatible de Aurora MySQL
- [Redshift.8] Los clústeres de Amazon Redshift no deben usar el nombre de usuario de administrador predeterminado
- [Redshift.10] Los clústeres de Redshift deben cifrarse en reposo
- [Redshift.15] Los grupos de seguridad de Redshift deberían permitir la entrada en el puerto del clúster solo desde orígenes restringidos
- [Redshift.16] Los grupos de subredes de clústeres de Redshift deben tener subredes de varias zonas de disponibilidad
- [Redshift.18] Los clústeres de Redshift deberían tener Multi-AZ las implementaciones habilitadas
- [RedshiftServerless.1] Los grupos de trabajo sin servidor de Amazon Redshift deberían utilizar un enrutamiento de VPC mejorado
- [RedshiftServerless.2] Las conexiones a los grupos de trabajo sin servidor de Redshift deberían ser obligatorias para usar SSL
- [RedshiftServerless.3] Los grupos de trabajo sin servidor de Redshift deberían prohibir el acceso público
- [RedshiftServerless.4] Los espacios de nombres de Redshift Serverless deben cifrarse y administrarse por el clienteAWS KMS keys
- [RedshiftServerless.5] Los espacios de nombres Redshift Serverless no deben usar el nombre de usuario de administrador predeterminado
- [RedshiftServerless.6] Los espacios de nombres Redshift Serverless deberían exportar los registros a los registros CloudWatch

- [Route53.1] Los controles de salud de Route 53 deben estar etiquetados
- [Route53.2] Las zonas alojadas públicas de Route 53 deberían registrar las consultas de DNS
- [S3.7] Los cubos de uso general de S3 deben utilizar la replicación entre regiones
- [S3.10] Los cubos de uso general de S3 con el control de versiones habilitado deben tener configuraciones de ciclo de vida
- [S3.11] Los cubos de uso general de S3 deben tener habilitadas las notificaciones de eventos
- [S3.12] Las ACL no deben usarse para administrar el acceso de los usuarios a los cubos de uso general de S3
- [S3.13] Los cubos de uso general de S3 deben tener configuraciones de ciclo de vida
- [S3.19] Los puntos de acceso S3 deben tener habilitada la configuración de bloqueo de acceso público
- [S3.20] Los cubos de uso general de S3 deben tener habilitada la eliminación de MFA
- [S3.22] Los cubos de uso general de S3 deben registrar los eventos de escritura a nivel de objeto
- [S3.23] Los cubos de uso general de S3 deben registrar los eventos de lectura a nivel de objeto
- [S3.24] Los puntos de Multi-Region acceso S3 deben tener habilitada la configuración de bloqueo del acceso público
- [S3.25] Los buckets de directorio de S3 deben tener configuraciones de ciclo de vida
- [SageMaker.1] Las instancias de Amazon SageMaker Notebook no deberían tener acceso directo a Internet
- [SageMaker.2] las instancias de SageMaker cuadernos deben lanzarse en una VPC personalizada
- [SageMaker.3] Los usuarios no deben tener acceso root a las instancias de los SageMaker cuadernos
- [SageMaker.4] Las variantes de producción de SageMaker terminales deben tener un recuento inicial de instancias superior a 1
- SageMaker Los modelos [SageMaker.5] deben tener habilitado el aislamiento de red
- [SageMaker.6] las configuraciones de imagen de la SageMaker aplicación deben estar etiquetadas
- [SageMaker.7] SageMaker las imágenes deben estar etiquetadas
- [SageMaker.8] las instancias de SageMaker notebooks deben ejecutarse en plataformas compatibles
- [SageMaker.9] las definiciones de trabajos de calidad de los SageMaker datos deben tener habilitado el cifrado del tráfico entre contenedores

- [SageMaker.10] Las definiciones de trabajos de explicabilidad del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores
- [SageMaker.11] las definiciones de trabajos SageMaker de calidad de los datos deben tener habilitado el aislamiento de red
- [SageMaker.12] las definiciones de trabajo basadas en el sesgo del SageMaker modelo deben tener habilitado el aislamiento de red
- [SageMaker.13] las definiciones de trabajos de calidad del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores
- [SageMaker.14] los programas SageMaker de monitoreo deben tener habilitado el aislamiento de la red
- [SageMaker.15] Las definiciones de trabajo basadas en el sesgo del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores
- SageMaker Los modelos [SageMaker.16] deben usar un registro privado en la VPC para los contenedores principales
- [SageMaker.17] SageMaker Las tiendas offline de los grupos de funciones deben cifrarse con AWS KMS claves
- [SageMaker.18] las tiendas en línea de grupos de SageMaker funciones con almacenamiento estándar deben cifrarse con AWS KMS claves
- [SageMaker.19] SageMaker los modelos deben usar un registro privado en la VPC para las canalizaciones de inferencia de varios contenedores
- [SES.3] Los conjuntos de configuración de SES deben tener el TLS habilitado para enviar correos electrónicos
- [ServiceCatalog.1] Las carteras de Service Catalog deben compartirse dentro de unAWSsolo una organización
- [SNS.4] Las políticas de acceso a los temas de SNS no deberían permitir el acceso público
- [SQS.1] Las colas de Amazon SQS deben cifrarse en reposo
- [SQS.2] Las colas de SQS deben estar etiquetadas
- [SQS.3] Las políticas de acceso a las colas de SQS no deberían permitir el acceso público
- [SSM.4] Los documentos SSM no deben ser públicos
- [SSM.6] SSM Automation debería tener el registro habilitado CloudWatch
- [SSM.7] Los documentos SSM deben tener habilitada la configuración de bloqueo para compartir en público

- [StepFunctions.1] Step Functions indica que las máquinas deben tener el registro activado
- [Transfer.2] Los servidores Transfer Family no deben usar el protocolo FTP para la conexión de puntos finales
- [Transfer.3] Los conectores Transfer Family deben tener habilitado el registro
- [Transfer.4] Los acuerdos Transfer Family deben estar etiquetados
- [WAF.1]AWS WAFEl registro de ACL web global clásico debe estar habilitado
- [WAF.2]AWS WAFLas reglas regionales clásicas deben tener al menos una condición
- [WAF.3]AWS WAFLos grupos de reglas regionales clásicos deben tener al menos una regla
- [WAF.4]AWS WAFLas ACL web regionales clásicas deben tener al menos una regla o grupo de reglas
- [WAF.6]AWS WAFLas reglas globales clásicas deben tener al menos una condición
- [WAF.7]AWS WAFLos grupos de reglas globales clásicos deben tener al menos una regla
- [WAF.8]AWS WAFLas ACL web globales clásicas deben tener al menos una regla o grupo de reglas
- [WAF.10]AWS WAFLas ACL web deben tener al menos una regla o grupo de reglas
- [WAF.12]AWS WAFlas reglas deben tener CloudWatch las métricas habilitadas
- [WorkSpaces.1] los volúmenes de WorkSpaces usuarios deben cifrarse en reposo
- [WorkSpaces.2] los volúmenes WorkSpaces raíz deben cifrarse en reposo

China (Pekín)

Los siguientes controles no se admiten en la región China (Pekín).

- [ACM.1] ACM-issued Los certificados importados y renovados deben renovarse después de un período de tiempo específico
- [ACM.2] Los certificados RSA gestionados por ACM deben utilizar una longitud de clave de al menos 2048 bits
- [Account.2]Cuentas de AWSdebe formar parte de unAWS Organizationsorganización
- [APIGateway.2] Las etapas de la API REST de API Gateway deben configurarse para usar certificados SSL para la autenticación de backend
- [APIGateway.10] Las integraciones de API Gateway V2 deben usar HTTPS para las conexiones privadas

- [APIGateway.11] Los nombres de dominio de API Gateway deben usar las políticas de seguridad recomendadas
- [Amplify.1] Las aplicaciones Amplify deben estar etiquetadas
- [Amplify.2] Amplify branches debe estar etiquetado
- [AppConfig.1]AWS AppConfiglas aplicaciones deben estar etiquetadas
- [AppConfig.2]AWS AppConfiglos perfiles de configuración deben estar etiquetados
- [AppConfig.3]AWS AppConfiglos entornos deben estar etiquetados
- [AppConfig.4]AWS AppConfiglas asociaciones de extensiones deben estar etiquetadas
- [AppFlow.1] AppFlow Los flujos de Amazon deben estar etiquetados
- [AppRunner.1] Los servicios de App Runner deben estar etiquetados
- [AppRunner.2] Los conectores VPC de App Runner deben estar etiquetados
- [AppSync.1]AWS AppSyncLas cachés de las API deben estar cifradas en reposo
- [AppSync.6]AWS AppSyncLas cachés de las API deben cifrarse en tránsito
- [Backup.1]AWS Backuplos puntos de recuperación deben estar cifrados en reposo
- [Backup.4]AWS Backuplos planes de informes deben estar etiquetados
- [Batch.1] Las colas de trabajos por lotes deben estar etiquetadas
- [Batch.2] Las políticas de programación de lotes deben estar etiquetadas
- [Batch.3] Los entornos de procesamiento por lotes deben etiquetarse
- [Batch.4] Las propiedades de los recursos de cómputo en los entornos de cómputo por lotes gestionados deben estar etiquetadas
- [BedrockAgentCore.1] Los AgentCore tiempos de ejecución de Bedrock deben configurarse con el modo de red VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways debería requerir autorización para las solicitudes entrantes
- [BedrockAgentCore.3] Bedrock AgentCore Memory debe estar cifrada y gestionada por el clienteAWS KMSclaves
- [BedrockAgentCore.4] Bedrock AgentCore Gateway debe cifrarse de forma que sea gestionada por el clienteAWS KMSclaves
- [BedrockAgentCore.5] Los navegadores AgentCore personalizados de Bedrock no deberían usar el modo de red pública

- [BedrockAgentCore.6] Los navegadores AgentCore personalizados de Bedrock deberían tener habilitada la grabación de sesiones
- [CloudFront.1] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado
- [CloudFront.3] CloudFront las distribuciones deben requerir el cifrado durante el tránsito
- [CloudFront.4] CloudFront las distribuciones deben tener configurada la conmutación por error de origen
- [CloudFront.5] CloudFront las distribuciones deben tener habilitado el registro
- [CloudFront.6] CloudFront las distribuciones deben tener WAF activado
- [CloudFront.7] CloudFront las distribuciones deben usar certificados personalizados SSL/TLS
- [CloudFront.8] CloudFront las distribuciones deben usar el SNI para atender las solicitudes HTTPS
- [CloudFront.9] CloudFront las distribuciones deben cifrar el tráfico para convertirlo en orígenes personalizados
- [CloudFront.10] CloudFront las distribuciones no deben usar protocolos SSL obsoletos entre ubicaciones de borde y orígenes personalizados
- [CloudFront.13] CloudFront las distribuciones deben usar el control de acceso al origen
- [CloudFront.14] CloudFront las distribuciones deben estar etiquetadas
- [CloudFront.15] CloudFront las distribuciones deben usar la política de seguridad TLS recomendada
- [CloudFront.16] CloudFront las distribuciones deben usar el control de acceso de origen para los orígenes de las URL de las funciones de Lambda
- [CloudFront.17] CloudFront las distribuciones deben usar grupos de claves confiables para las URL y cookies firmadas
- [CloudTrail.10] Los almacenes de datos de eventos de CloudTrail Lake deben estar cifrados y gestionados por el clienteAWS KMS keys
- [CodeArtifact.1] CodeArtifact los repositorios deben estar etiquetados
- [CodeGuruProfiler.1] Los grupos CodeGuru de creación de perfiles de Profiler deben estar etiquetados
- [CodeGuruReviewer.1] Las asociaciones de repositorios de CodeGuru Reviewer deben estar etiquetadas
- [Cognito.1] Los grupos de usuarios de Cognito deben tener activada la protección contra amenazas y el modo de aplicación con todas las funciones para la autenticación estándar

- [Cognito.2] Los grupos de identidades de Cognito no deben permitir identidades no autenticadas
- [Cognito.3] Las políticas de contraseñas para los grupos de usuarios de Cognito deben tener configuraciones sólidas
- [Cognito.4] Los grupos de usuarios de Cognito deben tener activada la protección contra amenazas y el modo de aplicación con todas las funciones para la autenticación personalizada
- [Cognito.5] La MFA debe estar habilitada para los grupos de usuarios de Cognito
- [Cognito.6] Los grupos de usuarios de Cognito deben tener habilitada la protección contra la eliminación
- [Connect.1] Los tipos de objetos de los perfiles de clientes de Amazon Connect deben estar etiquetados
- [Connect.2] Las instancias de Connect Customer deben tener el CloudWatch registro habilitado
- [DataFirehose.1] Los flujos de entrega de Firehose deben cifrarse en reposo
- [DataSync.2] DataSync las tareas deben estar etiquetadas
- [Detective.1] Los gráficos de comportamiento de los detectives deben estar etiquetados
- [DMS.10] Los puntos finales de DMS para las bases de datos de Neptune deben tener habilitada la autorización de IAM
- [DMS.11] Los puntos finales de DMS para MongoDB deben tener un mecanismo de autenticación habilitado
- [DMS.12] Los puntos finales de DMS para Redis OSS deben tener el TLS habilitado
- [DocumentDB.1] Los clústeres de Amazon DocumentDB deben cifrarse en reposo
- [DocumentDB.2] Los clústeres de Amazon DocumentDB deben tener un período de retención de copias de seguridad adecuado
- [DocumentDB.3] Las instantáneas de clústeres manuales de Amazon DocumentDB no deben ser públicas
- [DocumentDB.4] Los clústeres de Amazon DocumentDB deben publicar los registros de auditoría en Logs CloudWatch
- [DocumentDB.5] Los clústeres de Amazon DocumentDB deben tener habilitada la protección contra eliminaciones
- [DynamoDB.3] Los clústeres de DynamoDB Accelerator (DAX) deben cifrarse en reposo
- [DynamoDB.4] Las tablas de DynamoDB deben estar presentes en un plan de respaldo
- [DynamoDB.7] Los clústeres de DynamoDB Accelerator deben cifrarse en tránsito

- [EC2.20] Ambos túneles VPN para un AWS Site-to-Site La conexión VPN debería estar activa
- [EC2.22] Deben eliminarse los grupos de seguridad de Amazon EC2 no utilizados
- [EC2.23] Amazon EC2 Transit Gateways no debe aceptar automáticamente las solicitudes de adjuntos de VPC
- [EC2.28] Los volúmenes de EBS deben estar cubiertos por un plan de respaldo
- [EC2.36] Las pasarelas de clientes de EC2 deben estar etiquetadas
- [EC2.51] Los puntos finales EC2 Client VPN deben tener habilitado el registro de conexiones de clientes
- [EC2.53] Los grupos de seguridad de EC2 no deberían permitir la entrada desde la versión 0.0.0.0/0 a los puertos de administración remota del servidor
- [EC2.54] Los grupos de seguridad de EC2 no deberían permitir la entrada desde: :/0 a los puertos de administración remota del servidor
- [EC2.58] Las VPC deben configurarse con un punto final de interfaz para los contactos de Systems Manager Incident Manager
- [EC2.60] Las VPC deben configurarse con un punto final de interfaz para Systems Manager Incident Manager
- [EC2.171] Las conexiones VPN de EC2 deberían tener el registro habilitado
- [EC2.173] Las solicitudes de EC2 Spot Fleet con parámetros de lanzamiento deberían permitir el cifrado de los volúmenes de EBS adjuntos
- [EC2.174] Los conjuntos de opciones DHCP de EC2 deben estar etiquetados
- [EC2.175] Las plantillas de lanzamiento de EC2 deben estar etiquetadas
- [EC2.176] Las listas de prefijos de EC2 deben estar etiquetadas
- [EC2.177] Las sesiones de réplica de tráfico de EC2 deben etiquetarse
- [EC2.178] Los filtros espejo de tráfico EC2 deben estar etiquetados
- [EC2.179] Los objetivos del espejo de tráfico de EC2 deben estar etiquetados
- [EC2.180] Las interfaces de red EC2 deberían tener habilitada source/destination la verificación
- [EC2.183] Las conexiones VPN de EC2 deben utilizar el protocolo IKEv2
- [ECR.1] Los repositorios privados de ECR deben tener configurado el escaneo de imágenes
- [ECR.4] Los repositorios públicos de ECR deben etiquetarse
- [EFS.6] Los destinos de montaje de EFS no deben asociarse a subredes que asignan direcciones IP públicas en el momento del lanzamiento

- [EKS.3] Los clústeres de EKS deben usar secretos de Kubernetes cifrados
- [ELB.2] Los balanceadores de carga clásicos con SSL/HTTPS oyentes deben usar un certificado proporcionado por AWS Gestor de certificados
- [ELB.17] Los balanceadores de cargas de aplicaciones y redes con oyentes deben usar las políticas de seguridad recomendadas
- [ELB.21] Los grupos destinatarios de Application and Network Load Balancer deben utilizar protocolos de control de estado cifrados
- [ELB.22] Los grupos objetivo del ELB deben usar protocolos de transporte cifrados
- [ElastiCache.1] ElastiCache (Redis OSS) los clústeres deben tener habilitadas las copias de seguridad automáticas
- [ElasticBeanstalk.3] Elastic Beanstalk debería transmitir los registros a CloudWatch
- [EMR.2] La configuración de acceso público del bloque Amazon EMR debe estar habilitada
- [EMR.3] Las configuraciones de seguridad de Amazon EMR deben cifrarse en reposo
- [EMR.4] Las configuraciones de seguridad de Amazon EMR deben cifrarse en tránsito
- [ES.4] Debería estar habilitado el registro de errores de dominio de Elasticsearch en Logs CloudWatch
- [EventBridge.4] los puntos finales EventBridge globales deberían tener habilitada la replicación de eventos
- [FraudDetector.1] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.2] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas
- [FraudDetector.3] Los resultados de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.4] Las variables de Amazon Fraud Detector deben estar etiquetadas
- [FSx.1] FSx para sistemas de archivos OpenZFS debe configurarse para copiar etiquetas en copias de seguridad y volúmenes
- [FSx.2] Los sistemas de archivos FSx for Lustre deben configurarse para copiar etiquetas a las copias de seguridad
- [FSx.5] Los sistemas de archivos FSx for Windows File Server deben configurarse para Multi-AZ su implementación
- [GlobalAccelerator.1] Los aceleradores de Global Accelerator deben estar etiquetados
- [GuardDuty.3] Los GuardDuty IPSets deben estar etiquetados
- [GuardDuty.4] GuardDuty los detectores deben estar etiquetados

- [GuardDuty.5] La monitorización del registro de auditoría de GuardDuty EKS debe estar habilitada
- [GuardDuty.6] GuardDuty La protección Lambda debe estar habilitada
- [GuardDuty.7] La monitorización del tiempo de ejecución de GuardDuty EKS debe estar habilitada
- [GuardDuty.8] La protección contra GuardDuty malware para EC2 debe estar habilitada
- [GuardDuty.9] La protección GuardDuty RDS debe estar habilitada
- [GuardDuty.10] La protección GuardDuty S3 debe estar habilitada
- [GuardDuty.11] La monitorización del GuardDuty tiempo de ejecución debe estar habilitada
- [GuardDuty.12] La monitorización del tiempo de ejecución de GuardDuty ECS debe estar habilitada
- [GuardDuty.13] La monitorización del tiempo de ejecución de GuardDuty EC2 debe estar habilitada
- [IAM.6] La MFA de hardware debe estar habilitada para el usuario root
- [IAM.9] La MFA debe estar habilitada para el usuario root
- [IAM.21] Las políticas de IAM gestionadas por el cliente que cree no deberían permitir acciones comodín en los servicios
- [IAM.23] Los analizadores de IAM Access Analyzer deben estar etiquetados
- [IAM.24] Las funciones de IAM deben estar etiquetadas
- [IAM.25] Los usuarios de IAM deben estar etiquetados
- [IAM.26] SSL/TLS Los certificados caducados gestionados en IAM deben eliminarse
- [IAM.27] Las identidades de IAM no deberían tener la AWSCloudShellFullAccess política adjunta
- [IAM.28] El analizador de acceso externo de IAM Access Analyzer debe estar habilitado
- [Inspector.1] El escaneo EC2 de Amazon Inspector debe estar activado
- [Inspector.2] El escaneo ECR de Amazon Inspector debe estar activado
- [Inspector.3] El escaneo de código Lambda de Amazon Inspector Lambda debe estar activado
- [Inspector.4] El escaneo estándar de Amazon Inspector Lambda debe estar activado
- [IoTSiteWise.1]AWSLos modelos SiteWise de activos de IoT deben estar etiquetados
- [IoTSiteWise.2]AWS SiteWise Los paneles de IoT deben estar etiquetados
- [IoTSiteWise.3]AWS SiteWise Las pasarelas de IoT deben estar etiquetadas
- [IoTSiteWise.4]AWS SiteWise Los portales de IoT deben estar etiquetados
- [IoTSiteWise.5]AWS SiteWise Los proyectos de IoT deben estar etiquetados

- [IoTTwinMaker.1]AWSLos trabajos de TwinMaker sincronización de IoT deben estar etiquetados
- [IoTTwinMaker.2]AWS TwinMaker Los espacios de trabajo de IoT deben estar etiquetados
- [IoTTwinMaker.3]AWS TwinMaker Las escenas de IoT deben estar etiquetadas
- [IoTTwinMaker.4]AWS TwinMaker Las entidades de IoT deben estar etiquetadas
- [IoTWireless.1]AWSLos grupos de multidifusión de IoT Wireless deben estar etiquetados
- [IoTWireless.2]AWSLos perfiles de servicio de IoT Wireless deben estar etiquetados
- [IoTWireless.3]AWSLas tareas de IoT FUOTA deben estar etiquetadas
- [IVS.1] Los pares de teclas de reproducción IVS deben estar etiquetados
- [IVS.2] Las configuraciones de grabación de IVS deben estar etiquetadas
- [IVS.3] Los canales IVS deben estar etiquetados
- [Keyspaces.1] Los espacios clave de Amazon Keyspaces deben estar etiquetados
- [Macie.1] Amazon Macie debería estar activado
- [Macie.2] La detección automática de datos confidenciales por parte de Macie debería estar habilitada
- [MQ.2] Los corredores de ActiveMQ deben transmitir los registros de auditoría a CloudWatch
- [MSK.3] Los conectores MSK Connect deben estar cifrados en tránsito
- [MSK.5] Los conectores MSK deben tener el registro activado
- [Neptune.1] Los clústeres de bases de datos de Neptune deben cifrarse en reposo
- [Neptune.2] Los clústeres de bases de datos de Neptune deberían publicar registros de auditoría en Logs CloudWatch
- [Neptune.3] Las instantáneas del clúster de base de datos de Neptune no deben ser públicas
- [Neptune.4] Los clústeres de base de datos de Neptune deben tener habilitada la protección contra eliminación
- [Neptune.5] Los clústeres de Neptune DB deberían tener habilitadas las copias de seguridad automatizadas
- [Neptune.6] Las instantáneas del clúster de base de datos de Neptune deben cifrarse en reposo
- [Neptune.7] Los clústeres de base de datos de Neptune deben tener habilitada la autenticación de bases de datos de IAM
- [Neptune.8] Los clústeres de bases de datos de Neptune deben configurarse para copiar etiquetas a las instantáneas

- [Neptune.9] Los clústeres de base de datos Neptune deben implementarse en varias zonas de disponibilidad
- [NetworkFirewall.1] Los firewalls de Network Firewall deben implementarse en varias zonas de disponibilidad
- [NetworkFirewall.2] El registro de Network Firewall debe estar habilitado
- [NetworkFirewall.3] Las políticas de Network Firewall deben tener asociado al menos un grupo de reglas
- [NetworkFirewall.4] La acción sin estado predeterminada para las políticas de Network Firewall debe ser eliminar o reenviar paquetes completos
- [NetworkFirewall.5] La acción sin estado predeterminada para las políticas de Network Firewall debe ser eliminar o reenviar paquetes fragmentados
- [NetworkFirewall.6] El grupo de reglas de Stateless Network Firewall no debe estar vacío
- [NetworkFirewall.9] Los firewalls de Network Firewall deben tener habilitada la protección de eliminación
- [NetworkFirewall.10] Los firewalls de Network Firewall deben tener habilitada la protección contra cambios de subred
- [Opensearch.1] OpenSearch los dominios deben tener activado el cifrado en reposo
- [Opensearch.2] OpenSearch los dominios no deben ser de acceso público
- [Opensearch.3] OpenSearch los dominios deben cifrar los datos enviados entre nodos
- [Opensearch.4] El registro de errores de OpenSearch dominio en Logs debe estar habilitado CloudWatch
- [Opensearch.5] OpenSearch los dominios deben tener activado el registro de auditoría
- [Opensearch.6] OpenSearch los dominios deben tener al menos tres nodos de datos
- [Opensearch.7] OpenSearch los dominios deben tener habilitado un control de acceso detallado
- [Opensearch.8] Las conexiones a los OpenSearch dominios deben cifrarse con la última política de seguridad de TLS
- [Opensearch.11] OpenSearch los dominios deben tener al menos tres nodos principales dedicados
- [PCA.1]AWS Privada CALa autoridad emisora de certificados raíz debe estar deshabilitada
- [PCA.2]AWSLas autoridades de certificación de CA privadas deben estar etiquetadas
- [RDS.7] Los clústeres de RDS deben tener habilitada la protección contra eliminaciones
- [RDS.12] La autenticación de IAM debe configurarse para los clústeres de RDS

- [RDS.14] Los clústeres de Amazon Aurora deben tener habilitado el retroceso
- [RDS.15] Los clústeres de bases de datos de RDS deben configurarse para varias zonas de disponibilidad
- [RDS.16] Los clústeres de bases de datos de Aurora deben configurarse para copiar las etiquetas a las instantáneas de bases de datos
- [RDS.24] Los clústeres de bases de datos de RDS deben usar un nombre de usuario de administrador personalizado
- [RDS.25] Las instancias de bases de datos de RDS deben usar un nombre de usuario de administrador personalizado
- [RDS.26] Las instancias de base de datos de RDS deben protegerse mediante un plan de respaldo
- [RDS.27] Los clústeres de bases de datos de RDS deben cifrarse en reposo
- [RDS.28] Los clústeres de bases de datos de RDS deben etiquetarse
- [RDS.31] Los grupos de seguridad de la base de datos de RDS deben etiquetarse
- [RDS.34] Los clústeres de bases de datos Aurora MySQL deben publicar los registros de auditoría en Logs CloudWatch
- [RDS.35] Los clústeres de bases de datos de RDS deben tener habilitada la actualización automática de versiones secundarias
- [RDS.37] Los clústeres de bases de datos de Aurora PostgreSQL deben publicar los registros en Logs CloudWatch
- [RDS.42] Las instancias de base de datos de RDS para MariaDB deben publicar los registros en Logs CloudWatch
- [RDS.43] Los proxies de bases de datos de RDS deben requerir el cifrado TLS para las conexiones
- [RDS.44] Las instancias de base de datos de RDS para MariaDB deben cifrarse durante el tránsito
- [RDS.45] Los clústeres de bases de datos Aurora MySQL deben tener habilitado el registro de auditoría
- [RDS.47] Los clústeres de bases de datos de RDS para PostgreSQL deben configurarse para copiar las etiquetas a las instantáneas de bases de datos
- [RDS.48] Los clústeres de bases de datos de RDS para MySQL deben configurarse para copiar etiquetas a las instantáneas de bases de datos
- [RDS.50] Los clústeres de bases de datos de RDS deben tener un período de retención de copias de seguridad suficiente

- [RDS.51] Los clústeres globales de RDS deben ejecutarse en una versión compatible de Aurora MySQL
- [Redshift.10] Los clústeres de Redshift deben cifrarse en reposo
- [Redshift.15] Los grupos de seguridad de Redshift deberían permitir la entrada en el puerto del clúster solo desde orígenes restringidos
- [Redshift.17] Los grupos de parámetros del clúster de Redshift deben estar etiquetados
- [RedshiftServerless.1] Los grupos de trabajo sin servidor de Amazon Redshift deberían utilizar un enrutamiento de VPC mejorado
- [RedshiftServerless.2] Las conexiones a los grupos de trabajo sin servidor de Redshift deberían ser obligatorias para usar SSL
- [RedshiftServerless.3] Los grupos de trabajo sin servidor de Redshift deberían prohibir el acceso público
- [Route53.1] Los controles de salud de Route 53 deben estar etiquetados
- [Route53.2] Las zonas alojadas públicas de Route 53 deberían registrar las consultas de DNS
- [S3.22] Los cubos de uso general de S3 deben registrar los eventos de escritura a nivel de objeto
- [S3.23] Los cubos de uso general de S3 deben registrar los eventos de lectura a nivel de objeto
- [S3.24] Los puntos de Multi-Region acceso S3 deben tener habilitada la configuración de bloqueo del acceso público
- [S3.25] Los buckets de directorio de S3 deben tener configuraciones de ciclo de vida
- [SageMaker.4] Las variantes de producción de SageMaker terminales deben tener un recuento inicial de instancias superior a 1
- SageMaker Los modelos [SageMaker.5] deben tener habilitado el aislamiento de red
- [SageMaker.6] las configuraciones de imagen de la SageMaker aplicación deben estar etiquetadas
- [SageMaker.7] SageMaker las imágenes deben estar etiquetadas
- [SageMaker.9] las definiciones de trabajos de calidad de los SageMaker datos deben tener habilitado el cifrado del tráfico entre contenedores
- [SageMaker.10] Las definiciones de trabajos de explicabilidad del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores
- [SageMaker.11] las definiciones de trabajos SageMaker de calidad de los datos deben tener habilitado el aislamiento de red
- [SageMaker.12] las definiciones de trabajo basadas en el sesgo del SageMaker modelo deben tener habilitado el aislamiento de red

- [SageMaker.13] las definiciones de trabajos de calidad del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores
- [SageMaker.14] los programas SageMaker de monitoreo deben tener habilitado el aislamiento de la red
- [SageMaker.15] Las definiciones de trabajo basadas en el sesgo del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores
- SageMaker Los modelos [SageMaker.16] deben usar un registro privado en la VPC para los contenedores principales
- [SageMaker.19] SageMaker los modelos deben usar un registro privado en la VPC para las canalizaciones de inferencia de varios contenedores
- [SES.1] Las listas de contactos de SES deben estar etiquetadas
- [SES.2] Los conjuntos de configuración de SES deben estar etiquetados
- [SES.3] Los conjuntos de configuración de SES deben tener el TLS habilitado para enviar correos electrónicos
- [ServiceCatalog.1] Las carteras de Service Catalog deben compartirse dentro de unAWSsolo una organización
- [SSM.5] Los documentos SSM deben estar etiquetados
- [SSM.6] SSM Automation debería tener el registro habilitado CloudWatch
- [Transfer.2] Los servidores Transfer Family no deben usar el protocolo FTP para la conexión de puntos finales
- [Transfer.4] Los acuerdos Transfer Family deben estar etiquetados
- [Transfer.5] Los certificados Transfer Family deben estar etiquetados
- [Transfer.6] Los conectores Transfer Family deben estar etiquetados
- [Transfer.7] Los perfiles de Transfer Family deben estar etiquetados
- [WAF.1]AWS WAFEl registro de ACL web global clásico debe estar habilitado
- [WAF.3]AWS WAFLos grupos de reglas regionales clásicos deben tener al menos una regla
- [WAF.6]AWS WAFLas reglas globales clásicas deben tener al menos una condición
- [WAF.7]AWS WAFLos grupos de reglas globales clásicos deben tener al menos una regla
- [WAF.8]AWS WAFLas ACL web globales clásicas deben tener al menos una regla o grupo de reglas
- [WorkSpaces.1] los volúmenes de WorkSpaces usuarios deben cifrarse en reposo

- [WorkSpaces.2] los volúmenes WorkSpaces raíz deben cifrarse en reposo

China (Ningxia)

Los siguientes controles no se admiten en la región China (Ningxia).

- [ACM.1] ACM-issued Los certificados importados y renovados deben renovarse después de un período de tiempo específico
- [ACM.2] Los certificados RSA gestionados por ACM deben utilizar una longitud de clave de al menos 2048 bits
- [Account.2]Cuentas de AWSdebe formar parte de unAWS Organizationsorganización
- [APIGateway.2] Las etapas de la API REST de API Gateway deben configurarse para usar certificados SSL para la autenticación de backend
- [APIGateway.10] Las integraciones de API Gateway V2 deben usar HTTPS para las conexiones privadas
- [APIGateway.11] Los nombres de dominio de API Gateway deben usar las políticas de seguridad recomendadas
- [Amplify.1] Las aplicaciones Amplify deben estar etiquetadas
- [Amplify.2] Amplify branches debe estar etiquetado
- [AppConfig.1]AWS AppConfiglas aplicaciones deben estar etiquetadas
- [AppConfig.2]AWS AppConfiglos perfiles de configuración deben estar etiquetados
- [AppConfig.3]AWS AppConfiglos entornos deben estar etiquetados
- [AppConfig.4]AWS AppConfiglas asociaciones de extensiones deben estar etiquetadas
- [AppFlow.1] AppFlow Los flujos de Amazon deben estar etiquetados
- [AppRunner.1] Los servicios de App Runner deben estar etiquetados
- [AppRunner.2] Los conectores VPC de App Runner deben estar etiquetados
- [AppSync.1]AWS AppSyncLas cachés de las API deben estar cifradas en reposo
- [AppSync.6]AWS AppSyncLas cachés de las API deben cifrarse en tránsito
- [Backup.1]AWS Backuplos puntos de recuperación deben estar cifrados en reposo
- [Backup.4]AWS Backuplos planes de informes deben estar etiquetados
- [Batch.1] Las colas de trabajos por lotes deben estar etiquetadas

- [Batch.2] Las políticas de programación de lotes deben estar etiquetadas
- [Batch.3] Los entornos de procesamiento por lotes deben etiquetarse
- [Batch.4] Las propiedades de los recursos de cómputo en los entornos de cómputo por lotes gestionados deben estar etiquetadas
- [BedrockAgentCore.1] Los AgentCore tiempos de ejecución de Bedrock deben configurarse con el modo de red VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways debería requerir autorización para las solicitudes entrantes
- [BedrockAgentCore.3] Bedrock AgentCore Memory debe estar cifrada y gestionada por el clienteAWS KMSclaves
- [BedrockAgentCore.4] Bedrock AgentCore Gateway debe cifrarse de forma que sea gestionada por el clienteAWS KMSclaves
- [BedrockAgentCore.5] Los navegadores AgentCore personalizados de Bedrock no deberían usar el modo de red pública
- [BedrockAgentCore.6] Los navegadores AgentCore personalizados de Bedrock deberían tener habilitada la grabación de sesiones
- [CloudFront.1] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado
- [CloudFront.3] CloudFront las distribuciones deben requerir el cifrado durante el tránsito
- [CloudFront.4] CloudFront las distribuciones deben tener configurada la conmutación por error de origen
- [CloudFront.5] CloudFront las distribuciones deben tener habilitado el registro
- [CloudFront.6] CloudFront las distribuciones deben tener WAF activado
- [CloudFront.7] CloudFront las distribuciones deben usar certificados personalizados SSL/TLS
- [CloudFront.8] CloudFront las distribuciones deben usar el SNI para atender las solicitudes HTTPS
- [CloudFront.9] CloudFront las distribuciones deben cifrar el tráfico para convertirlo en orígenes personalizados
- [CloudFront.10] CloudFront las distribuciones no deben usar protocolos SSL obsoletos entre ubicaciones de borde y orígenes personalizados
- [CloudFront.12] CloudFront las distribuciones no deben apuntar a orígenes de S3 inexistentes
- [CloudFront.13] CloudFront las distribuciones deben usar el control de acceso al origen

- [CloudFront.14] CloudFront las distribuciones deben estar etiquetadas
- [CloudFront.15] CloudFront las distribuciones deben usar la política de seguridad TLS recomendada
- [CloudFront.16] CloudFront las distribuciones deben usar el control de acceso de origen para los orígenes de las URL de las funciones de Lambda
- [CloudFront.17] CloudFront las distribuciones deben usar grupos de claves confiables para las URL y cookies firmadas
- [CloudTrail.10] Los almacenes de datos de eventos de CloudTrail Lake deben estar cifrados y gestionados por el clienteAWS KMS keys
- [CodeArtifact.1] CodeArtifact los repositorios deben estar etiquetados
- [CodeGuruProfiler.1] Los grupos CodeGuru de creación de perfiles de Profiler deben estar etiquetados
- [CodeGuruReviewer.1] Las asociaciones de repositorios de CodeGuru Reviewer deben estar etiquetadas
- [Cognito.1] Los grupos de usuarios de Cognito deben tener activada la protección contra amenazas y el modo de aplicación con todas las funciones para la autenticación estándar
- [Cognito.2] Los grupos de identidades de Cognito no deben permitir identidades no autenticadas
- [Cognito.3] Las políticas de contraseñas para los grupos de usuarios de Cognito deben tener configuraciones sólidas
- [Cognito.4] Los grupos de usuarios de Cognito deben tener activada la protección contra amenazas y el modo de aplicación con todas las funciones para la autenticación personalizada
- [Cognito.5] La MFA debe estar habilitada para los grupos de usuarios de Cognito
- [Cognito.6] Los grupos de usuarios de Cognito deben tener habilitada la protección contra la eliminación
- [Connect.1] Los tipos de objetos de los perfiles de clientes de Amazon Connect deben estar etiquetados
- [Connect.2] Las instancias de Connect Customer deben tener el CloudWatch registro habilitado
- [DataFirehose.1] Los flujos de entrega de Firehose deben cifrarse en reposo
- [DataSync.2] DataSync las tareas deben estar etiquetadas
- [Detective.1] Los gráficos de comportamiento de los detectives deben estar etiquetados
- [DMS.10] Los puntos finales de DMS para las bases de datos de Neptune deben tener habilitada la autorización de IAM

- [DMS.11] Los puntos finales de DMS para MongoDB deben tener un mecanismo de autenticación habilitado
- [DMS.12] Los puntos finales de DMS para Redis OSS deben tener el TLS habilitado
- [DocumentDB.3] Las instantáneas de clústeres manuales de Amazon DocumentDB no deben ser públicas
- [DynamoDB.3] Los clústeres de DynamoDB Accelerator (DAX) deben cifrarse en reposo
- [DynamoDB.4] Las tablas de DynamoDB deben estar presentes en un plan de respaldo
- [DynamoDB.7] Los clústeres de DynamoDB Accelerator deben cifrarse en tránsito
- [EC2.20] Ambos túneles VPN para un AWS Site-to-Site La conexión VPN debería estar activa
- [EC2.22] Deben eliminarse los grupos de seguridad de Amazon EC2 no utilizados
- [EC2.23] Amazon EC2 Transit Gateways no debe aceptar automáticamente las solicitudes de adjuntos de VPC
- [EC2.24] No se deben utilizar los tipos de instancias paravirtuales de Amazon EC2
- [EC2.28] Los volúmenes de EBS deben estar cubiertos por un plan de respaldo
- [EC2.36] Las pasarelas de clientes de EC2 deben estar etiquetadas
- [EC2.50] Las pasarelas VPN de EC2 deben estar etiquetadas
- [EC2.51] Los puntos finales EC2 Client VPN deben tener habilitado el registro de conexiones de clientes
- [EC2.58] Las VPC deben configurarse con un punto final de interfaz para los contactos de Systems Manager Incident Manager
- [EC2.60] Las VPC deben configurarse con un punto final de interfaz para Systems Manager Incident Manager
- [EC2.171] Las conexiones VPN de EC2 deberían tener el registro habilitado
- [EC2.173] Las solicitudes de EC2 Spot Fleet con parámetros de lanzamiento deberían permitir el cifrado de los volúmenes de EBS adjuntos
- [EC2.174] Los conjuntos de opciones DHCP de EC2 deben estar etiquetados
- [EC2.175] Las plantillas de lanzamiento de EC2 deben estar etiquetadas
- [EC2.176] Las listas de prefijos de EC2 deben estar etiquetadas
- [EC2.177] Las sesiones de réplica de tráfico de EC2 deben etiquetarse
- [EC2.178] Los filtros espejo de tráfico EC2 deben estar etiquetados

- [EC2.179] Los objetivos del espejo de tráfico de EC2 deben estar etiquetados
- [EC2.183] Las conexiones VPN de EC2 deben utilizar el protocolo IKEv2
- [ECR.1] Los repositorios privados de ECR deben tener configurado el escaneo de imágenes
- [ECR.4] Los repositorios públicos de ECR deben etiquetarse
- [EFS.3] Los puntos de acceso EFS deben exigir un directorio raíz
- [EFS.4] Los puntos de acceso EFS deben exigir la identidad del usuario
- [EFS.6] Los destinos de montaje de EFS no deben asociarse a subredes que asignan direcciones IP públicas en el momento del lanzamiento
- [EKS.3] Los clústeres de EKS deben usar secretos de Kubernetes cifrados
- [ELB.2] Los balanceadores de carga clásicos con SSL/HTTPS oyentes deben usar un certificado proporcionado por AWS Gestor de certificados
- [ELB.17] Los balanceadores de cargas de aplicaciones y redes con oyentes deben usar las políticas de seguridad recomendadas
- [ELB.21] Los grupos destinatarios de Application and Network Load Balancer deben utilizar protocolos de control de estado cifrados
- [ELB.22] Los grupos objetivo del ELB deben usar protocolos de transporte cifrados
- [ElastiCache.1] ElastiCache (Redis OSS) los clústeres deben tener habilitadas las copias de seguridad automáticas
- [ElasticBeanstalk.3] Elastic Beanstalk debería transmitir los registros a CloudWatch
- [EMR.2] La configuración de acceso público del bloque Amazon EMR debe estar habilitada
- [EMR.3] Las configuraciones de seguridad de Amazon EMR deben cifrarse en reposo
- [EMR.4] Las configuraciones de seguridad de Amazon EMR deben cifrarse en tránsito
- [ES.4] Debería estar habilitado el registro de errores de dominio de Elasticsearch en Logs CloudWatch
- [EventBridge.4] los puntos finales EventBridge globales deberían tener habilitada la replicación de eventos
- [FraudDetector.1] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.2] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas
- [FraudDetector.3] Los resultados de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.4] Las variables de Amazon Fraud Detector deben estar etiquetadas

- [FSx.1] FSx para sistemas de archivos OpenZFS debe configurarse para copiar etiquetas en copias de seguridad y volúmenes
- [FSx.2] Los sistemas de archivos FSx for Lustre deben configurarse para copiar etiquetas a las copias de seguridad
- [FSx.5] Los sistemas de archivos FSx for Windows File Server deben configurarse para Multi-AZ su implementación
- [GlobalAccelerator.1] Los aceleradores de Global Accelerator deben estar etiquetados
- [Glue.3]AWS GlueLas transformaciones de aprendizaje automático deben cifrarse en reposo
- [GuardDuty.3] Los GuardDuty IPSets deben estar etiquetados
- [GuardDuty.4] GuardDuty los detectores deben estar etiquetados
- [GuardDuty.5] La monitorización del registro de auditoría de GuardDuty EKS debe estar habilitada
- [GuardDuty.6] GuardDuty La protección Lambda debe estar habilitada
- [GuardDuty.7] La monitorización del tiempo de ejecución de GuardDuty EKS debe estar habilitada
- [GuardDuty.8] La protección contra GuardDuty malware para EC2 debe estar habilitada
- [GuardDuty.9] La protección GuardDuty RDS debe estar habilitada
- [GuardDuty.10] La protección GuardDuty S3 debe estar habilitada
- [GuardDuty.11] La monitorización del GuardDuty tiempo de ejecución debe estar habilitada
- [GuardDuty.12] La monitorización del tiempo de ejecución de GuardDuty ECS debe estar habilitada
- [GuardDuty.13] La monitorización del tiempo de ejecución de GuardDuty EC2 debe estar habilitada
- [IAM.6] La MFA de hardware debe estar habilitada para el usuario root
- [IAM.9] La MFA debe estar habilitada para el usuario root
- [IAM.21] Las políticas de IAM gestionadas por el cliente que cree no deberían permitir acciones comodín en los servicios
- [IAM.23] Los analizadores de IAM Access Analyzer deben estar etiquetados
- [IAM.24] Las funciones de IAM deben estar etiquetadas
- [IAM.25] Los usuarios de IAM deben estar etiquetados
- [IAM.26] SSL/TLS Los certificados caducados gestionados en IAM deben eliminarse
- [IAM.27] Las identidades de IAM no deberían tener la AWSCloudShellFullAccess política adjunta
- [IAM.28] El analizador de acceso externo de IAM Access Analyzer debe estar habilitado

- [Inspector.1] El escaneo EC2 de Amazon Inspector debe estar activado
- [Inspector.2] El escaneo ECR de Amazon Inspector debe estar activado
- [Inspector.3] El escaneo de código Lambda de Amazon Inspector Lambda debe estar activado
- [Inspector.4] El escaneo estándar de Amazon Inspector Lambda debe estar activado
- [IoTSiteWise.1]AWSLos modelos SiteWise de activos de IoT deben estar etiquetados
- [IoTSiteWise.2]AWS SiteWise Los paneles de IoT deben estar etiquetados
- [IoTSiteWise.3]AWS SiteWise Las pasarelas de IoT deben estar etiquetadas
- [IoTSiteWise.4]AWS SiteWise Los portales de IoT deben estar etiquetados
- [IoTSiteWise.5]AWS SiteWise Los proyectos de IoT deben estar etiquetados
- [IoTTwinMaker.1]AWSLos trabajos de TwinMaker sincronización de IoT deben estar etiquetados
- [IoTTwinMaker.2]AWS TwinMaker Los espacios de trabajo de IoT deben estar etiquetados
- [IoTTwinMaker.3]AWS TwinMaker Las escenas de IoT deben estar etiquetadas
- [IoTTwinMaker.4]AWS TwinMaker Las entidades de IoT deben estar etiquetadas
- [IoTWireless.1]AWSLos grupos de multidifusión de IoT Wireless deben estar etiquetados
- [IoTWireless.2]AWSLos perfiles de servicio de IoT Wireless deben estar etiquetados
- [IoTWireless.3]AWSLas tareas de IoT FUOTA deben estar etiquetadas
- [IVS.1] Los pares de teclas de reproducción IVS deben estar etiquetados
- [IVS.2] Las configuraciones de grabación de IVS deben estar etiquetadas
- [IVS.3] Los canales IVS deben estar etiquetados
- [Keyspaces.1] Los espacios clave de Amazon Keyspaces deben estar etiquetados
- [Lambda.1] Las políticas de las funciones de Lambda deberían prohibir el acceso público
- [Lambda.2] Las funciones de Lambda deben usar los tiempos de ejecución compatibles
- [Lambda.3] Las funciones de Lambda deben estar en una VPC
- [Lambda.5] Las funciones de VPC Lambda deben funcionar en varias zonas de disponibilidad
- [Lambda.6] Las funciones de Lambda deben estar etiquetadas
- [Lambda.7] Las funciones de Lambda deberían tener AWS X-Ray el rastreo activo está habilitado
- [Macie.1] Amazon Macie debería estar activado
- [Macie.2] La detección automática de datos confidenciales por parte de Macie debería estar habilitada

- [MQ.2] Los corredores de ActiveMQ deben transmitir los registros de auditoría a CloudWatch
- [MSK.3] Los conectores MSK Connect deben estar cifrados en tránsito
- [MSK.5] Los conectores MSK deben tener el registro activado
- [Neptune.3] Las instantáneas del clúster de base de datos de Neptune no deben ser públicas
- [NetworkFirewall.1] Los firewalls de Network Firewall deben implementarse en varias zonas de disponibilidad
- [NetworkFirewall.2] El registro de Network Firewall debe estar habilitado
- [NetworkFirewall.3] Las políticas de Network Firewall deben tener asociado al menos un grupo de reglas
- [NetworkFirewall.4] La acción sin estado predeterminada para las políticas de Network Firewall debe ser eliminar o reenviar paquetes completos
- [NetworkFirewall.5] La acción sin estado predeterminada para las políticas de Network Firewall debe ser eliminar o reenviar paquetes fragmentados
- [NetworkFirewall.6] El grupo de reglas de Stateless Network Firewall no debe estar vacío
- [NetworkFirewall.9] Los firewalls de Network Firewall deben tener habilitada la protección de eliminación
- [NetworkFirewall.10] Los firewalls de Network Firewall deben tener habilitada la protección contra cambios de subred
- [Opensearch.1] OpenSearch los dominios deben tener activado el cifrado en reposo
- [Opensearch.2] OpenSearch los dominios no deben ser de acceso público
- [Opensearch.3] OpenSearch los dominios deben cifrar los datos enviados entre nodos
- [Opensearch.4] El registro de errores de OpenSearch dominio en Logs debe estar habilitado CloudWatch
- [Opensearch.5] OpenSearch los dominios deben tener activado el registro de auditoría
- [Opensearch.6] OpenSearch los dominios deben tener al menos tres nodos de datos
- [Opensearch.7] OpenSearch los dominios deben tener habilitado un control de acceso detallado
- [Opensearch.8] Las conexiones a los OpenSearch dominios deben cifrarse con la última política de seguridad de TLS
- [Opensearch.11] OpenSearch los dominios deben tener al menos tres nodos principales dedicados
- [PCA.1]AWS Privada CALa autoridad emisora de certificados raíz debe estar deshabilitada
- [PCA.2]AWSLas autoridades de certificación de CA privadas deben estar etiquetadas

- [RDS.14] Los clústeres de Amazon Aurora deben tener habilitado el retroceso
- [RDS.24] Los clústeres de bases de datos de RDS deben usar un nombre de usuario de administrador personalizado
- [RDS.25] Las instancias de bases de datos de RDS deben usar un nombre de usuario de administrador personalizado
- [RDS.26] Las instancias de base de datos de RDS deben protegerse mediante un plan de respaldo
- [RDS.31] Los grupos de seguridad de la base de datos de RDS deben etiquetarse
- [RDS.34] Los clústeres de bases de datos Aurora MySQL deben publicar los registros de auditoría en Logs CloudWatch
- [RDS.35] Los clústeres de bases de datos de RDS deben tener habilitada la actualización automática de versiones secundarias
- [RDS.42] Las instancias de base de datos de RDS para MariaDB deben publicar los registros en Logs CloudWatch
- [RDS.43] Los proxies de bases de datos de RDS deben requerir el cifrado TLS para las conexiones
- [RDS.44] Las instancias de base de datos de RDS para MariaDB deben cifrarse durante el tránsito
- [RDS.45] Los clústeres de bases de datos Aurora MySQL deben tener habilitado el registro de auditoría
- [RDS.50] Los clústeres de bases de datos de RDS deben tener un período de retención de copias de seguridad suficiente
- [RDS.51] Los clústeres globales de RDS deben ejecutarse en una versión compatible de Aurora MySQL
- [Redshift.10] Los clústeres de Redshift deben cifrarse en reposo
- [Redshift.15] Los grupos de seguridad de Redshift deberían permitir la entrada en el puerto del clúster solo desde orígenes restringidos
- [Redshift.17] Los grupos de parámetros del clúster de Redshift deben estar etiquetados
- [RedshiftServerless.1] Los grupos de trabajo sin servidor de Amazon Redshift deberían utilizar un enrutamiento de VPC mejorado
- [RedshiftServerless.2] Las conexiones a los grupos de trabajo sin servidor de Redshift deberían ser obligatorias para usar SSL
- [RedshiftServerless.3] Los grupos de trabajo sin servidor de Redshift deberían prohibir el acceso público

- [Route53.1] Los controles de salud de Route 53 deben estar etiquetados
- [Route53.2] Las zonas alojadas públicas de Route 53 deberían registrar las consultas de DNS
- [S3.24] Los puntos de Multi-Region acceso S3 deben tener habilitada la configuración de bloqueo del acceso público
- [S3.25] Los buckets de directorio de S3 deben tener configuraciones de ciclo de vida
- [SageMaker.4] Las variantes de producción de SageMaker terminales deben tener un recuento inicial de instancias superior a 1
- SageMaker Los modelos [SageMaker.5] deben tener habilitado el aislamiento de red
- [SageMaker.6] las configuraciones de imagen de la SageMaker aplicación deben estar etiquetadas
- [SageMaker.7] SageMaker las imágenes deben estar etiquetadas
- [SageMaker.9] las definiciones de trabajos de calidad de los SageMaker datos deben tener habilitado el cifrado del tráfico entre contenedores
- [SageMaker.10] Las definiciones de trabajos de explicabilidad del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores
- [SageMaker.11] las definiciones de trabajos SageMaker de calidad de los datos deben tener habilitado el aislamiento de red
- [SageMaker.12] las definiciones de trabajo basadas en el sesgo del SageMaker modelo deben tener habilitado el aislamiento de red
- [SageMaker.13] las definiciones de trabajos de calidad del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores
- [SageMaker.14] los programas SageMaker de monitoreo deben tener habilitado el aislamiento de la red
- [SageMaker.15] Las definiciones de trabajo basadas en el sesgo del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores
- SageMaker Los modelos [SageMaker.16] deben usar un registro privado en la VPC para los contenedores principales
- [SageMaker.19] SageMaker los modelos deben usar un registro privado en la VPC para las canalizaciones de inferencia de varios contenedores
- [SES.3] Los conjuntos de configuración de SES deben tener el TLS habilitado para enviar correos electrónicos
- [ServiceCatalog.1] Las carteras de Service Catalog deben compartirse dentro de unAWSsolo una organización

- [SSM.5] Los documentos SSM deben estar etiquetados
- [SSM.7] Los documentos SSM deben tener habilitada la configuración de bloqueo para compartir en público
- [StepFunctions.2] Las actividades de Step Functions deben estar etiquetadas
- [Transfer.2] Los servidores Transfer Family no deben usar el protocolo FTP para la conexión de puntos finales
- [Transfer.4] Los acuerdos Transfer Family deben estar etiquetados
- [Transfer.5] Los certificados Transfer Family deben estar etiquetados
- [Transfer.6] Los conectores Transfer Family deben estar etiquetados
- [Transfer.7] Los perfiles de Transfer Family deben estar etiquetados
- [WAF.1]AWS WAFEl registro de ACL web global clásico debe estar habilitado
- [WAF.3]AWS WAFLos grupos de reglas regionales clásicos deben tener al menos una regla
- [WAF.6]AWS WAFLas reglas globales clásicas deben tener al menos una condición
- [WAF.7]AWS WAFLos grupos de reglas globales clásicos deben tener al menos una regla
- [WAF.8]AWS WAFLas ACL web globales clásicas deben tener al menos una regla o grupo de reglas

Europa (Fráncfort)

Los siguientes controles no se admiten en la región Europa (Fráncfort).

- [CloudFront.1] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado
- [CloudFront.3] CloudFront las distribuciones deben requerir el cifrado durante el tránsito
- [CloudFront.4] CloudFront las distribuciones deben tener configurada la conmutación por error de origen
- [CloudFront.5] CloudFront las distribuciones deben tener habilitado el registro
- [CloudFront.6] CloudFront las distribuciones deben tener WAF activado
- [CloudFront.7] CloudFront las distribuciones deben usar certificados personalizados SSL/TLS
- [CloudFront.8] CloudFront las distribuciones deben usar el SNI para atender las solicitudes HTTPS
- [CloudFront.9] CloudFront las distribuciones deben cifrar el tráfico para convertirlo en orígenes personalizados

- [CloudFront.10] CloudFront las distribuciones no deben usar protocolos SSL obsoletos entre ubicaciones de borde y orígenes personalizados
- [CloudFront.12] CloudFront las distribuciones no deben apuntar a orígenes de S3 inexistentes
- [CloudFront.13] CloudFront las distribuciones deben usar el control de acceso al origen
- [CloudFront.14] CloudFront las distribuciones deben estar etiquetadas
- [CloudFront.15] CloudFront las distribuciones deben usar la política de seguridad TLS recomendada
- [CloudFront.16] CloudFront las distribuciones deben usar el control de acceso de origen para los orígenes de las URL de las funciones de Lambda
- [CloudFront.17] CloudFront las distribuciones deben usar grupos de claves confiables para las URL y cookies firmadas
- [EC2.173] Las solicitudes de EC2 Spot Fleet con parámetros de lanzamiento deberían permitir el cifrado de los volúmenes de EBS adjuntos
- [ECR.4] Los repositorios públicos de ECR deben etiquetarse
- [FraudDetector.1] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.2] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas
- [FraudDetector.3] Los resultados de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.4] Las variables de Amazon Fraud Detector deben estar etiquetadas
- [GlobalAccelerator.1] Los aceleradores de Global Accelerator deben estar etiquetados
- [IAM.26] SSL/TLS Los certificados caducados gestionados en IAM deben eliminarse
- [RDS.31] Los grupos de seguridad de la base de datos de RDS deben etiquetarse
- [Route53.1] Los controles de salud de Route 53 deben estar etiquetados
- [Route53.2] Las zonas alojadas públicas de Route 53 deberían registrar las consultas de DNS
- [S3.24] Los puntos de Multi-Region acceso S3 deben tener habilitada la configuración de bloqueo del acceso público
- [S3.25] Los buckets de directorio de S3 deben tener configuraciones de ciclo de vida
- SageMaker Los modelos [SageMaker.16] deben usar un registro privado en la VPC para los contenedores principales
- [WAF.1]AWS WAFEl registro de ACL web global clásico debe estar habilitado
- [WAF.6]AWS WAFLas reglas globales clásicas deben tener al menos una condición

- [WAF.7]AWS WAFLos grupos de reglas globales clásicos deben tener al menos una regla
- [WAF.8]AWS WAFLas ACL web globales clásicas deben tener al menos una regla o grupo de reglas

Europa (Irlanda)

Los siguientes controles no se admiten en la región Europa (Irlanda).

- [AppSync.1]AWS AppSyncLas cachés de las API deben estar cifradas en reposo
- [AppSync.6]AWS AppSyncLas cachés de las API deben cifrarse en tránsito
- [CloudFront.1] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado
- [CloudFront.3] CloudFront las distribuciones deben requerir el cifrado durante el tránsito
- [CloudFront.4] CloudFront las distribuciones deben tener configurada la conmutación por error de origen
- [CloudFront.5] CloudFront las distribuciones deben tener habilitado el registro
- [CloudFront.6] CloudFront las distribuciones deben tener WAF activado
- [CloudFront.7] CloudFront las distribuciones deben usar certificados personalizados SSL/TLS
- [CloudFront.8] CloudFront las distribuciones deben usar el SNI para atender las solicitudes HTTPS
- [CloudFront.9] CloudFront las distribuciones deben cifrar el tráfico para convertirlo en orígenes personalizados
- [CloudFront.10] CloudFront las distribuciones no deben usar protocolos SSL obsoletos entre ubicaciones de borde y orígenes personalizados
- [CloudFront.12] CloudFront las distribuciones no deben apuntar a orígenes de S3 inexistentes
- [CloudFront.13] CloudFront las distribuciones deben usar el control de acceso al origen
- [CloudFront.14] CloudFront las distribuciones deben estar etiquetadas
- [CloudFront.15] CloudFront las distribuciones deben usar la política de seguridad TLS recomendada
- [CloudFront.16] CloudFront las distribuciones deben usar el control de acceso de origen para los orígenes de las URL de las funciones de Lambda
- [CloudFront.17] CloudFront las distribuciones deben usar grupos de claves confiables para las URL y cookies firmadas

- [Connect.1] Los tipos de objetos de los perfiles de clientes de Amazon Connect deben estar etiquetados
- [Connect.2] Las instancias de Connect Customer deben tener el CloudWatch registro habilitado
- [ECR.4] Los repositorios públicos de ECR deben etiquetarse
- [GlobalAccelerator.1] Los aceleradores de Global Accelerator deben estar etiquetados
- [IAM.26] SSL/TLS Los certificados caducados gestionados en IAM deben eliminarse
- [Route53.1] Los controles de salud de Route 53 deben estar etiquetados
- [Route53.2] Las zonas alojadas públicas de Route 53 deberían registrar las consultas de DNS
- [S3.24] Los puntos de Multi-Region acceso S3 deben tener habilitada la configuración de bloqueo del acceso público
- [WAF.1]AWS WAFEl registro de ACL web global clásico debe estar habilitado
- [WAF.6]AWS WAFLas reglas globales clásicas deben tener al menos una condición
- [WAF.7]AWS WAFLos grupos de reglas globales clásicos deben tener al menos una regla
- [WAF.8]AWS WAFLas ACL web globales clásicas deben tener al menos una regla o grupo de reglas

Europa (Londres)

Los siguientes controles no se admiten en la región Europa (Londres).

- [AppRunner.2] Los conectores VPC de App Runner deben estar etiquetados
- [AppSync.1]AWS AppSyncLas cachés de las API deben estar cifradas en reposo
- [AppSync.6]AWS AppSyncLas cachés de las API deben cifrarse en tránsito
- [BedrockAgentCore.3] Bedrock AgentCore Memory debe estar cifrada y gestionada por el clienteAWS KMSclaves
- [CloudFront.1] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado
- [CloudFront.3] CloudFront las distribuciones deben requerir el cifrado durante el tránsito
- [CloudFront.4] CloudFront las distribuciones deben tener configurada la conmutación por error de origen
- [CloudFront.5] CloudFront las distribuciones deben tener habilitado el registro
- [CloudFront.6] CloudFront las distribuciones deben tener WAF activado

- [CloudFront.7] CloudFront las distribuciones deben usar certificados personalizados SSL/TLS
- [CloudFront.8] CloudFront las distribuciones deben usar el SNI para atender las solicitudes HTTPS
- [CloudFront.9] CloudFront las distribuciones deben cifrar el tráfico para convertirlo en orígenes personalizados
- [CloudFront.10] CloudFront las distribuciones no deben usar protocolos SSL obsoletos entre ubicaciones de borde y orígenes personalizados
- [CloudFront.12] CloudFront las distribuciones no deben apuntar a orígenes de S3 inexistentes
- [CloudFront.13] CloudFront las distribuciones deben usar el control de acceso al origen
- [CloudFront.14] CloudFront las distribuciones deben estar etiquetadas
- [CloudFront.15] CloudFront las distribuciones deben usar la política de seguridad TLS recomendada
- [CloudFront.16] CloudFront las distribuciones deben usar el control de acceso de origen para los orígenes de las URL de las funciones de Lambda
- [CloudFront.17] CloudFront las distribuciones deben usar grupos de claves confiables para las URL y cookies firmadas
- [EC2.24] No se deben utilizar los tipos de instancias paravirtuales de Amazon EC2
- [EC2.173] Las solicitudes de EC2 Spot Fleet con parámetros de lanzamiento deberían permitir el cifrado de los volúmenes de EBS adjuntos
- [ECR.4] Los repositorios públicos de ECR deben etiquetarse
- [FraudDetector.1] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.2] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas
- [FraudDetector.3] Los resultados de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.4] Las variables de Amazon Fraud Detector deben estar etiquetadas
- [GlobalAccelerator.1] Los aceleradores de Global Accelerator deben estar etiquetados
- [IAM.26] SSL/TLS Los certificados caducados gestionados en IAM deben eliminarse
- [IoTSiteWise.1]AWSLos modelos SiteWise de activos de IoT deben estar etiquetados
- [IoTSiteWise.2]AWS SiteWise Los paneles de IoT deben estar etiquetados
- [IoTSiteWise.3]AWS SiteWise Las pasarelas de IoT deben estar etiquetadas
- [IoTSiteWise.4]AWS SiteWise Los portales de IoT deben estar etiquetados
- [IoTSiteWise.5]AWS SiteWise Los proyectos de IoT deben estar etiquetados

- [IoTTwinMaker.1]AWSLos trabajos de TwinMaker sincronización de IoT deben estar etiquetados
- [IoTTwinMaker.2]AWS TwinMaker Los espacios de trabajo de IoT deben estar etiquetados
- [IoTTwinMaker.3]AWS TwinMaker Las escenas de IoT deben estar etiquetadas
- [IoTTwinMaker.4]AWS TwinMaker Las entidades de IoT deben estar etiquetadas
- [IoTWireless.1]AWSLos grupos de multidifusión de IoT Wireless deben estar etiquetados
- [IoTWireless.2]AWSLos perfiles de servicio de IoT Wireless deben estar etiquetados
- [IoTWireless.3]AWSLas tareas de IoT FUOTA deben estar etiquetadas
- [IVS.1] Los pares de teclas de reproducción IVS deben estar etiquetados
- [IVS.2] Las configuraciones de grabación de IVS deben estar etiquetadas
- [IVS.3] Los canales IVS deben estar etiquetados
- [RDS.31] Los grupos de seguridad de la base de datos de RDS deben etiquetarse
- [Route53.1] Los controles de salud de Route 53 deben estar etiquetados
- [Route53.2] Las zonas alojadas públicas de Route 53 deberían registrar las consultas de DNS
- [S3.24] Los puntos de Multi-Region acceso S3 deben tener habilitada la configuración de bloqueo del acceso público
- [S3.25] Los buckets de directorio de S3 deben tener configuraciones de ciclo de vida
- [SageMaker.19] SageMaker los modelos deben usar un registro privado en la VPC para las canalizaciones de inferencia de varios contenedores
- [WAF.1]AWS WAFEl registro de ACL web global clásico debe estar habilitado
- [WAF.6]AWS WAFLas reglas globales clásicas deben tener al menos una condición
- [WAF.7]AWS WAFLos grupos de reglas globales clásicos deben tener al menos una regla
- [WAF.8]AWS WAFLas ACL web globales clásicas deben tener al menos una regla o grupo de reglas

Europa (Milán)

Los siguientes controles no se admiten en la región Europa (Milán).

- [APIGateway.11] Los nombres de dominio de API Gateway deben usar las políticas de seguridad recomendadas
- [AppFlow.1] AppFlow Los flujos de Amazon deben estar etiquetados

- [AppRunner.1] Los servicios de App Runner deben estar etiquetados
- [AppRunner.2] Los conectores VPC de App Runner deben estar etiquetados
- [AppSync.1]AWS AppSyncLas cachés de las API deben estar cifradas en reposo
- [AppSync.6]AWS AppSyncLas cachés de las API deben cifrarse en tránsito
- [BedrockAgentCore.1] Los AgentCore tiempos de ejecución de Bedrock deben configurarse con el modo de red VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways debería requerir autorización para las solicitudes entrantes
- [BedrockAgentCore.3] Bedrock AgentCore Memory debe estar cifrada y gestionada por el clienteAWS KMSclaves
- [BedrockAgentCore.4] Bedrock AgentCore Gateway debe cifrarse de forma que sea gestionada por el clienteAWS KMSclaves
- [BedrockAgentCore.5] Los navegadores AgentCore personalizados de Bedrock no deberían usar el modo de red pública
- [BedrockAgentCore.6] Los navegadores AgentCore personalizados de Bedrock deberían tener habilitada la grabación de sesiones
- [CloudFront.1] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado
- [CloudFront.3] CloudFront las distribuciones deben requerir el cifrado durante el tránsito
- [CloudFront.4] CloudFront las distribuciones deben tener configurada la conmutación por error de origen
- [CloudFront.5] CloudFront las distribuciones deben tener habilitado el registro
- [CloudFront.6] CloudFront las distribuciones deben tener WAF activado
- [CloudFront.7] CloudFront las distribuciones deben usar certificados personalizados SSL/TLS
- [CloudFront.8] CloudFront las distribuciones deben usar el SNI para atender las solicitudes HTTPS
- [CloudFront.9] CloudFront las distribuciones deben cifrar el tráfico para convertirlo en orígenes personalizados
- [CloudFront.10] CloudFront las distribuciones no deben usar protocolos SSL obsoletos entre ubicaciones de borde y orígenes personalizados
- [CloudFront.12] CloudFront las distribuciones no deben apuntar a orígenes de S3 inexistentes
- [CloudFront.13] CloudFront las distribuciones deben usar el control de acceso al origen

- [CloudFront.14] CloudFront las distribuciones deben estar etiquetadas
- [CloudFront.15] CloudFront las distribuciones deben usar la política de seguridad TLS recomendada
- [CloudFront.16] CloudFront las distribuciones deben usar el control de acceso de origen para los orígenes de las URL de las funciones de Lambda
- [CloudFront.17] CloudFront las distribuciones deben usar grupos de claves confiables para las URL y cookies firmadas
- [CodeGuruProfiler.1] Los grupos CodeGuru de creación de perfiles de Profiler deben estar etiquetados
- [CodeGuruReviewer.1] Las asociaciones de repositorios de CodeGuru Reviewer deben estar etiquetadas
- [Connect.1] Los tipos de objetos de los perfiles de clientes de Amazon Connect deben estar etiquetados
- [Connect.2] Las instancias de Connect Customer deben tener el CloudWatch registro habilitado
- [DMS.10] Los puntos finales de DMS para las bases de datos de Neptune deben tener habilitada la autorización de IAM
- [DynamoDB.3] Los clústeres de DynamoDB Accelerator (DAX) deben cifrarse en reposo
- [DynamoDB.7] Los clústeres de DynamoDB Accelerator deben cifrarse en tránsito
- [EC2.4] Las instancias EC2 detenidas deben eliminarse después de un período de tiempo específico
- [EC2.14] Los grupos de seguridad no deberían permitir la entrada desde la versión 0.0.0. 0/0 o: :/0 al puerto 3389
- [EC2.24] No se deben utilizar los tipos de instancias paravirtuales de Amazon EC2
- [EC2.58] Las VPC deben configurarse con un punto final de interfaz para los contactos de Systems Manager Incident Manager
- [EC2.60] Las VPC deben configurarse con un punto final de interfaz para Systems Manager Incident Manager
- [EC2.173] Las solicitudes de EC2 Spot Fleet con parámetros de lanzamiento deberían permitir el cifrado de los volúmenes de EBS adjuntos
- [EC2.177] Las sesiones de réplica de tráfico de EC2 deben etiquetarse
- [ECR.4] Los repositorios públicos de ECR deben etiquetarse

- [ELB.2] Los balanceadores de carga clásicos con SSL/HTTPS oyentes deben usar un certificado proporcionado por AWS Gestor de certificados
- [EventBridge.4] los puntos finales EventBridge globales deberían tener habilitada la replicación de eventos
- [FraudDetector.1] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.2] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas
- [FraudDetector.3] Los resultados de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.4] Las variables de Amazon Fraud Detector deben estar etiquetadas
- [GlobalAccelerator.1] Los aceleradores de Global Accelerator deben estar etiquetados
- [IAM.18] Asegúrese de que se haya creado una función de soporte para gestionar los incidentes conAWS Support
- [IAM.26] SSL/TLS Los certificados caducados gestionados en IAM deben eliminarse
- [Inspector.3] El escaneo de código Lambda de Amazon Inspector Lambda debe estar activado
- [IoT.1]AWS IoT Device Defenderlos perfiles de seguridad deben estar etiquetados
- [IoT.2]AWS IoT Corelas acciones de mitigación deben estar etiquetadas
- [IoT.3]AWS IoT Corelas dimensiones deben estar etiquetadas
- [IoT.4]AWS IoT Corelos autorizadores deben estar etiquetados
- [IoT.5]AWS IoT CoreLos alias de los roles deben estar etiquetados
- [IoT.6]AWS IoT Corelas políticas deben estar etiquetadas
- [IoTSiteWise.1]AWSLos modelos SiteWise de activos de IoT deben estar etiquetados
- [IoTSiteWise.2]AWS SiteWise Los paneles de IoT deben estar etiquetados
- [IoTSiteWise.3]AWS SiteWise Las pasarelas de IoT deben estar etiquetadas
- [IoTSiteWise.4]AWS SiteWise Los portales de IoT deben estar etiquetados
- [IoTSiteWise.5]AWS SiteWise Los proyectos de IoT deben estar etiquetados
- [IoTTwinMaker.1]AWSLos trabajos de TwinMaker sincronización de IoT deben estar etiquetados
- [IoTTwinMaker.2]AWS TwinMaker Los espacios de trabajo de IoT deben estar etiquetados
- [IoTTwinMaker.3]AWS TwinMaker Las escenas de IoT deben estar etiquetadas
- [IoTTwinMaker.4]AWS TwinMaker Las entidades de IoT deben estar etiquetadas
- [IoTWireless.1]AWSLos grupos de multidifusión de IoT Wireless deben estar etiquetados

- [IoTWireless.2]AWSLos perfiles de servicio de IoT Wireless deben estar etiquetados
- [IoTWireless.3]AWSLas tareas de IoT FUOTA deben estar etiquetadas
- [IVS.1] Los pares de teclas de reproducción IVS deben estar etiquetados
- [IVS.2] Las configuraciones de grabación de IVS deben estar etiquetadas
- [IVS.3] Los canales IVS deben estar etiquetados
- [Keyspaces.1] Los espacios clave de Amazon Keyspaces deben estar etiquetados
- [MSK.3] Los conectores MSK Connect deben estar cifrados en tránsito
- [MSK.5] Los conectores MSK deben tener el registro activado
- [Neptune.1] Los clústeres de bases de datos de Neptune deben cifrarse en reposo
- [Neptune.2] Los clústeres de bases de datos de Neptune deberían publicar registros de auditoría en Logs CloudWatch
- [Neptune.3] Las instantáneas del clúster de base de datos de Neptune no deben ser públicas
- [Neptune.4] Los clústeres de base de datos de Neptune deben tener habilitada la protección contra eliminación
- [Neptune.5] Los clústeres de Neptune DB deberían tener habilitadas las copias de seguridad automatizadas
- [Neptune.6] Las instantáneas del clúster de base de datos de Neptune deben cifrarse en reposo
- [Neptune.7] Los clústeres de base de datos de Neptune deben tener habilitada la autenticación de bases de datos de IAM
- [Neptune.8] Los clústeres de bases de datos de Neptune deben configurarse para copiar etiquetas a las instantáneas
- [Neptune.9] Los clústeres de base de datos Neptune deben implementarse en varias zonas de disponibilidad
- [RDS.1] La instantánea de RDS debe ser privada
- [RDS.14] Los clústeres de Amazon Aurora deben tener habilitado el retroceso
- [RDS.31] Los grupos de seguridad de la base de datos de RDS deben etiquetarse
- [RedshiftServerless.1] Los grupos de trabajo sin servidor de Amazon Redshift deberían utilizar un enrutamiento de VPC mejorado
- [RedshiftServerless.2] Las conexiones a los grupos de trabajo sin servidor de Redshift deberían ser obligatorias para usar SSL

- [RedshiftServerless.3] Los grupos de trabajo sin servidor de Redshift deberían prohibir el acceso público
- [RedshiftServerless.4] Los espacios de nombres de Redshift Serverless deben cifrarse y administrarse por el clienteAWS KMS keys
- [RedshiftServerless.5] Los espacios de nombres Redshift Serverless no deben usar el nombre de usuario de administrador predeterminado
- [RedshiftServerless.6] Los espacios de nombres Redshift Serverless deberían exportar los registros a los registros CloudWatch
- [Route53.1] Los controles de salud de Route 53 deben estar etiquetados
- [Route53.2] Las zonas alojadas públicas de Route 53 deberían registrar las consultas de DNS
- [S3.24] Los puntos de Multi-Region acceso S3 deben tener habilitada la configuración de bloqueo del acceso público
- [S3.25] Los buckets de directorio de S3 deben tener configuraciones de ciclo de vida
- [SageMaker.9] las definiciones de trabajos de calidad de los SageMaker datos deben tener habilitado el cifrado del tráfico entre contenedores
- [SageMaker.10] Las definiciones de trabajos de explicabilidad del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores
- [SageMaker.11] las definiciones de trabajos SageMaker de calidad de los datos deben tener habilitado el aislamiento de red
- [SageMaker.12] las definiciones de trabajo basadas en el sesgo del SageMaker modelo deben tener habilitado el aislamiento de red
- [SageMaker.13] las definiciones de trabajos de calidad del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores
- [SageMaker.14] los programas SageMaker de monitoreo deben tener habilitado el aislamiento de la red
- [SageMaker.15] Las definiciones de trabajo basadas en el sesgo del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores
- [SSM.2] Las instancias de Amazon EC2 administradas por Systems Manager deben tener el estado de conformidad con los parches de CONFORMIDAD CON LOS PARCHES tras la instalación de un parche
- [WAF.1]AWS WAFEl registro de ACL web global clásico debe estar habilitado
- [WAF.6]AWS WAFLas reglas globales clásicas deben tener al menos una condición

- [WAF.7]AWS WAFLos grupos de reglas globales clásicos deben tener al menos una regla
- [WAF.8]AWS WAFLas ACL web globales clásicas deben tener al menos una regla o grupo de reglas
- [WorkSpaces.1] los volúmenes de WorkSpaces usuarios deben cifrarse en reposo
- [WorkSpaces.2] los volúmenes WorkSpaces raíz deben cifrarse en reposo

Europa (París)

Los siguientes controles no se admiten en la región Europa (París).

- [AppSync.1]AWS AppSyncLas cachés de las API deben estar cifradas en reposo
- [AppSync.6]AWS AppSyncLas cachés de las API deben cifrarse en tránsito
- [BedrockAgentCore.3] Bedrock AgentCore Memory debe estar cifrada y gestionada por el clienteAWS KMSclaves
- [CloudFront.1] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado
- [CloudFront.3] CloudFront las distribuciones deben requerir el cifrado durante el tránsito
- [CloudFront.4] CloudFront las distribuciones deben tener configurada la conmutación por error de origen
- [CloudFront.5] CloudFront las distribuciones deben tener habilitado el registro
- [CloudFront.6] CloudFront las distribuciones deben tener WAF activado
- [CloudFront.7] CloudFront las distribuciones deben usar certificados personalizados SSL/TLS
- [CloudFront.8] CloudFront las distribuciones deben usar el SNI para atender las solicitudes HTTPS
- [CloudFront.9] CloudFront las distribuciones deben cifrar el tráfico para convertirlo en orígenes personalizados
- [CloudFront.10] CloudFront las distribuciones no deben usar protocolos SSL obsoletos entre ubicaciones de borde y orígenes personalizados
- [CloudFront.12] CloudFront las distribuciones no deben apuntar a orígenes de S3 inexistentes
- [CloudFront.13] CloudFront las distribuciones deben usar el control de acceso al origen
- [CloudFront.14] CloudFront las distribuciones deben estar etiquetadas
- [CloudFront.15] CloudFront las distribuciones deben usar la política de seguridad TLS recomendada

- [CloudFront.16] CloudFront las distribuciones deben usar el control de acceso de origen para los orígenes de las URL de las funciones de Lambda
- [CloudFront.17] CloudFront las distribuciones deben usar grupos de claves confiables para las URL y cookies firmadas
- [CodeGuruProfiler.1] Los grupos CodeGuru de creación de perfiles de Profiler deben estar etiquetados
- [CodeGuruReviewer.1] Las asociaciones de repositorios de CodeGuru Reviewer deben estar etiquetadas
- [Connect.1] Los tipos de objetos de los perfiles de clientes de Amazon Connect deben estar etiquetados
- [Connect.2] Las instancias de Connect Customer deben tener el CloudWatch registro habilitado
- [DMS.13] Las instancias de replicación de DMS deben configurarse para usar varias zonas de disponibilidad
- [EC2.24] No se deben utilizar los tipos de instancias paravirtuales de Amazon EC2
- [EC2.173] Las solicitudes de EC2 Spot Fleet con parámetros de lanzamiento deberían permitir el cifrado de los volúmenes de EBS adjuntos
- [ECR.4] Los repositorios públicos de ECR deben etiquetarse
- [FraudDetector.1] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.2] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas
- [FraudDetector.3] Los resultados de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.4] Las variables de Amazon Fraud Detector deben estar etiquetadas
- [FSx.5] Los sistemas de archivos FSx for Windows File Server deben configurarse para Multi-AZ su implementación
- [GlobalAccelerator.1] Los aceleradores de Global Accelerator deben estar etiquetados
- [IAM.26] SSL/TLS Los certificados caducados gestionados en IAM deben eliminarse
- [Inspector.3] El escaneo de código Lambda de Amazon Inspector Lambda debe estar activado
- [IoTSiteWise.1]AWSLos modelos SiteWise de activos de IoT deben estar etiquetados
- [IoTSiteWise.2]AWS SiteWise Los paneles de IoT deben estar etiquetados
- [IoTSiteWise.3]AWS SiteWise Las pasarelas de IoT deben estar etiquetadas
- [IoTSiteWise.4]AWS SiteWise Los portales de IoT deben estar etiquetados

- [IoTSiteWise.5]AWS SiteWise Los proyectos de IoT deben estar etiquetados
- [IoTTwinMaker.1]AWSLos trabajos de TwinMaker sincronización de IoT deben estar etiquetados
- [IoTTwinMaker.2]AWS TwinMaker Los espacios de trabajo de IoT deben estar etiquetados
- [IoTTwinMaker.3]AWS TwinMaker Las escenas de IoT deben estar etiquetadas
- [IoTTwinMaker.4]AWS TwinMaker Las entidades de IoT deben estar etiquetadas
- [IoTWireless.1]AWSLos grupos de multidifusión de IoT Wireless deben estar etiquetados
- [IoTWireless.2]AWSLos perfiles de servicio de IoT Wireless deben estar etiquetados
- [IoTWireless.3]AWSLas tareas de IoT FUOTA deben estar etiquetadas
- [IVS.1] Los pares de teclas de reproducción IVS deben estar etiquetados
- [IVS.2] Las configuraciones de grabación de IVS deben estar etiquetadas
- [IVS.3] Los canales IVS deben estar etiquetados
- [RDS.31] Los grupos de seguridad de la base de datos de RDS deben etiquetarse
- [Route53.1] Los controles de salud de Route 53 deben estar etiquetados
- [Route53.2] Las zonas alojadas públicas de Route 53 deberían registrar las consultas de DNS
- [S3.24] Los puntos de Multi-Region acceso S3 deben tener habilitada la configuración de bloqueo del acceso público
- [S3.25] Los buckets de directorio de S3 deben tener configuraciones de ciclo de vida
- [SageMaker.19] SageMaker los modelos deben usar un registro privado en la VPC para las canalizaciones de inferencia de varios contenedores
- [WAF.1]AWS WAFEl registro de ACL web global clásico debe estar habilitado
- [WAF.6]AWS WAFLas reglas globales clásicas deben tener al menos una condición
- [WAF.7]AWS WAFLos grupos de reglas globales clásicos deben tener al menos una regla
- [WAF.8]AWS WAFLas ACL web globales clásicas deben tener al menos una regla o grupo de reglas
- [WorkSpaces.1] los volúmenes de WorkSpaces usuarios deben cifrarse en reposo
- [WorkSpaces.2] los volúmenes WorkSpaces raíz deben cifrarse en reposo

Europa (España)

Los siguientes controles no se admiten en la región Europa (España).

- [Account.2]Cuentas de AWSdebe formar parte de unAWS Organizationsorganización
- [APIGateway.8] Las rutas de API Gateway deben especificar un tipo de autorización
- [APIGateway.9] El registro de acceso debe configurarse para las etapas V2 de API Gateway
- [Amplify.1] Las aplicaciones Amplify deben estar etiquetadas
- [Amplify.2] Amplify branches debe estar etiquetado
- [AppConfig.1]AWS AppConfiglas aplicaciones deben estar etiquetadas
- [AppConfig.2]AWS AppConfiglos perfiles de configuración deben estar etiquetados
- [AppConfig.3]AWS AppConfiglos entornos deben estar etiquetados
- [AppFlow.1] AppFlow Los flujos de Amazon deben estar etiquetados
- [AppRunner.1] Los servicios de App Runner deben estar etiquetados
- [AppRunner.2] Los conectores VPC de App Runner deben estar etiquetados
- [AppSync.1]AWS AppSyncLas cachés de las API deben estar cifradas en reposo
- [AppSync.6]AWS AppSyncLas cachés de las API deben cifrarse en tránsito
- [Backup.1]AWS Backuplos puntos de recuperación deben estar cifrados en reposo
- [BedrockAgentCore.1] Los AgentCore tiempos de ejecución de Bedrock deben configurarse con el modo de red VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways debería requerir autorización para las solicitudes entrantes
- [BedrockAgentCore.3] Bedrock AgentCore Memory debe estar cifrada y gestionada por el clienteAWS KMSclaves
- [BedrockAgentCore.4] Bedrock AgentCore Gateway debe cifrarse de forma que sea gestionada por el clienteAWS KMSclaves
- [BedrockAgentCore.5] Los navegadores AgentCore personalizados de Bedrock no deberían usar el modo de red pública
- [BedrockAgentCore.6] Los navegadores AgentCore personalizados de Bedrock deberían tener habilitada la grabación de sesiones
- [CloudFormation.3] las CloudFormation pilas deben tener habilitada la protección de terminación
- [CloudFormation.4] las CloudFormation pilas deben tener funciones de servicio asociadas
- [CloudFront.1] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado

- [CloudFront.3] CloudFront las distribuciones deben requerir el cifrado durante el tránsito
- [CloudFront.4] CloudFront las distribuciones deben tener configurada la conmutación por error de origen
- [CloudFront.5] CloudFront las distribuciones deben tener habilitado el registro
- [CloudFront.6] CloudFront las distribuciones deben tener WAF activado
- [CloudFront.7] CloudFront las distribuciones deben usar certificados personalizados SSL/TLS
- [CloudFront.8] CloudFront las distribuciones deben usar el SNI para atender las solicitudes HTTPS
- [CloudFront.9] CloudFront las distribuciones deben cifrar el tráfico para convertirlo en orígenes personalizados
- [CloudFront.10] CloudFront las distribuciones no deben usar protocolos SSL obsoletos entre ubicaciones de borde y orígenes personalizados
- [CloudFront.12] CloudFront las distribuciones no deben apuntar a orígenes de S3 inexistentes
- [CloudFront.13] CloudFront las distribuciones deben usar el control de acceso al origen
- [CloudFront.14] CloudFront las distribuciones deben estar etiquetadas
- [CloudFront.15] CloudFront las distribuciones deben usar la política de seguridad TLS recomendada
- [CloudFront.16] CloudFront las distribuciones deben usar el control de acceso de origen para los orígenes de las URL de las funciones de Lambda
- [CloudFront.17] CloudFront las distribuciones deben usar grupos de claves confiables para las URL y cookies firmadas
- [CodeArtifact.1] CodeArtifact los repositorios deben estar etiquetados
- [CodeGuruProfiler.1] Los grupos CodeGuru de creación de perfiles de Profiler deben estar etiquetados
- [CodeGuruReviewer.1] Las asociaciones de repositorios de CodeGuru Reviewer deben estar etiquetadas
- [Cognito.1] Los grupos de usuarios de Cognito deben tener activada la protección contra amenazas y el modo de aplicación con todas las funciones para la autenticación estándar
- [Cognito.2] Los grupos de identidades de Cognito no deben permitir identidades no autenticadas
- [Connect.1] Los tipos de objetos de los perfiles de clientes de Amazon Connect deben estar etiquetados
- [Connect.2] Las instancias de Connect Customer deben tener el CloudWatch registro habilitado

- [Detective.1] Los gráficos de comportamiento de los detectives deben estar etiquetados
- [DMS.2] Los certificados DMS deben estar etiquetados
- [DMS.3] Las suscripciones a eventos de DMS deben estar etiquetadas
- [DMS.4] Las instancias de replicación de DMS deben estar etiquetadas
- [DMS.5] Los grupos de subredes de replicación del DMS deben estar etiquetados
- [DMS.6] Las instancias de replicación de DMS deben tener habilitada la actualización automática de las versiones secundarias
- [DMS.7] Las tareas de replicación del DMS para la base de datos de destino deben tener el registro habilitado
- [DMS.8] Las tareas de replicación del DMS para la base de datos de origen deben tener el registro activado
- [DMS.9] Los puntos finales del DMS deben usar SSL
- [DMS.10] Los puntos finales de DMS para las bases de datos de Neptune deben tener habilitada la autorización de IAM
- [DMS.11] Los puntos finales de DMS para MongoDB deben tener un mecanismo de autenticación habilitado
- [DMS.12] Los puntos finales de DMS para Redis OSS deben tener el TLS habilitado
- [DMS.13] Las instancias de replicación de DMS deben configurarse para usar varias zonas de disponibilidad
- [DocumentDB.1] Los clústeres de Amazon DocumentDB deben cifrarse en reposo
- [DocumentDB.2] Los clústeres de Amazon DocumentDB deben tener un período de retención de copias de seguridad adecuado
- [DocumentDB.3] Las instantáneas de clústeres manuales de Amazon DocumentDB no deben ser públicas
- [DocumentDB.4] Los clústeres de Amazon DocumentDB deben publicar los registros de auditoría en Logs CloudWatch
- [DocumentDB.5] Los clústeres de Amazon DocumentDB deben tener habilitada la protección contra eliminaciones
- [DocumentDB.6] Los clústeres de Amazon DocumentDB deben cifrarse en tránsito
- [DynamoDB.3] Los clústeres de DynamoDB Accelerator (DAX) deben cifrarse en reposo
- [DynamoDB.7] Los clústeres de DynamoDB Accelerator deben cifrarse en tránsito

- [EC2.1] Las instantáneas de Amazon EBS no deben configurarse para que se puedan restaurar públicamente
- [EC2.4] Las instancias EC2 detenidas deben eliminarse después de un período de tiempo específico
- [EC2.14] Los grupos de seguridad no deberían permitir la entrada desde la versión 0.0.0. 0/0 o: :/0 al puerto 3389
- [EC2.22] Deben eliminarse los grupos de seguridad de Amazon EC2 no utilizados
- [EC2.24] No se deben utilizar los tipos de instancias paravirtuales de Amazon EC2
- [EC2.25] Las plantillas de lanzamiento de Amazon EC2 no deben asignar direcciones IP públicas a las interfaces de red
- [EC2.34] Las tablas de rutas de la pasarela de tránsito EC2 deben estar etiquetadas
- [EC2.40] Las pasarelas NAT EC2 deben estar etiquetadas
- [EC2.51] Los puntos finales EC2 Client VPN deben tener habilitado el registro de conexiones de clientes
- [EC2.58] Las VPC deben configurarse con un punto final de interfaz para los contactos de Systems Manager Incident Manager
- [EC2.60] Las VPC deben configurarse con un punto final de interfaz para Systems Manager Incident Manager
- [EC2.170] Las plantillas de lanzamiento de EC2 deben utilizar la versión 2 del servicio de metadatos de instancias (IMDSv2)
- [EC2.173] Las solicitudes de EC2 Spot Fleet con parámetros de lanzamiento deberían permitir el cifrado de los volúmenes de EBS adjuntos
- [EC2.175] Las plantillas de lanzamiento de EC2 deben estar etiquetadas
- [EC2.177] Las sesiones de réplica de tráfico de EC2 deben etiquetarse
- [EC2.179] Los objetivos del espejo de tráfico de EC2 deben estar etiquetados
- [EC2.180] Las interfaces de red EC2 deberían tener habilitada source/destination la verificación
- [EC2.181] Las plantillas de lanzamiento de EC2 deberían permitir el cifrado de los volúmenes de EBS adjuntos
- [ECR.4] Los repositorios públicos de ECR deben etiquetarse
- [EFS.1] Elastic File System debe configurarse para cifrar los datos de los archivos en reposo mediante AWS KMS

- [EFS.2] Los volúmenes de Amazon EFS deben figurar en los planes de copia de seguridad
- [ELB.2] Los balanceadores de carga clásicos con SSL/HTTPS oyentes deben usar un certificado proporcionado por AWS Gestor de certificados
- [ELB.14] El balanceador de carga clásico debe configurarse con el modo defensivo o de mitigación de desincronización más estricto
- [ELB.17] Los balanceadores de cargas de aplicaciones y redes con oyentes deben usar las políticas de seguridad recomendadas
- [ELB.18] Los oyentes del balanceador de cargas de red y aplicaciones deben usar protocolos seguros para cifrar los datos en tránsito
- [ElastiCache.1] ElastiCache (Redis OSS) los clústeres deben tener habilitadas las copias de seguridad automáticas
- [ElastiCache.6] ElastiCache (Redis OSS) Los grupos de replicación de versiones anteriores deberían tener habilitada la autenticación de Redis OSS
- [ElastiCache.7] los ElastiCache clústeres no deben usar el grupo de subredes predeterminado
- [ElasticBeanstalk.1] Los entornos de Elastic Beanstalk deberían tener habilitados los informes de estado mejorados
- [ElasticBeanstalk.2] Las actualizaciones de la plataforma gestionada de Elastic Beanstalk deben estar habilitadas
- [ElasticBeanstalk.3] Elastic Beanstalk debería transmitir los registros a CloudWatch
- [EMR.1] Los nodos principales del clúster de Amazon EMR no deben tener direcciones IP públicas
- [ES.4] Debería estar habilitado el registro de errores de dominio de Elasticsearch en Logs CloudWatch
- [EventBridge.4] los puntos finales EventBridge globales deberían tener habilitada la replicación de eventos
- [FraudDetector.1] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.2] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas
- [FraudDetector.3] Los resultados de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.4] Las variables de Amazon Fraud Detector deben estar etiquetadas
- [GlobalAccelerator.1] Los aceleradores de Global Accelerator deben estar etiquetados
- [Glue.4]AWS GlueLos trabajos de Spark deberían ejecutarse en versiones compatibles deAWS Glue

- GuardDuty Los filtros [GuardDuty.2] deben estar etiquetados
- [IAM.1] Las políticas de IAM no deberían permitir todos los privilegios administrativos «*»
- [IAM.2] Los usuarios de IAM no deberían tener políticas de IAM adjuntas
- [IAM.3] Las claves de acceso de los usuarios de IAM deben rotarse cada 90 días o menos
- [IAM.4] La clave de acceso del usuario raíz de IAM no debería existir
- [IAM.5] La MFA debe estar habilitada para todos los usuarios de IAM que tengan una contraseña de consola
- [IAM.8] Se deben eliminar las credenciales de usuario de IAM no utilizadas
- [IAM.18] Asegúrese de que se haya creado una función de soporte para gestionar los incidentes conAWS Support
- [IAM.19] La MFA debe estar habilitada para todos los usuarios de IAM
- [IAM.21] Las políticas de IAM gestionadas por el cliente que cree no deberían permitir acciones comodín en los servicios
- [IAM.22] Se deben eliminar las credenciales de usuario de IAM que no se hayan utilizado durante 45 días
- [IAM.24] Las funciones de IAM deben estar etiquetadas
- [IAM.25] Los usuarios de IAM deben estar etiquetados
- [IAM.26] SSL/TLS Los certificados caducados gestionados en IAM deben eliminarse
- [IAM.27] Las identidades de IAM no deberían tener la AWSCloudShellFullAccess política adjunta
- [Inspector.1] El escaneo EC2 de Amazon Inspector debe estar activado
- [Inspector.2] El escaneo ECR de Amazon Inspector debe estar activado
- [Inspector.3] El escaneo de código Lambda de Amazon Inspector Lambda debe estar activado
- [Inspector.4] El escaneo estándar de Amazon Inspector Lambda debe estar activado
- [IoTSiteWise.1]AWSLos modelos SiteWise de activos de IoT deben estar etiquetados
- [IoTSiteWise.2]AWS SiteWise Los paneles de IoT deben estar etiquetados
- [IoTSiteWise.3]AWS SiteWise Las pasarelas de IoT deben estar etiquetadas
- [IoTSiteWise.4]AWS SiteWise Los portales de IoT deben estar etiquetados
- [IoTSiteWise.5]AWS SiteWise Los proyectos de IoT deben estar etiquetados
- [IoTTwinMaker.1]AWSLos trabajos de TwinMaker sincronización de IoT deben estar etiquetados
- [IoTTwinMaker.2]AWS TwinMaker Los espacios de trabajo de IoT deben estar etiquetados

- [IoTTwinMaker.3]AWS TwinMaker Las escenas de IoT deben estar etiquetadas
- [IoTTwinMaker.4]AWS TwinMaker Las entidades de IoT deben estar etiquetadas
- [IoTWireless.1]AWSLos grupos de multidifusión de IoT Wireless deben estar etiquetados
- [IoTWireless.2]AWSLos perfiles de servicio de IoT Wireless deben estar etiquetados
- [IoTWireless.3]AWSLas tareas de IoT FUOTA deben estar etiquetadas
- [IVS.1] Los pares de teclas de reproducción IVS deben estar etiquetados
- [IVS.2] Las configuraciones de grabación de IVS deben estar etiquetadas
- [IVS.3] Los canales IVS deben estar etiquetados
- [Keyspaces.1] Los espacios clave de Amazon Keyspaces deben estar etiquetados
- [KMS.1] Las políticas gestionadas por los clientes de IAM no deberían permitir acciones de descifrado en todas las claves de KMS
- [KMS.2] Los directores de IAM no deberían tener políticas integradas de IAM que permitan realizar acciones de descifrado en todas las claves de KMS
- [Lambda.1] Las políticas de las funciones de Lambda deberían prohibir el acceso público
- [Lambda.7] Las funciones de Lambda deberían tener AWS X-Ray el rastreo activo está habilitado
- [Macie.1] Amazon Macie debería estar activado
- [Macie.2] La detección automática de datos confidenciales por parte de Macie debería estar habilitada
- [MQ.2] Los corredores de ActiveMQ deben transmitir los registros de auditoría a CloudWatch
- [MQ.4] Los corredores de Amazon MQ deben estar etiquetados
- [MQ.5] Los corredores de ActiveMQ deberían usar el modo de implementación active/standby
- [MQ.6] Los corredores de RabbitMQ deberían usar el modo de despliegue de clústeres
- [MSK.3] Los conectores MSK Connect deben estar cifrados en tránsito
- [MSK.4] Los clústeres de MSK deben tener el acceso público deshabilitado
- [MSK.5] Los conectores MSK deben tener el registro activado
- [MSK.6] Los clústeres de MSK deberían deshabilitar el acceso no autenticado
- [Neptune.1] Los clústeres de bases de datos de Neptune deben cifrarse en reposo
- [Neptune.2] Los clústeres de bases de datos de Neptune deberían publicar registros de auditoría en Logs CloudWatch
- [Neptune.3] Las instantáneas del clúster de base de datos de Neptune no deben ser públicas

- [Neptune.4] Los clústeres de base de datos de Neptune deben tener habilitada la protección contra eliminación
- [Neptune.5] Los clústeres de Neptune DB deberían tener habilitadas las copias de seguridad automatizadas
- [Neptune.6] Las instantáneas del clúster de base de datos de Neptune deben cifrarse en reposo
- [Neptune.7] Los clústeres de base de datos de Neptune deben tener habilitada la autenticación de bases de datos de IAM
- [Neptune.8] Los clústeres de bases de datos de Neptune deben configurarse para copiar etiquetas a las instantáneas
- [Neptune.9] Los clústeres de base de datos Neptune deben implementarse en varias zonas de disponibilidad
- [Opensearch.1] OpenSearch los dominios deben tener activado el cifrado en reposo
- [Opensearch.2] OpenSearch los dominios no deben ser de acceso público
- [Opensearch.3] OpenSearch los dominios deben cifrar los datos enviados entre nodos
- [Opensearch.4] El registro de errores de OpenSearch dominio en Logs debe estar habilitado CloudWatch
- [Opensearch.5] OpenSearch los dominios deben tener activado el registro de auditoría
- [Opensearch.6] OpenSearch los dominios deben tener al menos tres nodos de datos
- [Opensearch.7] OpenSearch los dominios deben tener habilitado un control de acceso detallado
- [Opensearch.8] Las conexiones a los OpenSearch dominios deben cifrarse con la última política de seguridad de TLS
- [Opensearch.9] OpenSearch los dominios deben estar etiquetados
- [Opensearch.10] OpenSearch los dominios deben tener instalada la última actualización de software
- [Opensearch.11] OpenSearch los dominios deben tener al menos tres nodos principales dedicados
- [RDS.1] La instantánea de RDS debe ser privada
- [RDS.14] Los clústeres de Amazon Aurora deben tener habilitado el retroceso
- [RDS.31] Los grupos de seguridad de la base de datos de RDS deben etiquetarse
- [RDS.35] Los clústeres de bases de datos de RDS deben tener habilitada la actualización automática de versiones secundarias
- [RDS.37] Los clústeres de bases de datos de Aurora PostgreSQL deben publicar los registros en Logs CloudWatch

- [Redshift.10] Los clústeres de Redshift deben cifrarse en reposo
- [Redshift.18] Los clústeres de Redshift deberían tener Multi-AZ las implementaciones habilitadas
- [Route53.1] Los controles de salud de Route 53 deben estar etiquetados
- [Route53.2] Las zonas alojadas públicas de Route 53 deberían registrar las consultas de DNS
- [S3.24] Los puntos de Multi-Region acceso S3 deben tener habilitada la configuración de bloqueo del acceso público
- [S3.25] Los buckets de directorio de S3 deben tener configuraciones de ciclo de vida
- [SageMaker.1] Las instancias de Amazon SageMaker Notebook no deberían tener acceso directo a Internet
- [SageMaker.2] las instancias de SageMaker cuadernos deben lanzarse en una VPC personalizada
- [SageMaker.3] Los usuarios no deben tener acceso root a las instancias de los SageMaker cuadernos
- SageMaker Los modelos [SageMaker.5] deben tener habilitado el aislamiento de red
- [SageMaker.9] las definiciones de trabajos de calidad de los SageMaker datos deben tener habilitado el cifrado del tráfico entre contenedores
- [SageMaker.10] Las definiciones de trabajos de explicabilidad del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores
- [SageMaker.11] las definiciones de trabajos SageMaker de calidad de los datos deben tener habilitado el aislamiento de red
- [SageMaker.12] las definiciones de trabajo basadas en el sesgo del SageMaker modelo deben tener habilitado el aislamiento de red
- [SageMaker.13] las definiciones de trabajos de calidad del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores
- [SageMaker.14] los programas SageMaker de monitoreo deben tener habilitado el aislamiento de la red
- [SageMaker.15] Las definiciones de trabajo basadas en el sesgo del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores
- SageMaker Los modelos [SageMaker.16] deben usar un registro privado en la VPC para los contenedores principales
- [SageMaker.19] SageMaker los modelos deben usar un registro privado en la VPC para las canalizaciones de inferencia de varios contenedores

- [SES.1] Las listas de contactos de SES deben estar etiquetadas
- [SES.2] Los conjuntos de configuración de SES deben estar etiquetados
- [SES.3] Los conjuntos de configuración de SES deben tener el TLS habilitado para enviar correos electrónicos
- [SQS.1] Las colas de Amazon SQS deben cifrarse en reposo
- [SQS.2] Las colas de SQS deben estar etiquetadas
- [SQS.3] Las políticas de acceso a las colas de SQS no deberían permitir el acceso público
- [SSM.6] SSM Automation debería tener el registro habilitado CloudWatch
- [SSM.7] Los documentos SSM deben tener habilitada la configuración de bloqueo para compartir en público
- [Transfer.3] Los conectores Transfer Family deben tener habilitado el registro
- [Transfer.4] Los acuerdos Transfer Family deben estar etiquetados
- [WAF.1]AWS WAFEl registro de ACL web global clásico debe estar habilitado
- [WAF.3]AWS WAFLos grupos de reglas regionales clásicos deben tener al menos una regla
- [WAF.6]AWS WAFLas reglas globales clásicas deben tener al menos una condición
- [WAF.7]AWS WAFLos grupos de reglas globales clásicos deben tener al menos una regla
- [WAF.8]AWS WAFLas ACL web globales clásicas deben tener al menos una regla o grupo de reglas
- [WAF.10]AWS WAFLas ACL web deben tener al menos una regla o grupo de reglas
- [WorkSpaces.1] los volúmenes de WorkSpaces usuarios deben cifrarse en reposo
- [WorkSpaces.2] los volúmenes WorkSpaces raíz deben cifrarse en reposo

Europa (Estocolmo)

Los siguientes controles no se admiten en la región Europa (Estocolmo).

- [AppFlow.1] AppFlow Los flujos de Amazon deben estar etiquetados
- [AppRunner.1] Los servicios de App Runner deben estar etiquetados
- [AppRunner.2] Los conectores VPC de App Runner deben estar etiquetados
- [AppSync.1]AWS AppSyncLas cachés de las API deben estar cifradas en reposo
- [AppSync.6]AWS AppSyncLas cachés de las API deben cifrarse en tránsito

- [BedrockAgentCore.3] Bedrock AgentCore Memory debe estar cifrada y gestionada por el clienteAWS KMSclaves
- [CloudFront.1] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado
- [CloudFront.3] CloudFront las distribuciones deben requerir el cifrado durante el tránsito
- [CloudFront.4] CloudFront las distribuciones deben tener configurada la conmutación por error de origen
- [CloudFront.5] CloudFront las distribuciones deben tener habilitado el registro
- [CloudFront.6] CloudFront las distribuciones deben tener WAF activado
- [CloudFront.7] CloudFront las distribuciones deben usar certificados personalizados SSL/TLS
- [CloudFront.8] CloudFront las distribuciones deben usar el SNI para atender las solicitudes HTTPS
- [CloudFront.9] CloudFront las distribuciones deben cifrar el tráfico para convertirlo en orígenes personalizados
- [CloudFront.10] CloudFront las distribuciones no deben usar protocolos SSL obsoletos entre ubicaciones de borde y orígenes personalizados
- [CloudFront.12] CloudFront las distribuciones no deben apuntar a orígenes de S3 inexistentes
- [CloudFront.13] CloudFront las distribuciones deben usar el control de acceso al origen
- [CloudFront.14] CloudFront las distribuciones deben estar etiquetadas
- [CloudFront.15] CloudFront las distribuciones deben usar la política de seguridad TLS recomendada
- [CloudFront.16] CloudFront las distribuciones deben usar el control de acceso de origen para los orígenes de las URL de las funciones de Lambda
- [CloudFront.17] CloudFront las distribuciones deben usar grupos de claves confiables para las URL y cookies firmadas
- [Connect.1] Los tipos de objetos de los perfiles de clientes de Amazon Connect deben estar etiquetados
- [Connect.2] Las instancias de Connect Customer deben tener el CloudWatch registro habilitado
- [DocumentDB.1] Los clústeres de Amazon DocumentDB deben cifrarse en reposo
- [DocumentDB.2] Los clústeres de Amazon DocumentDB deben tener un período de retención de copias de seguridad adecuado
- [DocumentDB.3] Las instantáneas de clústeres manuales de Amazon DocumentDB no deben ser públicas

- [DocumentDB.4] Los clústeres de Amazon DocumentDB deben publicar los registros de auditoría en Logs CloudWatch
- [DocumentDB.5] Los clústeres de Amazon DocumentDB deben tener habilitada la protección contra eliminaciones
- [DocumentDB.6] Los clústeres de Amazon DocumentDB deben cifrarse en tránsito
- [DynamoDB.3] Los clústeres de DynamoDB Accelerator (DAX) deben cifrarse en reposo
- [DynamoDB.7] Los clústeres de DynamoDB Accelerator deben cifrarse en tránsito
- [EC2.24] No se deben utilizar los tipos de instancias paravirtuales de Amazon EC2
- [EC2.173] Las solicitudes de EC2 Spot Fleet con parámetros de lanzamiento deberían permitir el cifrado de los volúmenes de EBS adjuntos
- [ECR.4] Los repositorios públicos de ECR deben etiquetarse
- [FraudDetector.1] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.2] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas
- [FraudDetector.3] Los resultados de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.4] Las variables de Amazon Fraud Detector deben estar etiquetadas
- [GlobalAccelerator.1] Los aceleradores de Global Accelerator deben estar etiquetados
- [IAM.26] SSL/TLS Los certificados caducados gestionados en IAM deben eliminarse
- [IoTSiteWise.1]AWSLos modelos SiteWise de activos de IoT deben estar etiquetados
- [IoTSiteWise.2]AWS SiteWise Los paneles de IoT deben estar etiquetados
- [IoTSiteWise.3]AWS SiteWise Las pasarelas de IoT deben estar etiquetadas
- [IoTSiteWise.4]AWS SiteWise Los portales de IoT deben estar etiquetados
- [IoTSiteWise.5]AWS SiteWise Los proyectos de IoT deben estar etiquetados
- [IoTTwinMaker.1]AWSLos trabajos de TwinMaker sincronización de IoT deben estar etiquetados
- [IoTTwinMaker.2]AWS TwinMaker Los espacios de trabajo de IoT deben estar etiquetados
- [IoTTwinMaker.3]AWS TwinMaker Las escenas de IoT deben estar etiquetadas
- [IoTTwinMaker.4]AWS TwinMaker Las entidades de IoT deben estar etiquetadas
- [IoTWireless.1]AWSLos grupos de multidifusión de IoT Wireless deben estar etiquetados
- [IoTWireless.2]AWSLos perfiles de servicio de IoT Wireless deben estar etiquetados
- [IoTWireless.3]AWSLas tareas de IoT FUOTA deben estar etiquetadas

- [IVS.1] Los pares de teclas de reproducción IVS deben estar etiquetados
- [IVS.2] Las configuraciones de grabación de IVS deben estar etiquetadas
- [IVS.3] Los canales IVS deben estar etiquetados
- [RDS.14] Los clústeres de Amazon Aurora deben tener habilitado el retroceso
- [RDS.31] Los grupos de seguridad de la base de datos de RDS deben etiquetarse
- [Route53.1] Los controles de salud de Route 53 deben estar etiquetados
- [Route53.2] Las zonas alojadas públicas de Route 53 deberían registrar las consultas de DNS
- [S3.24] Los puntos de Multi-Region acceso S3 deben tener habilitada la configuración de bloqueo del acceso público
- [SageMaker.12] las definiciones de trabajo basadas en el sesgo del SageMaker modelo deben tener habilitado el aislamiento de red
- [SageMaker.15] Las definiciones de trabajo basadas en el sesgo del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores
- [SageMaker.19] SageMaker los modelos deben usar un registro privado en la VPC para las canalizaciones de inferencia de varios contenedores
- [WAF.1]AWS WAFEl registro de ACL web global clásico debe estar habilitado
- [WAF.6]AWS WAFLas reglas globales clásicas deben tener al menos una condición
- [WAF.7]AWS WAFLos grupos de reglas globales clásicos deben tener al menos una regla
- [WAF.8]AWS WAFLas ACL web globales clásicas deben tener al menos una regla o grupo de reglas
- [WorkSpaces.1] los volúmenes de WorkSpaces usuarios deben cifrarse en reposo
- [WorkSpaces.2] los volúmenes WorkSpaces raíz deben cifrarse en reposo

Europa (Zúrich)

Los siguientes controles no se admiten en la región Europa (Zúrich).

- [APIGateway.8] Las rutas de API Gateway deben especificar un tipo de autorización
- [APIGateway.9] El registro de acceso debe configurarse para las etapas V2 de API Gateway
- [Amplify.1] Las aplicaciones Amplify deben estar etiquetadas
- [Amplify.2] Amplify branches debe estar etiquetado

- [AppConfig.1]AWS AppConfiglas aplicaciones deben estar etiquetadas
- [AppConfig.2]AWS AppConfiglos perfiles de configuración deben estar etiquetados
- [AppConfig.3]AWS AppConfiglos entornos deben estar etiquetados
- [AppFlow.1] AppFlow Los flujos de Amazon deben estar etiquetados
- [AppRunner.1] Los servicios de App Runner deben estar etiquetados
- [AppRunner.2] Los conectores VPC de App Runner deben estar etiquetados
- [AppSync.1]AWS AppSyncLas cachés de las API deben estar cifradas en reposo
- [AppSync.6]AWS AppSyncLas cachés de las API deben cifrarse en tránsito
- [Backup.1]AWS Backuplos puntos de recuperación deben estar cifrados en reposo
- [BedrockAgentCore.1] Los AgentCore tiempos de ejecución de Bedrock deben configurarse con el modo de red VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways debería requerir autorización para las solicitudes entrantes
- [BedrockAgentCore.3] Bedrock AgentCore Memory debe estar cifrada y gestionada por el clienteAWS KMSclaves
- [BedrockAgentCore.4] Bedrock AgentCore Gateway debe cifrarse de forma que sea gestionada por el clienteAWS KMSclaves
- [BedrockAgentCore.5] Los navegadores AgentCore personalizados de Bedrock no deberían usar el modo de red pública
- [BedrockAgentCore.6] Los navegadores AgentCore personalizados de Bedrock deberían tener habilitada la grabación de sesiones
- [CloudFormation.3] las CloudFormation pilas deben tener habilitada la protección de terminación
- [CloudFormation.4] las CloudFormation pilas deben tener funciones de servicio asociadas
- [CloudFront.1] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado
- [CloudFront.3] CloudFront las distribuciones deben requerir el cifrado durante el tránsito
- [CloudFront.4] CloudFront las distribuciones deben tener configurada la conmutación por error de origen
- [CloudFront.5] CloudFront las distribuciones deben tener habilitado el registro
- [CloudFront.6] CloudFront las distribuciones deben tener WAF activado
- [CloudFront.7] CloudFront las distribuciones deben usar certificados personalizados SSL/TLS

- [CloudFront.8] CloudFront las distribuciones deben usar el SNI para atender las solicitudes HTTPS
- [CloudFront.9] CloudFront las distribuciones deben cifrar el tráfico para convertirlo en orígenes personalizados
- [CloudFront.10] CloudFront las distribuciones no deben usar protocolos SSL obsoletos entre ubicaciones de borde y orígenes personalizados
- [CloudFront.12] CloudFront las distribuciones no deben apuntar a orígenes de S3 inexistentes
- [CloudFront.13] CloudFront las distribuciones deben usar el control de acceso al origen
- [CloudFront.14] CloudFront las distribuciones deben estar etiquetadas
- [CloudFront.15] CloudFront las distribuciones deben usar la política de seguridad TLS recomendada
- [CloudFront.16] CloudFront las distribuciones deben usar el control de acceso de origen para los orígenes de las URL de las funciones de Lambda
- [CloudFront.17] CloudFront las distribuciones deben usar grupos de claves confiables para las URL y cookies firmadas
- [CloudTrail.6] Asegúrese de que el depósito de S3 que se utiliza para almacenar CloudTrail los registros no sea de acceso público
- [CloudTrail.7] Asegúrese de que el registro de acceso al bucket de S3 esté habilitado en el CloudTrail bucket de S3
- [CodeArtifact.1] CodeArtifact los repositorios deben estar etiquetados
- [CodeGuruProfiler.1] Los grupos CodeGuru de creación de perfiles de Profiler deben estar etiquetados
- [CodeGuruReviewer.1] Las asociaciones de repositorios de CodeGuru Reviewer deben estar etiquetadas
- [Cognito.1] Los grupos de usuarios de Cognito deben tener activada la protección contra amenazas y el modo de aplicación con todas las funciones para la autenticación estándar
- [Cognito.2] Los grupos de identidades de Cognito no deben permitir identidades no autenticadas
- [Connect.1] Los tipos de objetos de los perfiles de clientes de Amazon Connect deben estar etiquetados
- [Connect.2] Las instancias de Connect Customer deben tener el CloudWatch registro habilitado
- [Detective.1] Los gráficos de comportamiento de los detectives deben estar etiquetados
- [DMS.2] Los certificados DMS deben estar etiquetados

- [DMS.3] Las suscripciones a eventos de DMS deben estar etiquetadas
- [DMS.4] Las instancias de replicación de DMS deben estar etiquetadas
- [DMS.5] Los grupos de subredes de replicación del DMS deben estar etiquetados
- [DMS.6] Las instancias de replicación de DMS deben tener habilitada la actualización automática de las versiones secundarias
- [DMS.7] Las tareas de replicación del DMS para la base de datos de destino deben tener el registro habilitado
- [DMS.8] Las tareas de replicación del DMS para la base de datos de origen deben tener el registro activado
- [DMS.9] Los puntos finales del DMS deben usar SSL
- [DMS.10] Los puntos finales de DMS para las bases de datos de Neptune deben tener habilitada la autorización de IAM
- [DMS.11] Los puntos finales de DMS para MongoDB deben tener un mecanismo de autenticación habilitado
- [DMS.12] Los puntos finales de DMS para Redis OSS deben tener el TLS habilitado
- [DMS.13] Las instancias de replicación de DMS deben configurarse para usar varias zonas de disponibilidad
- [DocumentDB.1] Los clústeres de Amazon DocumentDB deben cifrarse en reposo
- [DocumentDB.2] Los clústeres de Amazon DocumentDB deben tener un período de retención de copias de seguridad adecuado
- [DocumentDB.3] Las instantáneas de clústeres manuales de Amazon DocumentDB no deben ser públicas
- [DocumentDB.4] Los clústeres de Amazon DocumentDB deben publicar los registros de auditoría en Logs CloudWatch
- [DocumentDB.5] Los clústeres de Amazon DocumentDB deben tener habilitada la protección contra eliminaciones
- [DocumentDB.6] Los clústeres de Amazon DocumentDB deben cifrarse en tránsito
- [DynamoDB.3] Los clústeres de DynamoDB Accelerator (DAX) deben cifrarse en reposo
- [DynamoDB.7] Los clústeres de DynamoDB Accelerator deben cifrarse en tránsito
- [EC2.4] Las instancias EC2 detenidas deben eliminarse después de un período de tiempo específico

- [EC2.14] Los grupos de seguridad no deberían permitir la entrada desde la versión 0.0.0. 0/0 o: :/0 al puerto 3389
- [EC2.22] Deben eliminarse los grupos de seguridad de Amazon EC2 no utilizados
- [EC2.24] No se deben utilizar los tipos de instancias paravirtuales de Amazon EC2
- [EC2.25] Las plantillas de lanzamiento de Amazon EC2 no deben asignar direcciones IP públicas a las interfaces de red
- [EC2.58] Las VPC deben configurarse con un punto final de interfaz para los contactos de Systems Manager Incident Manager
- [EC2.60] Las VPC deben configurarse con un punto final de interfaz para Systems Manager Incident Manager
- [EC2.170] Las plantillas de lanzamiento de EC2 deben utilizar la versión 2 del servicio de metadatos de instancias (IMDSv2)
- [EC2.173] Las solicitudes de EC2 Spot Fleet con parámetros de lanzamiento deberían permitir el cifrado de los volúmenes de EBS adjuntos
- [EC2.175] Las plantillas de lanzamiento de EC2 deben estar etiquetadas
- [EC2.180] Las interfaces de red EC2 deberían tener habilitada source/destination la verificación
- [EC2.181] Las plantillas de lanzamiento de EC2 deberían permitir el cifrado de los volúmenes de EBS adjuntos
- [ECR.4] Los repositorios públicos de ECR deben etiquetarse
- [EFS.1] Elastic File System debe configurarse para cifrar los datos de los archivos en reposo mediante AWS KMS
- [EFS.2] Los volúmenes de Amazon EFS deben figurar en los planes de copia de seguridad
- [ELB.2] Los balanceadores de carga clásicos con SSL/HTTPS oyentes deben usar un certificado proporcionado por AWS Gestor de certificados
- [ELB.14] El balanceador de carga clásico debe configurarse con el modo defensivo o de mitigación de desincronización más estricto
- [ELB.17] Los balanceadores de cargas de aplicaciones y redes con oyentes deben usar las políticas de seguridad recomendadas
- [ELB.18] Los oyentes del balanceador de cargas de red y aplicaciones deben usar protocolos seguros para cifrar los datos en tránsito
- [ElastiCache.1] ElastiCache (Redis OSS) los clústeres deben tener habilitadas las copias de seguridad automáticas

- [ElastiCache.6] ElastiCache (Redis OSS) Los grupos de replicación de versiones anteriores deberían tener habilitada la autenticación de Redis OSS
- [ElastiCache.7] los ElastiCache clústeres no deben usar el grupo de subredes predeterminado
- [ElasticBeanstalk.1] Los entornos de Elastic Beanstalk deberían tener habilitados los informes de estado mejorados
- [ElasticBeanstalk.2] Las actualizaciones de la plataforma gestionada de Elastic Beanstalk deben estar habilitadas
- [ElasticBeanstalk.3] Elastic Beanstalk debería transmitir los registros a CloudWatch
- [EMR.1] Los nodos principales del clúster de Amazon EMR no deben tener direcciones IP públicas
- [ES.4] Debería estar habilitado el registro de errores de dominio de Elasticsearch en Logs CloudWatch
- [EventBridge.4] los puntos finales EventBridge globales deberían tener habilitada la replicación de eventos
- [FraudDetector.1] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.2] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas
- [FraudDetector.3] Los resultados de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.4] Las variables de Amazon Fraud Detector deben estar etiquetadas
- [GlobalAccelerator.1] Los aceleradores de Global Accelerator deben estar etiquetados
- [Glue.4]AWS GlueLos trabajos de Spark deberían ejecutarse en versiones compatibles deAWS Glue
- GuardDuty Los filtros [GuardDuty.2] deben estar etiquetados
- [IAM.1] Las políticas de IAM no deberían permitir todos los privilegios administrativos «*»
- [IAM.2] Los usuarios de IAM no deberían tener políticas de IAM adjuntas
- [IAM.3] Las claves de acceso de los usuarios de IAM deben rotarse cada 90 días o menos
- [IAM.4] La clave de acceso del usuario raíz de IAM no debería existir
- [IAM.5] La MFA debe estar habilitada para todos los usuarios de IAM que tengan una contraseña de consola
- [IAM.8] Se deben eliminar las credenciales de usuario de IAM no utilizadas
- [IAM.18] Asegúrese de que se haya creado una función de soporte para gestionar los incidentes conAWS Support
- [IAM.19] La MFA debe estar habilitada para todos los usuarios de IAM

- [IAM.21] Las políticas de IAM gestionadas por el cliente que cree no deberían permitir acciones comodín en los servicios
- [IAM.22] Se deben eliminar las credenciales de usuario de IAM que no se hayan utilizado durante 45 días
- [IAM.24] Las funciones de IAM deben estar etiquetadas
- [IAM.25] Los usuarios de IAM deben estar etiquetados
- [IAM.26] SSL/TLS Los certificados caducados gestionados en IAM deben eliminarse
- [IAM.27] Las identidades de IAM no deberían tener la AWSCloudShellFullAccess política adjunta
- [Inspector.3] El escaneo de código Lambda de Amazon Inspector Lambda debe estar activado
- [IoT.1]AWS IoT Device Defenderlos perfiles de seguridad deben estar etiquetados
- [IoT.2]AWS IoT Corelas acciones de mitigación deben estar etiquetadas
- [IoT.3]AWS IoT Corelas dimensiones deben estar etiquetadas
- [IoT.4]AWS IoT Corelos autorizadores deben estar etiquetados
- [IoT.5]AWS IoT CoreLos alias de los roles deben estar etiquetados
- [IoT.6]AWS IoT Corelas políticas deben estar etiquetadas
- [IoTSiteWise.1]AWSLos modelos SiteWise de activos de IoT deben estar etiquetados
- [IoTSiteWise.2]AWS SiteWise Los paneles de IoT deben estar etiquetados
- [IoTSiteWise.3]AWS SiteWise Las pasarelas de IoT deben estar etiquetadas
- [IoTSiteWise.4]AWS SiteWise Los portales de IoT deben estar etiquetados
- [IoTSiteWise.5]AWS SiteWise Los proyectos de IoT deben estar etiquetados
- [IoTTwinMaker.1]AWSLos trabajos de TwinMaker sincronización de IoT deben estar etiquetados
- [IoTTwinMaker.2]AWS TwinMaker Los espacios de trabajo de IoT deben estar etiquetados
- [IoTTwinMaker.3]AWS TwinMaker Las escenas de IoT deben estar etiquetadas
- [IoTTwinMaker.4]AWS TwinMaker Las entidades de IoT deben estar etiquetadas
- [IoTWireless.1]AWSLos grupos de multidifusión de IoT Wireless deben estar etiquetados
- [IoTWireless.2]AWSLos perfiles de servicio de IoT Wireless deben estar etiquetados
- [IoTWireless.3]AWSLas tareas de IoT FUOTA deben estar etiquetadas
- [IVS.1] Los pares de teclas de reproducción IVS deben estar etiquetados
- [IVS.2] Las configuraciones de grabación de IVS deben estar etiquetadas

- [IVS.3] Los canales IVS deben estar etiquetados
- [Keyspaces.1] Los espacios clave de Amazon Keyspaces deben estar etiquetados
- [KMS.1] Las políticas gestionadas por los clientes de IAM no deberían permitir acciones de descifrado en todas las claves de KMS
- [KMS.2] Los directores de IAM no deberían tener políticas integradas de IAM que permitan realizar acciones de descifrado en todas las claves de KMS
- [Lambda.7] Las funciones de Lambda deberían tener AWS X-Ray el rastreo activo está habilitado
- [Macie.1] Amazon Macie debería estar activado
- [Macie.2] La detección automática de datos confidenciales por parte de Macie debería estar habilitada
- [MQ.2] Los corredores de ActiveMQ deben transmitir los registros de auditoría a CloudWatch
- [MQ.4] Los corredores de Amazon MQ deben estar etiquetados
- [MQ.5] Los corredores de ActiveMQ deberían usar el modo de implementación active/standby
- [MQ.6] Los corredores de RabbitMQ deberían usar el modo de despliegue de clústeres
- [MSK.3] Los conectores MSK Connect deben estar cifrados en tránsito
- [MSK.4] Los clústeres de MSK deben tener el acceso público deshabilitado
- [MSK.5] Los conectores MSK deben tener el registro activado
- [MSK.6] Los clústeres de MSK deberían deshabilitar el acceso no autenticado
- [Neptune.1] Los clústeres de bases de datos de Neptune deben cifrarse en reposo
- [Neptune.2] Los clústeres de bases de datos de Neptune deberían publicar registros de auditoría en Logs CloudWatch
- [Neptune.3] Las instantáneas del clúster de base de datos de Neptune no deben ser públicas
- [Neptune.4] Los clústeres de base de datos de Neptune deben tener habilitada la protección contra eliminación
- [Neptune.5] Los clústeres de Neptune DB deberían tener habilitadas las copias de seguridad automatizadas
- [Neptune.6] Las instantáneas del clúster de base de datos de Neptune deben cifrarse en reposo
- [Neptune.7] Los clústeres de base de datos de Neptune deben tener habilitada la autenticación de bases de datos de IAM
- [Neptune.8] Los clústeres de bases de datos de Neptune deben configurarse para copiar etiquetas a las instantáneas

- [Neptune.9] Los clústeres de base de datos Neptune deben implementarse en varias zonas de disponibilidad
- [Opensearch.1] OpenSearch los dominios deben tener activado el cifrado en reposo
- [Opensearch.2] OpenSearch los dominios no deben ser de acceso público
- [Opensearch.3] OpenSearch los dominios deben cifrar los datos enviados entre nodos
- [Opensearch.4] El registro de errores de OpenSearch dominio en Logs debe estar habilitado CloudWatch
- [Opensearch.5] OpenSearch los dominios deben tener activado el registro de auditoría
- [Opensearch.6] OpenSearch los dominios deben tener al menos tres nodos de datos
- [Opensearch.7] OpenSearch los dominios deben tener habilitado un control de acceso detallado
- [Opensearch.8] Las conexiones a los OpenSearch dominios deben cifrarse con la última política de seguridad de TLS
- [Opensearch.9] OpenSearch los dominios deben estar etiquetados
- [Opensearch.10] OpenSearch los dominios deben tener instalada la última actualización de software
- [Opensearch.11] OpenSearch los dominios deben tener al menos tres nodos principales dedicados
- [RDS.1] La instantánea de RDS debe ser privada
- [RDS.14] Los clústeres de Amazon Aurora deben tener habilitado el retroceso
- [RDS.31] Los grupos de seguridad de la base de datos de RDS deben etiquetarse
- [RDS.35] Los clústeres de bases de datos de RDS deben tener habilitada la actualización automática de versiones secundarias
- [Redshift.18] Los clústeres de Redshift deberían tener Multi-AZ las implementaciones habilitadas
- [Route53.1] Los controles de salud de Route 53 deben estar etiquetados
- [Route53.2] Las zonas alojadas públicas de Route 53 deberían registrar las consultas de DNS
- [S3.24] Los puntos de Multi-Region acceso S3 deben tener habilitada la configuración de bloqueo del acceso público
- [S3.25] Los buckets de directorio de S3 deben tener configuraciones de ciclo de vida
- [SageMaker.1] Las instancias de Amazon SageMaker Notebook no deberían tener acceso directo a Internet
- [SageMaker.2] las instancias de SageMaker cuadernos deben lanzarse en una VPC personalizada

- [SageMaker.3] Los usuarios no deben tener acceso root a las instancias de los SageMaker cuadernos
- SageMaker Los modelos [SageMaker.5] deben tener habilitado el aislamiento de red
- [SageMaker.6] las configuraciones de imagen de la SageMaker aplicación deben estar etiquetadas
- [SageMaker.7] SageMaker las imágenes deben estar etiquetadas
- [SageMaker.9] las definiciones de trabajos de calidad de los SageMaker datos deben tener habilitado el cifrado del tráfico entre contenedores
- [SageMaker.10] Las definiciones de trabajos de explicabilidad del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores
- [SageMaker.11] las definiciones de trabajos SageMaker de calidad de los datos deben tener habilitado el aislamiento de red
- [SageMaker.12] las definiciones de trabajo basadas en el sesgo del SageMaker modelo deben tener habilitado el aislamiento de red
- [SageMaker.13] las definiciones de trabajos de calidad del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores
- [SageMaker.14] los programas SageMaker de monitoreo deben tener habilitado el aislamiento de la red
- [SageMaker.15] Las definiciones de trabajo basadas en el sesgo del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores
- SageMaker Los modelos [SageMaker.16] deben usar un registro privado en la VPC para los contenedores principales
- [SageMaker.19] SageMaker los modelos deben usar un registro privado en la VPC para las canalizaciones de inferencia de varios contenedores
- [SES.3] Los conjuntos de configuración de SES deben tener el TLS habilitado para enviar correos electrónicos
- [SQS.1] Las colas de Amazon SQS deben cifrarse en reposo
- [SQS.2] Las colas de SQS deben estar etiquetadas
- [SQS.3] Las políticas de acceso a las colas de SQS no deberían permitir el acceso público
- [SSM.6] SSM Automation debería tener el registro habilitado CloudWatch
- [SSM.7] Los documentos SSM deben tener habilitada la configuración de bloqueo para compartir en público
- [Transfer.3] Los conectores Transfer Family deben tener habilitado el registro

- [Transfer.4] Los acuerdos Transfer Family deben estar etiquetados
- [WAF.1]AWS WAFEl registro de ACL web global clásico debe estar habilitado
- [WAF.3]AWS WAFLos grupos de reglas regionales clásicos deben tener al menos una regla
- [WAF.6]AWS WAFLas reglas globales clásicas deben tener al menos una condición
- [WAF.7]AWS WAFLos grupos de reglas globales clásicos deben tener al menos una regla
- [WAF.8]AWS WAFLas ACL web globales clásicas deben tener al menos una regla o grupo de reglas
- [WAF.10]AWS WAFLas ACL web deben tener al menos una regla o grupo de reglas
- [WorkSpaces.1] los volúmenes de WorkSpaces usuarios deben cifrarse en reposo
- [WorkSpaces.2] los volúmenes WorkSpaces raíz deben cifrarse en reposo

Israel (Tel Aviv)

Los siguientes controles no se admiten en la región Israel (Tel Aviv).

- [APIGateway.8] Las rutas de API Gateway deben especificar un tipo de autorización
- [APIGateway.9] El registro de acceso debe configurarse para las etapas V2 de API Gateway
- [Amplify.1] Las aplicaciones Amplify deben estar etiquetadas
- [Amplify.2] Amplify branches debe estar etiquetado
- [AppFlow.1] AppFlow Los flujos de Amazon deben estar etiquetados
- [AppRunner.1] Los servicios de App Runner deben estar etiquetados
- [AppRunner.2] Los conectores VPC de App Runner deben estar etiquetados
- [AppSync.1]AWS AppSyncLas cachés de las API deben estar cifradas en reposo
- [AppSync.2]AWS AppSyncdebe tener habilitado el registro a nivel de campo
- [AppSync.5]AWS AppSyncLas API de GraphQL no deben autenticarse con claves de API
- [AppSync.6]AWS AppSyncLas cachés de las API deben cifrarse en tránsito
- [Backup.1]AWS Backuplos puntos de recuperación deben estar cifrados en reposo
- [Backup.4]AWS Backuplos planes de informes deben estar etiquetados
- [Batch.1] Las colas de trabajos por lotes deben estar etiquetadas
- [Batch.3] Los entornos de procesamiento por lotes deben etiquetarse

- [Batch.4] Las propiedades de los recursos de cómputo en los entornos de cómputo por lotes gestionados deben estar etiquetadas
- [BedrockAgentCore.1] Los AgentCore tiempos de ejecución de Bedrock deben configurarse con el modo de red VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways debería requerir autorización para las solicitudes entrantes
- [BedrockAgentCore.3] Bedrock AgentCore Memory debe estar cifrada y gestionada por el clienteAWS KMSclaves
- [BedrockAgentCore.4] Bedrock AgentCore Gateway debe cifrarse de forma que sea gestionada por el clienteAWS KMSclaves
- [BedrockAgentCore.5] Los navegadores AgentCore personalizados de Bedrock no deberían usar el modo de red pública
- [BedrockAgentCore.6] Los navegadores AgentCore personalizados de Bedrock deberían tener habilitada la grabación de sesiones
- [CloudFormation.3] las CloudFormation pilas deben tener habilitada la protección de terminación
- [CloudFormation.4] las CloudFormation pilas deben tener funciones de servicio asociadas
- [CloudFront.1] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado
- [CloudFront.3] CloudFront las distribuciones deben requerir el cifrado durante el tránsito
- [CloudFront.4] CloudFront las distribuciones deben tener configurada la conmutación por error de origen
- [CloudFront.5] CloudFront las distribuciones deben tener habilitado el registro
- [CloudFront.6] CloudFront las distribuciones deben tener WAF activado
- [CloudFront.7] CloudFront las distribuciones deben usar certificados personalizados SSL/TLS
- [CloudFront.8] CloudFront las distribuciones deben usar el SNI para atender las solicitudes HTTPS
- [CloudFront.9] CloudFront las distribuciones deben cifrar el tráfico para convertirlo en orígenes personalizados
- [CloudFront.10] CloudFront las distribuciones no deben usar protocolos SSL obsoletos entre ubicaciones de borde y orígenes personalizados
- [CloudFront.12] CloudFront las distribuciones no deben apuntar a orígenes de S3 inexistentes
- [CloudFront.13] CloudFront las distribuciones deben usar el control de acceso al origen

- [CloudFront.14] CloudFront las distribuciones deben estar etiquetadas
- [CloudFront.15] CloudFront las distribuciones deben usar la política de seguridad TLS recomendada
- [CloudFront.16] CloudFront las distribuciones deben usar el control de acceso de origen para los orígenes de las URL de las funciones de Lambda
- [CloudFront.17] CloudFront las distribuciones deben usar grupos de claves confiables para las URL y cookies firmadas
- [CodeArtifact.1] CodeArtifact los repositorios deben estar etiquetados
- [CodeGuruProfiler.1] Los grupos CodeGuru de creación de perfiles de Profiler deben estar etiquetados
- [CodeGuruReviewer.1] Las asociaciones de repositorios de CodeGuru Reviewer deben estar etiquetadas
- [Cognito.2] Los grupos de identidades de Cognito no deben permitir identidades no autenticadas
- [Connect.1] Los tipos de objetos de los perfiles de clientes de Amazon Connect deben estar etiquetados
- [Connect.2] Las instancias de Connect Customer deben tener el CloudWatch registro habilitado
- [DMS.2] Los certificados DMS deben estar etiquetados
- [DMS.3] Las suscripciones a eventos de DMS deben estar etiquetadas
- [DMS.4] Las instancias de replicación de DMS deben estar etiquetadas
- [DMS.5] Los grupos de subredes de replicación del DMS deben estar etiquetados
- [DMS.6] Las instancias de replicación de DMS deben tener habilitada la actualización automática de las versiones secundarias
- [DMS.7] Las tareas de replicación del DMS para la base de datos de destino deben tener el registro habilitado
- [DMS.8] Las tareas de replicación del DMS para la base de datos de origen deben tener el registro activado
- [DMS.9] Los puntos finales del DMS deben usar SSL
- [DMS.10] Los puntos finales de DMS para las bases de datos de Neptune deben tener habilitada la autorización de IAM
- [DMS.11] Los puntos finales de DMS para MongoDB deben tener un mecanismo de autenticación habilitado

- [DMS.12] Los puntos finales de DMS para Redis OSS deben tener el TLS habilitado
- [DMS.13] Las instancias de replicación de DMS deben configurarse para usar varias zonas de disponibilidad
- [DocumentDB.1] Los clústeres de Amazon DocumentDB deben cifrarse en reposo
- [DocumentDB.2] Los clústeres de Amazon DocumentDB deben tener un período de retención de copias de seguridad adecuado
- [DocumentDB.3] Las instantáneas de clústeres manuales de Amazon DocumentDB no deben ser públicas
- [DocumentDB.4] Los clústeres de Amazon DocumentDB deben publicar los registros de auditoría en Logs CloudWatch
- [DocumentDB.5] Los clústeres de Amazon DocumentDB deben tener habilitada la protección contra eliminaciones
- [DocumentDB.6] Los clústeres de Amazon DocumentDB deben cifrarse en tránsito
- [DynamoDB.3] Los clústeres de DynamoDB Accelerator (DAX) deben cifrarse en reposo
- [DynamoDB.4] Las tablas de DynamoDB deben estar presentes en un plan de respaldo
- [DynamoDB.7] Los clústeres de DynamoDB Accelerator deben cifrarse en tránsito
- [EC2.4] Las instancias EC2 detenidas deben eliminarse después de un período de tiempo específico
- [EC2.14] Los grupos de seguridad no deberían permitir la entrada desde la versión 0.0.0. 0/0 o: :/0 al puerto 3389
- [EC2.22] Deben eliminarse los grupos de seguridad de Amazon EC2 no utilizados
- [EC2.23] Amazon EC2 Transit Gateways no debe aceptar automáticamente las solicitudes de adjuntos de VPC
- [EC2.24] No se deben utilizar los tipos de instancias paravirtuales de Amazon EC2
- [EC2.25] Las plantillas de lanzamiento de Amazon EC2 no deben asignar direcciones IP públicas a las interfaces de red
- [EC2.28] Los volúmenes de EBS deben estar cubiertos por un plan de respaldo
- [EC2.34] Las tablas de rutas de la pasarela de tránsito EC2 deben estar etiquetadas
- [EC2.40] Las pasarelas NAT EC2 deben estar etiquetadas
- [EC2.51] Los puntos finales EC2 Client VPN deben tener habilitado el registro de conexiones de clientes

- [EC2.55] Las VPC deben configurarse con un punto final de interfaz para la API de ECR
- [EC2.56] Las VPC deben configurarse con un punto final de interfaz para Docker Registry
- [EC2.57] Las VPC deben configurarse con un punto final de interfaz para Systems Manager
- [EC2.58] Las VPC deben configurarse con un punto final de interfaz para los contactos de Systems Manager Incident Manager
- [EC2.60] Las VPC deben configurarse con un punto final de interfaz para Systems Manager Incident Manager
- [EC2.170] Las plantillas de lanzamiento de EC2 deben utilizar la versión 2 del servicio de metadatos de instancias (IMDSv2)
- [EC2.173] Las solicitudes de EC2 Spot Fleet con parámetros de lanzamiento deberían permitir el cifrado de los volúmenes de EBS adjuntos
- [EC2.175] Las plantillas de lanzamiento de EC2 deben estar etiquetadas
- [EC2.177] Las sesiones de réplica de tráfico de EC2 deben etiquetarse
- [EC2.179] Los objetivos del espejo de tráfico de EC2 deben estar etiquetados
- [EC2.180] Las interfaces de red EC2 deberían tener habilitada source/destination la verificación
- [EC2.181] Las plantillas de lanzamiento de EC2 deberían permitir el cifrado de los volúmenes de EBS adjuntos
- [ECR.2] Los repositorios privados de ECR deben tener configurada la inmutabilidad de etiquetas
- [ECR.3] Los repositorios de ECR deben tener configurada al menos una política de ciclo de vida
- [ECR.4] Los repositorios públicos de ECR deben etiquetarse
- [ECR.5] Los repositorios de ECR deben estar cifrados y ser gestionados por el cliente AWS KMS keys
- [EFS.1] Elastic File System debe configurarse para cifrar los datos de los archivos en reposo mediante AWS KMS
- [EFS.2] Los volúmenes de Amazon EFS deben figurar en los planes de copia de seguridad
- [EFS.3] Los puntos de acceso EFS deben exigir un directorio raíz
- [EFS.4] Los puntos de acceso EFS deben exigir la identidad del usuario
- [EFS.8] Los sistemas de archivos EFS deben cifrarse en reposo
- [EKS.2] Los clústeres de EKS deben ejecutarse en una versión de Kubernetes compatible
- [EKS.7] Las configuraciones del proveedor de identidad de EKS deben etiquetarse

- [EKS.8] Los clústeres de EKS deben tener habilitado el registro de auditoría
- [ELB.2] Los balanceadores de carga clásicos con SSL/HTTPS oyentes deben usar un certificado proporcionado por AWS Gestor de certificados
- [ELB.14] El balanceador de carga clásico debe configurarse con el modo defensivo o de mitigación de desincronización más estricto
- [ELB.17] Los balanceadores de cargas de aplicaciones y redes con oyentes deben usar las políticas de seguridad recomendadas
- [ELB.18] Los oyentes del balanceador de cargas de red y aplicaciones deben usar protocolos seguros para cifrar los datos en tránsito
- [ElastiCache.1] ElastiCache (Redis OSS) los clústeres deben tener habilitadas las copias de seguridad automáticas
- [ElastiCache.2] ElastiCache los clústeres deberían tener habilitadas las actualizaciones automáticas de las versiones secundarias
- [ElastiCache.3] los grupos de ElastiCache replicación deberían tener habilitada la conmutación por error automática
- [ElastiCache.4] los grupos de ElastiCache replicación deben cifrarse en reposo
- [ElastiCache.5] los grupos de ElastiCache replicación deben cifrarse en tránsito
- [ElastiCache.6] ElastiCache (Redis OSS) Los grupos de replicación de versiones anteriores deberían tener habilitada la autenticación de Redis OSS
- [ElastiCache.7] los ElastiCache clústeres no deben usar el grupo de subredes predeterminado
- [ElasticBeanstalk.1] Los entornos de Elastic Beanstalk deberían tener habilitados los informes de estado mejorados
- [ElasticBeanstalk.2] Las actualizaciones de la plataforma gestionada de Elastic Beanstalk deben estar habilitadas
- [ElasticBeanstalk.3] Elastic Beanstalk debería transmitir los registros a CloudWatch
- [EMR.1] Los nodos principales del clúster de Amazon EMR no deben tener direcciones IP públicas
- [ES.4] Debería estar habilitado el registro de errores de dominio de Elasticsearch en Logs CloudWatch
- [EventBridge.4] los puntos finales EventBridge globales deberían tener habilitada la replicación de eventos
- [FraudDetector.1] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.2] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas

- [FraudDetector.3] Los resultados de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.4] Las variables de Amazon Fraud Detector deben estar etiquetadas
- [GlobalAccelerator.1] Los aceleradores de Global Accelerator deben estar etiquetados
- [Glue.4]AWS GlueLos trabajos de Spark deberían ejecutarse en versiones compatibles deAWS Glue
- GuardDuty Los filtros [GuardDuty.2] deben estar etiquetados
- [IAM.1] Las políticas de IAM no deberían permitir todos los privilegios administrativos «*»
- [IAM.2] Los usuarios de IAM no deberían tener políticas de IAM adjuntas
- [IAM.3] Las claves de acceso de los usuarios de IAM deben rotarse cada 90 días o menos
- [IAM.4] La clave de acceso del usuario raíz de IAM no debería existir
- [IAM.5] La MFA debe estar habilitada para todos los usuarios de IAM que tengan una contraseña de consola
- [IAM.6] La MFA de hardware debe estar habilitada para el usuario root
- [IAM.7] Las políticas de contraseñas para los usuarios de IAM deben tener configuraciones sólidas
- [IAM.8] Se deben eliminar las credenciales de usuario de IAM no utilizadas
- [IAM.9] La MFA debe estar habilitada para el usuario root
- [IAM.10] Las políticas de contraseñas para los usuarios de IAM deben tener configuraciones sólidas
- [IAM.11] Asegúrese de que la política de contraseñas de IAM requiera al menos una letra mayúscula
- [IAM.12] Asegúrese de que la política de contraseñas de IAM requiera al menos una letra minúscula
- [IAM.13] Asegúrese de que la política de contraseñas de IAM requiera al menos un símbolo
- [IAM.14] Asegúrese de que la política de contraseñas de IAM requiera al menos un número
- [IAM.15] Asegúrese de que la política de contraseñas de IAM exija una longitud de contraseña mínima de 14 o más
- [IAM.16] Asegúrese de que la política de contraseñas de IAM impida la reutilización de contraseñas
- [IAM.17] Asegúrese de que la política de contraseñas de IAM haga caducar las contraseñas en un plazo de 90 días o menos

- [IAM.18] Asegúrese de que se haya creado una función de soporte para gestionar los incidentes conAWS Support
- [IAM.19] La MFA debe estar habilitada para todos los usuarios de IAM
- [IAM.21] Las políticas de IAM gestionadas por el cliente que cree no deberían permitir acciones comodín en los servicios
- [IAM.22] Se deben eliminar las credenciales de usuario de IAM que no se hayan utilizado durante 45 días
- [IAM.24] Las funciones de IAM deben estar etiquetadas
- [IAM.25] Los usuarios de IAM deben estar etiquetados
- [IAM.26] SSL/TLS Los certificados caducados gestionados en IAM deben eliminarse
- [IAM.27] Las identidades de IAM no deberían tener la AWSCloudShellFullAccess política adjunta
- [IAM.28] El analizador de acceso externo de IAM Access Analyzer debe estar habilitado
- [Inspector.1] El escaneo EC2 de Amazon Inspector debe estar activado
- [Inspector.2] El escaneo ECR de Amazon Inspector debe estar activado
- [Inspector.3] El escaneo de código Lambda de Amazon Inspector Lambda debe estar activado
- [Inspector.4] El escaneo estándar de Amazon Inspector Lambda debe estar activado
- [IoT.1]AWS IoT Device Defenderlos perfiles de seguridad deben estar etiquetados
- [IoT.2]AWS IoT Corelas acciones de mitigación deben estar etiquetadas
- [IoT.3]AWS IoT Corelas dimensiones deben estar etiquetadas
- [IoT.4]AWS IoT Corelos autorizadores deben estar etiquetados
- [IoT.5]AWS IoT CoreLos alias de los roles deben estar etiquetados
- [IoT.6]AWS IoT Corelas políticas deben estar etiquetadas
- [IoTSiteWise.1]AWSLos modelos SiteWise de activos de IoT deben estar etiquetados
- [IoTSiteWise.2]AWS SiteWise Los paneles de IoT deben estar etiquetados
- [IoTSiteWise.3]AWS SiteWise Las pasarelas de IoT deben estar etiquetadas
- [IoTSiteWise.4]AWS SiteWise Los portales de IoT deben estar etiquetados
- [IoTSiteWise.5]AWS SiteWise Los proyectos de IoT deben estar etiquetados
- [IoTTwinMaker.1]AWSLos trabajos de TwinMaker sincronización de IoT deben estar etiquetados
- [IoTTwinMaker.2]AWS TwinMaker Los espacios de trabajo de IoT deben estar etiquetados

- [IoTTwinMaker.3]AWS TwinMaker Las escenas de IoT deben estar etiquetadas
- [IoTTwinMaker.4]AWS TwinMaker Las entidades de IoT deben estar etiquetadas
- [IoTWireless.1]AWSLos grupos de multidifusión de IoT Wireless deben estar etiquetados
- [IoTWireless.2]AWSLos perfiles de servicio de IoT Wireless deben estar etiquetados
- [IoTWireless.3]AWSLas tareas de IoT FUOTA deben estar etiquetadas
- [IVS.1] Los pares de teclas de reproducción IVS deben estar etiquetados
- [IVS.2] Las configuraciones de grabación de IVS deben estar etiquetadas
- [IVS.3] Los canales IVS deben estar etiquetados
- [Keyspaces.1] Los espacios clave de Amazon Keyspaces deben estar etiquetados
- [Kinesis.1] Las transmisiones de Kinesis deben cifrarse en reposo
- [Kinesis.3] Las transmisiones de Kinesis deben tener un período de retención de datos adecuado
- [KMS.1] Las políticas gestionadas por los clientes de IAM no deberían permitir acciones de descifrado en todas las claves de KMS
- [KMS.2] Los directores de IAM no deberían tener políticas integradas de IAM que permitan realizar acciones de descifrado en todas las claves de KMS
- [Lambda.5] Las funciones de VPC Lambda deben funcionar en varias zonas de disponibilidad
- [Lambda.7] Las funciones de Lambda deberían tener AWS X-Ray el rastreo activo está habilitado
- [Macie.1] Amazon Macie debería estar activado
- [MQ.2] Los corredores de ActiveMQ deben transmitir los registros de auditoría a CloudWatch
- [MQ.4] Los corredores de Amazon MQ deben estar etiquetados
- [MQ.5] Los corredores de ActiveMQ deberían usar el modo de implementación active/standby
- [MQ.6] Los corredores de RabbitMQ deberían usar el modo de despliegue de clústeres
- [MSK.1] Los clústeres de MSK deben cifrarse en tránsito entre los nodos de intermediación
- [MSK.2] Los clústeres de MSK deberían tener configurada una supervisión mejorada
- [MSK.3] Los conectores MSK Connect deben estar cifrados en tránsito
- [MSK.4] Los clústeres de MSK deben tener el acceso público deshabilitado
- [MSK.5] Los conectores MSK deben tener el registro activado
- [MSK.6] Los clústeres de MSK deberían deshabilitar el acceso no autenticado
- [Neptune.3] Las instantáneas del clúster de base de datos de Neptune no deben ser públicas

- [Neptune.6] Las instantáneas del clúster de base de datos de Neptune deben cifrarse en reposo
- [NetworkFirewall.10] Los firewalls de Network Firewall deben tener habilitada la protección contra cambios de subred
- [Opensearch.1] OpenSearch los dominios deben tener activado el cifrado en reposo
- [Opensearch.2] OpenSearch los dominios no deben ser de acceso público
- [Opensearch.3] OpenSearch los dominios deben cifrar los datos enviados entre nodos
- [Opensearch.4] El registro de errores de OpenSearch dominio en Logs debe estar habilitado CloudWatch
- [Opensearch.5] OpenSearch los dominios deben tener activado el registro de auditoría
- [Opensearch.6] OpenSearch los dominios deben tener al menos tres nodos de datos
- [Opensearch.7] OpenSearch los dominios deben tener habilitado un control de acceso detallado
- [Opensearch.8] Las conexiones a los OpenSearch dominios deben cifrarse con la última política de seguridad de TLS
- [Opensearch.9] OpenSearch los dominios deben estar etiquetados
- [Opensearch.10] OpenSearch los dominios deben tener instalada la última actualización de software
- [Opensearch.11] OpenSearch los dominios deben tener al menos tres nodos principales dedicados
- [RDS.1] La instantánea de RDS debe ser privada
- [RDS.4] Las instantáneas de clústeres de RDS y las instantáneas de bases de datos deben cifrarse en reposo
- [RDS.14] Los clústeres de Amazon Aurora deben tener habilitado el retroceso
- [RDS.26] Las instancias de base de datos de RDS deben protegerse mediante un plan de respaldo
- [RDS.29] Las instantáneas del clúster de bases de datos de RDS deben etiquetarse
- [RDS.31] Los grupos de seguridad de la base de datos de RDS deben etiquetarse
- [RDS.35] Los clústeres de bases de datos de RDS deben tener habilitada la actualización automática de versiones secundarias
- [RDS.37] Los clústeres de bases de datos de Aurora PostgreSQL deben publicar los registros en Logs CloudWatch
- [Redshift.8] Los clústeres de Amazon Redshift no deben usar el nombre de usuario de administrador predeterminado

- [Redshift.18] Los clústeres de Redshift deberían tener Multi-AZ las implementaciones habilitadas
- [RedshiftServerless.1] Los grupos de trabajo sin servidor de Amazon Redshift deberían utilizar un enrutamiento de VPC mejorado
- [RedshiftServerless.2] Las conexiones a los grupos de trabajo sin servidor de Redshift deberían ser obligatorias para usar SSL
- [Route53.1] Los controles de salud de Route 53 deben estar etiquetados
- [Route53.2] Las zonas alojadas públicas de Route 53 deberían registrar las consultas de DNS
- [S3.24] Los puntos de Multi-Region acceso S3 deben tener habilitada la configuración de bloqueo del acceso público
- [S3.25] Los buckets de directorio de S3 deben tener configuraciones de ciclo de vida
- [SageMaker.1] Las instancias de Amazon SageMaker Notebook no deberían tener acceso directo a Internet
- [SageMaker.2] las instancias de SageMaker cuadernos deben lanzarse en una VPC personalizada
- [SageMaker.3] Los usuarios no deben tener acceso root a las instancias de los SageMaker cuadernos
- SageMaker Los modelos [SageMaker.5] deben tener habilitado el aislamiento de red
- [SageMaker.9] las definiciones de trabajos de calidad de los SageMaker datos deben tener habilitado el cifrado del tráfico entre contenedores
- [SageMaker.10] Las definiciones de trabajos de explicabilidad del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores
- [SageMaker.11] las definiciones de trabajos SageMaker de calidad de los datos deben tener habilitado el aislamiento de red
- [SageMaker.12] las definiciones de trabajo basadas en el sesgo del SageMaker modelo deben tener habilitado el aislamiento de red
- [SageMaker.13] las definiciones de trabajos de calidad del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores
- [SageMaker.14] los programas SageMaker de monitoreo deben tener habilitado el aislamiento de la red
- [SageMaker.15] Las definiciones de trabajo basadas en el sesgo del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores
- SageMaker Los modelos [SageMaker.16] deben usar un registro privado en la VPC para los contenedores principales

- [SageMaker.19] SageMaker los modelos deben usar un registro privado en la VPC para las canalizaciones de inferencia de varios contenedores
- [ServiceCatalog.1] Las carteras de Service Catalog deben compartirse dentro de unAWSsolo una organización
- [SQS.1] Las colas de Amazon SQS deben cifrarse en reposo
- [SQS.2] Las colas de SQS deben estar etiquetadas
- [SQS.3] Las políticas de acceso a las colas de SQS no deberían permitir el acceso público
- [SSM.4] Los documentos SSM no deben ser públicos
- [SSM.6] SSM Automation debería tener el registro habilitado CloudWatch
- [SSM.7] Los documentos SSM deben tener habilitada la configuración de bloqueo para compartir en público
- [StepFunctions.1] Step Functions indica que las máquinas deben tener el registro activado
- [Transfer.3] Los conectores Transfer Family deben tener habilitado el registro
- [Transfer.4] Los acuerdos Transfer Family deben estar etiquetados
- [WAF.1]AWS WAFEl registro de ACL web global clásico debe estar habilitado
- [WAF.3]AWS WAFLos grupos de reglas regionales clásicos deben tener al menos una regla
- [WAF.6]AWS WAFLas reglas globales clásicas deben tener al menos una condición
- [WAF.7]AWS WAFLos grupos de reglas globales clásicos deben tener al menos una regla
- [WAF.8]AWS WAFLas ACL web globales clásicas deben tener al menos una regla o grupo de reglas
- [WorkSpaces.1] los volúmenes de WorkSpaces usuarios deben cifrarse en reposo
- [WorkSpaces.2] los volúmenes WorkSpaces raíz deben cifrarse en reposo

México (centro)

Los siguientes controles no se admiten en la región México (centro).

- [ACM.1] ACM-issued Los certificados importados y renovados deben renovarse después de un período de tiempo específico
- [ACM.2] Los certificados RSA gestionados por ACM deben utilizar una longitud de clave de al menos 2048 bits
- [Account.1] La información de contacto de seguridad debe proporcionarse para unCuenta de AWS

- [Account.2]Cuentas de AWSdebe formar parte de unAWS Organizationsorganización
- [APIGateway.8] Las rutas de API Gateway deben especificar un tipo de autorización
- [APIGateway.9] El registro de acceso debe configurarse para las etapas V2 de API Gateway
- [APIGateway.10] Las integraciones de API Gateway V2 deben usar HTTPS para las conexiones privadas
- [Amplify.1] Las aplicaciones Amplify deben estar etiquetadas
- [Amplify.2] Amplify branches debe estar etiquetado
- [AppConfig.1]AWS AppConfiglas aplicaciones deben estar etiquetadas
- [AppConfig.2]AWS AppConfiglos perfiles de configuración deben estar etiquetados
- [AppConfig.3]AWS AppConfiglos entornos deben estar etiquetados
- [AppConfig.4]AWS AppConfiglas asociaciones de extensiones deben estar etiquetadas
- [AppFlow.1] AppFlow Los flujos de Amazon deben estar etiquetados
- [AppRunner.1] Los servicios de App Runner deben estar etiquetados
- [AppRunner.2] Los conectores VPC de App Runner deben estar etiquetados
- [AppSync.1]AWS AppSyncLas cachés de las API deben estar cifradas en reposo
- [AppSync.2]AWS AppSyncdebe tener habilitado el registro a nivel de campo
- [AppSync.4]AWS AppSyncLas API de GraphQL deben estar etiquetadas
- [AppSync.5]AWS AppSyncLas API de GraphQL no deben autenticarse con claves de API
- [AppSync.6]AWS AppSyncLas cachés de las API deben cifrarse en tránsito
- [Athena.4] Los grupos de trabajo de Athena deberían tener habilitado el registro
- [AutoScaling.2] El grupo Amazon EC2 Auto Scaling debe cubrir varias zonas de disponibilidad
- [AutoScaling.3] Las configuraciones de lanzamiento grupal de Auto Scaling deberían configurar las instancias EC2 para que requieran la versión 2 del Servicio de Metadatos de Instancia (IMDSv2)
- [AutoScaling.6] Los grupos de Auto Scaling deben usar varios tipos de instancias en múltiples zonas de disponibilidad
- [AutoScaling.9] Los grupos de Amazon EC2 Auto Scaling deben utilizar las plantillas de lanzamiento de Amazon EC2
- [Backup.1]AWS Backuplos puntos de recuperación deben estar cifrados en reposo
- [Backup.2]AWS Backuplos puntos de recuperación deben estar etiquetados

- [Backup.4]AWS Backuplos planes de informes deben estar etiquetados
- [Batch.1] Las colas de trabajos por lotes deben estar etiquetadas
- [Batch.2] Las políticas de programación de lotes deben estar etiquetadas
- [Batch.3] Los entornos de procesamiento por lotes deben etiquetarse
- [Batch.4] Las propiedades de los recursos de cómputo en los entornos de cómputo por lotes gestionados deben estar etiquetadas
- [BedrockAgentCore.1] Los AgentCore tiempos de ejecución de Bedrock deben configurarse con el modo de red VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways debería requerir autorización para las solicitudes entrantes
- [BedrockAgentCore.3] Bedrock AgentCore Memory debe estar cifrada y gestionada por el clienteAWS KMSclaves
- [BedrockAgentCore.4] Bedrock AgentCore Gateway debe cifrarse de forma que sea gestionada por el clienteAWS KMSclaves
- [BedrockAgentCore.5] Los navegadores AgentCore personalizados de Bedrock no deberían usar el modo de red pública
- [BedrockAgentCore.6] Los navegadores AgentCore personalizados de Bedrock deberían tener habilitada la grabación de sesiones
- [CloudFormation.3] las CloudFormation pilas deben tener habilitada la protección de terminación
- [CloudFormation.4] las CloudFormation pilas deben tener funciones de servicio asociadas
- [CloudFront.1] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado
- [CloudFront.3] CloudFront las distribuciones deben requerir el cifrado durante el tránsito
- [CloudFront.4] CloudFront las distribuciones deben tener configurada la conmutación por error de origen
- [CloudFront.5] CloudFront las distribuciones deben tener habilitado el registro
- [CloudFront.6] CloudFront las distribuciones deben tener WAF activado
- [CloudFront.7] CloudFront las distribuciones deben usar certificados personalizados SSL/TLS
- [CloudFront.8] CloudFront las distribuciones deben usar el SNI para atender las solicitudes HTTPS
- [CloudFront.9] CloudFront las distribuciones deben cifrar el tráfico para convertirlo en orígenes personalizados

- [CloudFront.10] CloudFront las distribuciones no deben usar protocolos SSL obsoletos entre ubicaciones de borde y orígenes personalizados
- [CloudFront.12] CloudFront las distribuciones no deben apuntar a orígenes de S3 inexistentes
- [CloudFront.13] CloudFront las distribuciones deben usar el control de acceso al origen
- [CloudFront.14] CloudFront las distribuciones deben estar etiquetadas
- [CloudFront.15] CloudFront las distribuciones deben usar la política de seguridad TLS recomendada
- [CloudFront.16] CloudFront las distribuciones deben usar el control de acceso de origen para los orígenes de las URL de las funciones de Lambda
- [CloudFront.17] CloudFront las distribuciones deben usar grupos de claves confiables para las URL y cookies firmadas
- [CloudTrail.6] Asegúrese de que el depósito de S3 que se utiliza para almacenar CloudTrail los registros no sea de acceso público
- [CloudTrail.7] Asegúrese de que el registro de acceso al bucket de S3 esté habilitado en el CloudTrail bucket de S3
- [CloudTrail.10] Los almacenes de datos de eventos de CloudTrail Lake deben estar cifrados y gestionados por el clienteAWS KMS keys
- [CloudWatch.17] las acciones CloudWatch de alarma deben estar activadas
- [CodeArtifact.1] CodeArtifact los repositorios deben estar etiquetados
- [CodeBuild.1] Las URL del repositorio fuente de CodeBuild Bitbucket no deben contener credenciales confidenciales
- [CodeBuild.2] las variables de entorno CodeBuild del proyecto no deben contener credenciales de texto claro
- [CodeBuild.3] Los registros de CodeBuild S3 deben estar cifrados
- [CodeBuild.4] los entornos de CodeBuild proyectos deben tener un registroAWS ConfigDuración
- [CodeBuild.7] las exportaciones de grupos de CodeBuild informes deben cifrarse en reposo
- [CodeGuruProfiler.1] Los grupos CodeGuru de creación de perfiles de Profiler deben estar etiquetados
- [CodeGuruReviewer.1] Las asociaciones de repositorios de CodeGuru Reviewer deben estar etiquetadas
- [Cognito.1] Los grupos de usuarios de Cognito deben tener activada la protección contra amenazas y el modo de aplicación con todas las funciones para la autenticación estándar

- [Cognito.2] Los grupos de identidades de Cognito no deben permitir identidades no autenticadas
- [Cognito.3] Las políticas de contraseñas para los grupos de usuarios de Cognito deben tener configuraciones sólidas
- [Cognito.4] Los grupos de usuarios de Cognito deben tener activada la protección contra amenazas y el modo de aplicación con todas las funciones para la autenticación personalizada
- [Cognito.5] La MFA debe estar habilitada para los grupos de usuarios de Cognito
- [Cognito.6] Los grupos de usuarios de Cognito deben tener habilitada la protección contra la eliminación
- [Connect.1] Los tipos de objetos de los perfiles de clientes de Amazon Connect deben estar etiquetados
- [Connect.2] Las instancias de Connect Customer deben tener el CloudWatch registro habilitado
- [DataFirehose.1] Los flujos de entrega de Firehose deben cifrarse en reposo
- [DataSync.1] DataSync las tareas deberían tener el registro activado
- [DataSync.2] DataSync las tareas deben estar etiquetadas
- [Detective.1] Los gráficos de comportamiento de los detectives deben estar etiquetados
- [DMS.2] Los certificados DMS deben estar etiquetados
- [DMS.3] Las suscripciones a eventos de DMS deben estar etiquetadas
- [DMS.4] Las instancias de replicación de DMS deben estar etiquetadas
- [DMS.5] Los grupos de subredes de replicación del DMS deben estar etiquetados
- [DMS.6] Las instancias de replicación de DMS deben tener habilitada la actualización automática de las versiones secundarias
- [DMS.7] Las tareas de replicación del DMS para la base de datos de destino deben tener el registro habilitado
- [DMS.8] Las tareas de replicación del DMS para la base de datos de origen deben tener el registro activado
- [DMS.9] Los puntos finales del DMS deben usar SSL
- [DMS.10] Los puntos finales de DMS para las bases de datos de Neptune deben tener habilitada la autorización de IAM
- [DMS.11] Los puntos finales de DMS para MongoDB deben tener un mecanismo de autenticación habilitado
- [DMS.12] Los puntos finales de DMS para Redis OSS deben tener el TLS habilitado

- [DMS.13] Las instancias de replicación de DMS deben configurarse para usar varias zonas de disponibilidad
- [DocumentDB.1] Los clústeres de Amazon DocumentDB deben cifrarse en reposo
- [DocumentDB.2] Los clústeres de Amazon DocumentDB deben tener un período de retención de copias de seguridad adecuado
- [DocumentDB.3] Las instantáneas de clústeres manuales de Amazon DocumentDB no deben ser públicas
- [DocumentDB.4] Los clústeres de Amazon DocumentDB deben publicar los registros de auditoría en Logs CloudWatch
- [DocumentDB.5] Los clústeres de Amazon DocumentDB deben tener habilitada la protección contra eliminaciones
- [DocumentDB.6] Los clústeres de Amazon DocumentDB deben cifrarse en tránsito
- [DynamoDB.3] Los clústeres de DynamoDB Accelerator (DAX) deben cifrarse en reposo
- [DynamoDB.4] Las tablas de DynamoDB deben estar presentes en un plan de respaldo
- [DynamoDB.6] Las tablas de DynamoDB deben tener habilitada la protección de eliminación
- [DynamoDB.7] Los clústeres de DynamoDB Accelerator deben cifrarse en tránsito
- [EC2.4] Las instancias EC2 detenidas deben eliminarse después de un período de tiempo específico
- [EC2.21] Las ACL de red no deberían permitir la entrada desde la versión 0.0.0. 0/0 al puerto 22 o al puerto 3389
- [EC2.22] Deben eliminarse los grupos de seguridad de Amazon EC2 no utilizados
- [EC2.23] Amazon EC2 Transit Gateways no debe aceptar automáticamente las solicitudes de adjuntos de VPC
- [EC2.24] No se deben utilizar los tipos de instancias paravirtuales de Amazon EC2
- [EC2.25] Las plantillas de lanzamiento de Amazon EC2 no deben asignar direcciones IP públicas a las interfaces de red
- [EC2.28] Los volúmenes de EBS deben estar cubiertos por un plan de respaldo
- [EC2.34] Las tablas de rutas de la pasarela de tránsito EC2 deben estar etiquetadas
- [EC2.40] Las pasarelas NAT EC2 deben estar etiquetadas
- [EC2.51] Los puntos finales EC2 Client VPN deben tener habilitado el registro de conexiones de clientes

- [EC2.53] Los grupos de seguridad de EC2 no deberían permitir la entrada desde la versión 0.0.0.0/0 a los puertos de administración remota del servidor
- [EC2.54] Los grupos de seguridad de EC2 no deberían permitir la entrada desde: :/0 a los puertos de administración remota del servidor
- [EC2.55] Las VPC deben configurarse con un punto final de interfaz para la API de ECR
- [EC2.56] Las VPC deben configurarse con un punto final de interfaz para Docker Registry
- [EC2.57] Las VPC deben configurarse con un punto final de interfaz para Systems Manager
- [EC2.58] Las VPC deben configurarse con un punto final de interfaz para los contactos de Systems Manager Incident Manager
- [EC2.60] Las VPC deben configurarse con un punto final de interfaz para Systems Manager Incident Manager
- [EC2.170] Las plantillas de lanzamiento de EC2 deben utilizar la versión 2 del servicio de metadatos de instancias (IMDSv2)
- [EC2.171] Las conexiones VPN de EC2 deberían tener el registro habilitado
- [EC2.172] La configuración de acceso público del bloque de VPC de EC2 debería bloquear el tráfico de la puerta de enlace de Internet
- [EC2.173] Las solicitudes de EC2 Spot Fleet con parámetros de lanzamiento deberían permitir el cifrado de los volúmenes de EBS adjuntos
- [EC2.174] Los conjuntos de opciones DHCP de EC2 deben estar etiquetados
- [EC2.175] Las plantillas de lanzamiento de EC2 deben estar etiquetadas
- [EC2.176] Las listas de prefijos de EC2 deben estar etiquetadas
- [EC2.177] Las sesiones de réplica de tráfico de EC2 deben etiquetarse
- [EC2.178] Los filtros espejo de tráfico EC2 deben estar etiquetados
- [EC2.179] Los objetivos del espejo de tráfico de EC2 deben estar etiquetados
- [EC2.180] Las interfaces de red EC2 deberían tener habilitada source/destination la verificación
- [EC2.181] Las plantillas de lanzamiento de EC2 deberían permitir el cifrado de los volúmenes de EBS adjuntos
- [EC2.182] La configuración de bloqueo de acceso público debe estar habilitada para las instantáneas de Amazon EBS
- [EC2.183] Las conexiones VPN de EC2 deben utilizar el protocolo IKEv2
- [ECR.1] Los repositorios privados de ECR deben tener configurado el escaneo de imágenes

- [ECR.2] Los repositorios privados de ECR deben tener configurada la inmutabilidad de etiquetas
- [ECR.3] Los repositorios de ECR deben tener configurada al menos una política de ciclo de vida
- [ECR.4] Los repositorios públicos de ECR deben etiquetarse
- [ECR.5] Los repositorios de ECR deben estar cifrados y ser gestionados por el cliente AWS KMS keys
- [ECS.3] Las definiciones de tareas de ECS no deben compartir el espacio de nombres del proceso del host
- [ECS.4] Los contenedores ECS deben ejecutarse sin privilegios
- [ECS.5] Las definiciones de tareas de ECS deben configurar los contenedores para que se limiten al acceso de solo lectura a los sistemas de archivos raíz
- [ECS.8] Los secretos no deben transmitirse como variables de entorno de contenedores
- [ECS.9] Las definiciones de tareas de ECS deben tener una configuración de registro
- [ECS.10] Los servicios Fargate de ECS deberían ejecutarse en la última versión de la plataforma Fargate
- [ECS.12] Los clústeres de ECS deben usar Container Insights
- [ECS.16] Los conjuntos de tareas de ECS no deben asignar automáticamente direcciones IP públicas
- [ECS.17] Las definiciones de tareas de ECS no deben usar el modo de red host
- [ECS.18] Las definiciones de tareas de ECS deben utilizar el cifrado en tránsito para los volúmenes de EFS
- [ECS.19] Los proveedores de capacidad de ECS deberían tener habilitada la protección de terminación gestionada
- [ECS.20] Las definiciones de tareas de ECS deben configurar a los usuarios no root en las definiciones de contenedores de Linux
- [ECS.21] Las definiciones de tareas de ECS deberían configurar a los usuarios no administradores en las definiciones de contenedores de Windows
- [EFS.1] Elastic File System debe configurarse para cifrar los datos de los archivos en reposo mediante AWS KMS
- [EFS.2] Los volúmenes de Amazon EFS deben figurar en los planes de copia de seguridad
- [EFS.3] Los puntos de acceso EFS deben exigir un directorio raíz
- [EFS.4] Los puntos de acceso EFS deben exigir la identidad del usuario

- [EFS.6] Los destinos de montaje de EFS no deben asociarse a subredes que asignan direcciones IP públicas en el momento del lanzamiento
- [] Los sistemas de archivos EFS deben tener habilitadas las copias de seguridad automáticas EFS.7
- [EFS.8] Los sistemas de archivos EFS deben cifrarse en reposo
- [EKS.2] Los clústeres de EKS deben ejecutarse en una versión de Kubernetes compatible
- [EKS.3] Los clústeres de EKS deben usar secretos de Kubernetes cifrados
- [EKS.7] Las configuraciones del proveedor de identidad de EKS deben etiquetarse
- [EKS.8] Los clústeres de EKS deben tener habilitado el registro de auditoría
- [EKS.9] Los grupos de nodos de EKS deben ejecutarse en una versión de Kubernetes compatible
- [ELB.10] El balanceador de carga clásico debe abarcar varias zonas de disponibilidad
- [ELB.12] El balanceador de carga de aplicaciones debe configurarse con el modo defensivo o de mitigación de desincronización más estricto
- [ELB.13] Los balanceadores de carga de aplicaciones, redes y puertas de enlace deben abarcar varias zonas de disponibilidad
- [ELB.14] El balanceador de carga clásico debe configurarse con el modo defensivo o de mitigación de desincronización más estricto
- [ELB.17] Los balanceadores de cargas de aplicaciones y redes con oyentes deben usar las políticas de seguridad recomendadas
- [ELB.18] Los oyentes del balanceador de cargas de red y aplicaciones deben usar protocolos seguros para cifrar los datos en tránsito
- [ElastiCache.1] ElastiCache (Redis OSS) los clústeres deben tener habilitadas las copias de seguridad automáticas
- [ElastiCache.2] ElastiCache los clústeres deberían tener habilitadas las actualizaciones automáticas de las versiones secundarias
- [ElastiCache.3] los grupos de ElastiCache replicación deberían tener habilitada la conmutación por error automática
- [ElastiCache.4] los grupos de ElastiCache replicación deben cifrarse en reposo
- [ElastiCache.5] los grupos de ElastiCache replicación deben cifrarse en tránsito
- [ElastiCache.6] ElastiCache (Redis OSS) Los grupos de replicación de versiones anteriores deberían tener habilitada la autenticación de Redis OSS
- [ElastiCache.7] los ElastiCache clústeres no deben usar el grupo de subredes predeterminado

- [ElasticBeanstalk.1] Los entornos de Elastic Beanstalk deberían tener habilitados los informes de estado mejorados
- [ElasticBeanstalk.2] Las actualizaciones de la plataforma gestionada de Elastic Beanstalk deben estar habilitadas
- [ElasticBeanstalk.3] Elastic Beanstalk debería transmitir los registros a CloudWatch
- [EMR.1] Los nodos principales del clúster de Amazon EMR no deben tener direcciones IP públicas
- [EMR.2] La configuración de acceso público del bloque Amazon EMR debe estar habilitada
- [EMR.3] Las configuraciones de seguridad de Amazon EMR deben cifrarse en reposo
- [EMR.4] Las configuraciones de seguridad de Amazon EMR deben cifrarse en tránsito
- [ES.3] Los dominios de Elasticsearch deben cifrar los datos enviados entre nodos
- [ES.4] Debería estar habilitado el registro de errores de dominio de Elasticsearch en Logs CloudWatch
- [ES.9] Los dominios de Elasticsearch deben etiquetarse
- [EventBridge.3] los autobuses de eventos EventBridge personalizados deben tener adjunta una política basada en los recursos
- [EventBridge.4] los puntos finales EventBridge globales deberían tener habilitada la replicación de eventos
- [FraudDetector.1] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.2] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas
- [FraudDetector.3] Los resultados de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.4] Las variables de Amazon Fraud Detector deben estar etiquetadas
- [FSx.1] FSx para sistemas de archivos OpenZFS debe configurarse para copiar etiquetas en copias de seguridad y volúmenes
- [FSx.2] Los sistemas de archivos FSx for Lustre deben configurarse para copiar etiquetas a las copias de seguridad
- [FSx.3] FSx para sistemas de archivos OpenZFS debe configurarse para su implementación Multi-AZ
- [FSx.4] FSx para sistemas de archivos NetApp ONTAP debe configurarse para su implementación Multi-AZ
- [FSx.5] Los sistemas de archivos FSx for Windows File Server deben configurarse para Multi-AZ su implementación

- [GlobalAccelerator.1] Los aceleradores de Global Accelerator deben estar etiquetados
- [Glue.1]AWS Gluelos trabajos deben estar etiquetados
- [Glue.3]AWS GlueLas transformaciones de aprendizaje automático deben cifrarse en reposo
- [Glue.4]AWS GlueLos trabajos de Spark deberían ejecutarse en versiones compatibles deAWS Glue
- [GuardDuty.1] GuardDuty debería estar activado
- GuardDuty Los filtros [GuardDuty.2] deben estar etiquetados
- [GuardDuty.5] La monitorización del registro de auditoría de GuardDuty EKS debe estar habilitada
- [GuardDuty.6] GuardDuty La protección Lambda debe estar habilitada
- [GuardDuty.7] La monitorización del tiempo de ejecución de GuardDuty EKS debe estar habilitada
- [GuardDuty.8] La protección contra GuardDuty malware para EC2 debe estar habilitada
- [GuardDuty.9] La protección GuardDuty RDS debe estar habilitada
- [GuardDuty.10] La protección GuardDuty S3 debe estar habilitada
- [GuardDuty.11] La monitorización del GuardDuty tiempo de ejecución debe estar habilitada
- [GuardDuty.12] La monitorización del tiempo de ejecución de GuardDuty ECS debe estar habilitada
- [GuardDuty.13] La monitorización del tiempo de ejecución de GuardDuty EC2 debe estar habilitada
- [IAM.1] Las políticas de IAM no deberían permitir todos los privilegios administrativos «*»
- [IAM.2] Los usuarios de IAM no deberían tener políticas de IAM adjuntas
- [IAM.3] Las claves de acceso de los usuarios de IAM deben rotarse cada 90 días o menos
- [IAM.4] La clave de acceso del usuario raíz de IAM no debería existir
- [IAM.5] La MFA debe estar habilitada para todos los usuarios de IAM que tengan una contraseña de consola
- [IAM.6] La MFA de hardware debe estar habilitada para el usuario root
- [IAM.7] Las políticas de contraseñas para los usuarios de IAM deben tener configuraciones sólidas
- [IAM.8] Se deben eliminar las credenciales de usuario de IAM no utilizadas
- [IAM.9] La MFA debe estar habilitada para el usuario root
- [IAM.10] Las políticas de contraseñas para los usuarios de IAM deben tener configuraciones sólidas

- [IAM.11] Asegúrese de que la política de contraseñas de IAM requiera al menos una letra mayúscula
- [IAM.12] Asegúrese de que la política de contraseñas de IAM requiera al menos una letra minúscula
- [IAM.13] Asegúrese de que la política de contraseñas de IAM requiera al menos un símbolo
- [IAM.14] Asegúrese de que la política de contraseñas de IAM requiera al menos un número
- [IAM.15] Asegúrese de que la política de contraseñas de IAM exija una longitud de contraseña mínima de 14 o más
- [IAM.16] Asegúrese de que la política de contraseñas de IAM impida la reutilización de contraseñas
- [IAM.17] Asegúrese de que la política de contraseñas de IAM haga caducar las contraseñas en un plazo de 90 días o menos
- [IAM.18] Asegúrese de que se haya creado una función de soporte para gestionar los incidentes conAWS Support
- [IAM.19] La MFA debe estar habilitada para todos los usuarios de IAM
- [IAM.21] Las políticas de IAM gestionadas por el cliente que cree no deberían permitir acciones comodín en los servicios
- [IAM.22] Se deben eliminar las credenciales de usuario de IAM que no se hayan utilizado durante 45 días
- [IAM.24] Las funciones de IAM deben estar etiquetadas
- [IAM.25] Los usuarios de IAM deben estar etiquetados
- [IAM.26] SSL/TLS Los certificados caducados gestionados en IAM deben eliminarse
- [IAM.27] Las identidades de IAM no deberían tener la AWSCloudShellFullAccess política adjunta
- [IAM.28] El analizador de acceso externo de IAM Access Analyzer debe estar habilitado
- [Inspector.1] El escaneo EC2 de Amazon Inspector debe estar activado
- [Inspector.2] El escaneo ECR de Amazon Inspector debe estar activado
- [Inspector.3] El escaneo de código Lambda de Amazon Inspector Lambda debe estar activado
- [Inspector.4] El escaneo estándar de Amazon Inspector Lambda debe estar activado
- [IoT.1]AWS IoT Device Defenderlos perfiles de seguridad deben estar etiquetados
- [IoT.2]AWS IoT Corelas acciones de mitigación deben estar etiquetadas

- [IoT.3]AWS IoT Corelas dimensiones deben estar etiquetadas
- [IoT.4]AWS IoT Corelos autorizadores deben estar etiquetados
- [IoT.5]AWS IoT CoreLos alias de los roles deben estar etiquetados
- [IoT.6]AWS IoT Corelas políticas deben estar etiquetadas
- [IoTSiteWise.1]AWSLos modelos SiteWise de activos de IoT deben estar etiquetados
- [IoTSiteWise.2]AWS SiteWise Los paneles de IoT deben estar etiquetados
- [IoTSiteWise.3]AWS SiteWise Las pasarelas de IoT deben estar etiquetadas
- [IoTSiteWise.4]AWS SiteWise Los portales de IoT deben estar etiquetados
- [IoTSiteWise.5]AWS SiteWise Los proyectos de IoT deben estar etiquetados
- [IoTTwinMaker.1]AWSLos trabajos de TwinMaker sincronización de IoT deben estar etiquetados
- [IoTTwinMaker.2]AWS TwinMaker Los espacios de trabajo de IoT deben estar etiquetados
- [IoTTwinMaker.3]AWS TwinMaker Las escenas de IoT deben estar etiquetadas
- [IoTTwinMaker.4]AWS TwinMaker Las entidades de IoT deben estar etiquetadas
- [IoTWireless.1]AWSLos grupos de multidifusión de IoT Wireless deben estar etiquetados
- [IoTWireless.2]AWSLos perfiles de servicio de IoT Wireless deben estar etiquetados
- [IoTWireless.3]AWSLas tareas de IoT FUOTA deben estar etiquetadas
- [IVS.1] Los pares de teclas de reproducción IVS deben estar etiquetados
- [IVS.2] Las configuraciones de grabación de IVS deben estar etiquetadas
- [IVS.3] Los canales IVS deben estar etiquetados
- [Keyspaces.1] Los espacios clave de Amazon Keyspaces deben estar etiquetados
- [Kinesis.1] Las transmisiones de Kinesis deben cifrarse en reposo
- [Kinesis.3] Las transmisiones de Kinesis deben tener un período de retención de datos adecuado
- [KMS.1] Las políticas gestionadas por los clientes de IAM no deberían permitir acciones de descifrado en todas las claves de KMS
- [KMS.2] Los directores de IAM no deberían tener políticas integradas de IAM que permitan realizar acciones de descifrado en todas las claves de KMS
- [KMS.5] Las claves KMS no deben ser de acceso público
- [Lambda.5] Las funciones de VPC Lambda deben funcionar en varias zonas de disponibilidad
- [Lambda.7] Las funciones de Lambda deberían tener AWS X-Ray el rastreo activo está habilitado

- [Macie.1] Amazon Macie debería estar activado
- [Macie.2] La detección automática de datos confidenciales por parte de Macie debería estar habilitada
- [MQ.2] Los corredores de ActiveMQ deben transmitir los registros de auditoría a CloudWatch
- [MQ.4] Los corredores de Amazon MQ deben estar etiquetados
- [MQ.5] Los corredores de ActiveMQ deberían usar el modo de implementación active/standby
- [MQ.6] Los corredores de RabbitMQ deberían usar el modo de despliegue de clústeres
- [MSK.1] Los clústeres de MSK deben cifrarse en tránsito entre los nodos de intermediación
- [MSK.2] Los clústeres de MSK deberían tener configurada una supervisión mejorada
- [MSK.3] Los conectores MSK Connect deben estar cifrados en tránsito
- [MSK.4] Los clústeres de MSK deben tener el acceso público deshabilitado
- [MSK.5] Los conectores MSK deben tener el registro activado
- [MSK.6] Los clústeres de MSK deberían deshabilitar el acceso no autenticado
- [Neptune.1] Los clústeres de bases de datos de Neptune deben cifrarse en reposo
- [Neptune.2] Los clústeres de bases de datos de Neptune deberían publicar registros de auditoría en Logs CloudWatch
- [Neptune.3] Las instantáneas del clúster de base de datos de Neptune no deben ser públicas
- [Neptune.4] Los clústeres de base de datos de Neptune deben tener habilitada la protección contra eliminación
- [Neptune.5] Los clústeres de Neptune DB deberían tener habilitadas las copias de seguridad automatizadas
- [Neptune.6] Las instantáneas del clúster de base de datos de Neptune deben cifrarse en reposo
- [Neptune.7] Los clústeres de base de datos de Neptune deben tener habilitada la autenticación de bases de datos de IAM
- [Neptune.8] Los clústeres de bases de datos de Neptune deben configurarse para copiar etiquetas a las instantáneas
- [Neptune.9] Los clústeres de base de datos Neptune deben implementarse en varias zonas de disponibilidad
- [NetworkFirewall.1] Los firewalls de Network Firewall deben implementarse en varias zonas de disponibilidad
- [NetworkFirewall.2] El registro de Network Firewall debe estar habilitado

- [NetworkFirewall.3] Las políticas de Network Firewall deben tener asociado al menos un grupo de reglas
- [NetworkFirewall.4] La acción sin estado predeterminada para las políticas de Network Firewall debe ser eliminar o reenviar paquetes completos
- [NetworkFirewall.5] La acción sin estado predeterminada para las políticas de Network Firewall debe ser eliminar o reenviar paquetes fragmentados
- [NetworkFirewall.6] El grupo de reglas de Stateless Network Firewall no debe estar vacío
- [NetworkFirewall.9] Los firewalls de Network Firewall deben tener habilitada la protección de eliminación
- [NetworkFirewall.10] Los firewalls de Network Firewall deben tener habilitada la protección contra cambios de subred
- [Opensearch.1] OpenSearch los dominios deben tener activado el cifrado en reposo
- [Opensearch.2] OpenSearch los dominios no deben ser de acceso público
- [Opensearch.3] OpenSearch los dominios deben cifrar los datos enviados entre nodos
- [Opensearch.4] El registro de errores de OpenSearch dominio en Logs debe estar habilitado CloudWatch
- [Opensearch.5] OpenSearch los dominios deben tener activado el registro de auditoría
- [Opensearch.6] OpenSearch los dominios deben tener al menos tres nodos de datos
- [Opensearch.7] OpenSearch los dominios deben tener habilitado un control de acceso detallado
- [Opensearch.8] Las conexiones a los OpenSearch dominios deben cifrarse con la última política de seguridad de TLS
- [Opensearch.9] OpenSearch los dominios deben estar etiquetados
- [Opensearch.10] OpenSearch los dominios deben tener instalada la última actualización de software
- [Opensearch.11] OpenSearch los dominios deben tener al menos tres nodos principales dedicados
- [PCA.1]AWS Privada CALa autoridad emisora de certificados raíz debe estar deshabilitada
- [PCA.2]AWSLas autoridades de certificación de CA privadas deben estar etiquetadas
- [RDS.14] Los clústeres de Amazon Aurora deben tener habilitado el retroceso
- [RDS.24] Los clústeres de bases de datos de RDS deben usar un nombre de usuario de administrador personalizado
- [RDS.25] Las instancias de bases de datos de RDS deben usar un nombre de usuario de administrador personalizado

- [RDS.26] Las instancias de base de datos de RDS deben protegerse mediante un plan de respaldo
- [RDS.27] Los clústeres de bases de datos de RDS deben cifrarse en reposo
- [RDS.31] Los grupos de seguridad de la base de datos de RDS deben etiquetarse
- [RDS.34] Los clústeres de bases de datos Aurora MySQL deben publicar los registros de auditoría en Logs CloudWatch
- [RDS.35] Los clústeres de bases de datos de RDS deben tener habilitada la actualización automática de versiones secundarias
- [RDS.36] Las instancias de base de datos de RDS para PostgreSQL deben publicar los registros en Logs CloudWatch
- [RDS.37] Los clústeres de bases de datos de Aurora PostgreSQL deben publicar los registros en Logs CloudWatch
- [RDS.38] Las instancias de base de datos de RDS para PostgreSQL deben cifrarse en tránsito
- [RDS.39] Las instancias de base de datos de RDS para MySQL deben cifrarse en tránsito
- [RDS.40] Las instancias de base de datos de RDS para SQL Server deben publicar los registros en Logs CloudWatch
- [RDS.41] Las instancias de base de datos de RDS para SQL Server deben cifrarse en tránsito
- [RDS.42] Las instancias de base de datos de RDS para MariaDB deben publicar los registros en Logs CloudWatch
- [RDS.43] Los proxies de bases de datos de RDS deben requerir el cifrado TLS para las conexiones
- [RDS.44] Las instancias de base de datos de RDS para MariaDB deben cifrarse durante el tránsito
- [RDS.45] Los clústeres de bases de datos Aurora MySQL deben tener habilitado el registro de auditoría
- [RDS.46] Las instancias de base de datos de RDS no deben implementarse en subredes públicas con rutas a pasarelas de Internet
- [RDS.47] Los clústeres de bases de datos de RDS para PostgreSQL deben configurarse para copiar las etiquetas a las instantáneas de bases de datos
- [RDS.48] Los clústeres de bases de datos de RDS para MySQL deben configurarse para copiar etiquetas a las instantáneas de bases de datos
- [RDS.51] Los clústeres globales de RDS deben ejecutarse en una versión compatible de Aurora MySQL

- [Redshift.1] Los clústeres de Amazon Redshift deberían prohibir el acceso público
- [Redshift.2] Las conexiones a los clústeres de Amazon Redshift deben cifrarse en tránsito
- [Redshift.3] Los clústeres de Amazon Redshift deben tener habilitadas las instantáneas automáticas
- [Redshift.4] Los clústeres de Amazon Redshift deben tener habilitado el registro de auditoría
- [Redshift.6] Amazon Redshift debería tener habilitadas las actualizaciones automáticas a las versiones principales
- [Redshift.7] Los clústeres de Redshift deberían utilizar un enrutamiento de VPC mejorado
- [Redshift.8] Los clústeres de Amazon Redshift no deben usar el nombre de usuario de administrador predeterminado
- [Redshift.10] Los clústeres de Redshift deben cifrarse en reposo
- [Redshift.11] Los clústeres de Redshift deben estar etiquetados
- [Redshift.13] Las instantáneas del clúster de Redshift deben estar etiquetadas
- [Redshift.15] Los grupos de seguridad de Redshift deberían permitir la entrada en el puerto del clúster solo desde orígenes restringidos
- [Redshift.16] Los grupos de subredes de clústeres de Redshift deben tener subredes de varias zonas de disponibilidad
- [Redshift.17] Los grupos de parámetros del clúster de Redshift deben estar etiquetados
- [Redshift.18] Los clústeres de Redshift deberían tener Multi-AZ las implementaciones habilitadas
- [RedshiftServerless.1] Los grupos de trabajo sin servidor de Amazon Redshift deberían utilizar un enrutamiento de VPC mejorado
- [RedshiftServerless.2] Las conexiones a los grupos de trabajo sin servidor de Redshift deberían ser obligatorias para usar SSL
- [RedshiftServerless.3] Los grupos de trabajo sin servidor de Redshift deberían prohibir el acceso público
- [RedshiftServerless.4] Los espacios de nombres de Redshift Serverless deben cifrarse y administrarse por el clienteAWS KMS keys
- [RedshiftServerless.5] Los espacios de nombres Redshift Serverless no deben usar el nombre de usuario de administrador predeterminado
- [RedshiftServerless.6] Los espacios de nombres Redshift Serverless deberían exportar los registros a los registros CloudWatch

- [Route53.1] Los controles de salud de Route 53 deben estar etiquetados
- [Route53.2] Las zonas alojadas públicas de Route 53 deberían registrar las consultas de DNS
- [S3.7] Los cubos de uso general de S3 deben utilizar la replicación entre regiones
- [S3.10] Los cubos de uso general de S3 con el control de versiones habilitado deben tener configuraciones de ciclo de vida
- [S3.11] Los cubos de uso general de S3 deben tener habilitadas las notificaciones de eventos
- [S3.12] Las ACL no deben usarse para administrar el acceso de los usuarios a los cubos de uso general de S3
- [S3.13] Los cubos de uso general de S3 deben tener configuraciones de ciclo de vida
- [S3.19] Los puntos de acceso S3 deben tener habilitada la configuración de bloqueo de acceso público
- [S3.20] Los cubos de uso general de S3 deben tener habilitada la eliminación de MFA
- [S3.22] Los cubos de uso general de S3 deben registrar los eventos de escritura a nivel de objeto
- [S3.23] Los cubos de uso general de S3 deben registrar los eventos de lectura a nivel de objeto
- [S3.24] Los puntos de Multi-Region acceso S3 deben tener habilitada la configuración de bloqueo del acceso público
- [S3.25] Los buckets de directorio de S3 deben tener configuraciones de ciclo de vida
- [SageMaker.1] Las instancias de Amazon SageMaker Notebook no deberían tener acceso directo a Internet
- [SageMaker.2] las instancias de SageMaker cuadernos deben lanzarse en una VPC personalizada
- [SageMaker.3] Los usuarios no deben tener acceso root a las instancias de los SageMaker cuadernos
- [SageMaker.4] Las variantes de producción de SageMaker terminales deben tener un recuento inicial de instancias superior a 1
- SageMaker Los modelos [SageMaker.5] deben tener habilitado el aislamiento de red
- [SageMaker.6] las configuraciones de imagen de la SageMaker aplicación deben estar etiquetadas
- [SageMaker.7] SageMaker las imágenes deben estar etiquetadas
- [SageMaker.8] las instancias de SageMaker notebooks deben ejecutarse en plataformas compatibles
- [SageMaker.9] las definiciones de trabajos de calidad de los SageMaker datos deben tener habilitado el cifrado del tráfico entre contenedores

- [SageMaker.10] Las definiciones de trabajos de explicabilidad del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores
- [SageMaker.11] las definiciones de trabajos SageMaker de calidad de los datos deben tener habilitado el aislamiento de red
- [SageMaker.12] las definiciones de trabajo basadas en el sesgo del SageMaker modelo deben tener habilitado el aislamiento de red
- [SageMaker.13] las definiciones de trabajos de calidad del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores
- [SageMaker.14] los programas SageMaker de monitoreo deben tener habilitado el aislamiento de la red
- [SageMaker.15] Las definiciones de trabajo basadas en el sesgo del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores
- SageMaker Los modelos [SageMaker.16] deben usar un registro privado en la VPC para los contenedores principales
- [SageMaker.17] SageMaker Las tiendas offline de los grupos de funciones deben cifrarse con AWS KMS claves
- [SageMaker.18] las tiendas en línea de grupos de SageMaker funciones con almacenamiento estándar deben cifrarse con AWS KMS claves
- [SageMaker.19] SageMaker los modelos deben usar un registro privado en la VPC para las canalizaciones de inferencia de varios contenedores
- [SES.1] Las listas de contactos de SES deben estar etiquetadas
- [SES.2] Los conjuntos de configuración de SES deben estar etiquetados
- [SES.3] Los conjuntos de configuración de SES deben tener el TLS habilitado para enviar correos electrónicos
- [ServiceCatalog.1] Las carteras de Service Catalog deben compartirse dentro de unAWSsolo una organización
- [SNS.4] Las políticas de acceso a los temas de SNS no deberían permitir el acceso público
- [SQS.1] Las colas de Amazon SQS deben cifrarse en reposo
- [SQS.2] Las colas de SQS deben estar etiquetadas
- [SQS.3] Las políticas de acceso a las colas de SQS no deberían permitir el acceso público
- [SSM.3] Las instancias de Amazon EC2 administradas por Systems Manager deben tener el estado de conformidad de la asociación de COMPLIANT

- [SSM.4] Los documentos SSM no deben ser públicos
- [SSM.5] Los documentos SSM deben estar etiquetados
- [SSM.6] SSM Automation debería tener el registro habilitado CloudWatch
- [SSM.7] Los documentos SSM deben tener habilitada la configuración de bloqueo para compartir en público
- [StepFunctions.1] Step Functions indica que las máquinas deben tener el registro activado
- [Transfer.2] Los servidores Transfer Family no deben usar el protocolo FTP para la conexión de puntos finales
- [Transfer.3] Los conectores Transfer Family deben tener habilitado el registro
- [Transfer.4] Los acuerdos Transfer Family deben estar etiquetados
- [Transfer.5] Los certificados Transfer Family deben estar etiquetados
- [Transfer.6] Los conectores Transfer Family deben estar etiquetados
- [Transfer.7] Los perfiles de Transfer Family deben estar etiquetados
- [WAF.1]AWS WAFEl registro de ACL web global clásico debe estar habilitado
- [WAF.2]AWS WAFLas reglas regionales clásicas deben tener al menos una condición
- [WAF.3]AWS WAFLos grupos de reglas regionales clásicos deben tener al menos una regla
- [WAF.4]AWS WAFLas ACL web regionales clásicas deben tener al menos una regla o grupo de reglas
- [WAF.6]AWS WAFLas reglas globales clásicas deben tener al menos una condición
- [WAF.7]AWS WAFLos grupos de reglas globales clásicos deben tener al menos una regla
- [WAF.8]AWS WAFLas ACL web globales clásicas deben tener al menos una regla o grupo de reglas
- [WAF.10]AWS WAFLas ACL web deben tener al menos una regla o grupo de reglas
- [WAF.12]AWS WAFlas reglas deben tener CloudWatch las métricas habilitadas
- [WorkSpaces.1] los volúmenes de WorkSpaces usuarios deben cifrarse en reposo
- [WorkSpaces.2] los volúmenes WorkSpaces raíz deben cifrarse en reposo

Middle East (Bahrain)

Los siguientes controles no se admiten en la región Medio Oriente (Baréin).

- [APIGateway.11] Los nombres de dominio de API Gateway deben usar las políticas de seguridad recomendadas
- [AppFlow.1] AppFlow Los flujos de Amazon deben estar etiquetados
- [AppRunner.1] Los servicios de App Runner deben estar etiquetados
- [AppRunner.2] Los conectores VPC de App Runner deben estar etiquetados
- [BedrockAgentCore.1] Los AgentCore tiempos de ejecución de Bedrock deben configurarse con el modo de red VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways debería requerir autorización para las solicitudes entrantes
- [BedrockAgentCore.3] Bedrock AgentCore Memory debe estar cifrada y gestionada por el clienteAWS KMSclaves
- [BedrockAgentCore.4] Bedrock AgentCore Gateway debe cifrarse de forma que sea gestionada por el clienteAWS KMSclaves
- [BedrockAgentCore.5] Los navegadores AgentCore personalizados de Bedrock no deberían usar el modo de red pública
- [BedrockAgentCore.6] Los navegadores AgentCore personalizados de Bedrock deberían tener habilitada la grabación de sesiones
- [CloudFront.1] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado
- [CloudFront.3] CloudFront las distribuciones deben requerir el cifrado durante el tránsito
- [CloudFront.4] CloudFront las distribuciones deben tener configurada la conmutación por error de origen
- [CloudFront.5] CloudFront las distribuciones deben tener habilitado el registro
- [CloudFront.6] CloudFront las distribuciones deben tener WAF activado
- [CloudFront.7] CloudFront las distribuciones deben usar certificados personalizados SSL/TLS
- [CloudFront.8] CloudFront las distribuciones deben usar el SNI para atender las solicitudes HTTPS
- [CloudFront.9] CloudFront las distribuciones deben cifrar el tráfico para convertirlo en orígenes personalizados
- [CloudFront.10] CloudFront las distribuciones no deben usar protocolos SSL obsoletos entre ubicaciones de borde y orígenes personalizados
- [CloudFront.12] CloudFront las distribuciones no deben apuntar a orígenes de S3 inexistentes

- [CloudFront.13] CloudFront las distribuciones deben usar el control de acceso al origen
- [CloudFront.14] CloudFront las distribuciones deben estar etiquetadas
- [CloudFront.15] CloudFront las distribuciones deben usar la política de seguridad TLS recomendada
- [CloudFront.16] CloudFront las distribuciones deben usar el control de acceso de origen para los orígenes de las URL de las funciones de Lambda
- [CloudFront.17] CloudFront las distribuciones deben usar grupos de claves confiables para las URL y cookies firmadas
- [CloudTrail.10] Los almacenes de datos de eventos de CloudTrail Lake deben estar cifrados y gestionados por el clienteAWS KMS keys
- [CodeArtifact.1] CodeArtifact los repositorios deben estar etiquetados
- [CodeGuruProfiler.1] Los grupos CodeGuru de creación de perfiles de Profiler deben estar etiquetados
- [CodeGuruReviewer.1] Las asociaciones de repositorios de CodeGuru Reviewer deben estar etiquetadas
- [Connect.1] Los tipos de objetos de los perfiles de clientes de Amazon Connect deben estar etiquetados
- [Connect.2] Las instancias de Connect Customer deben tener el CloudWatch registro habilitado
- [DocumentDB.1] Los clústeres de Amazon DocumentDB deben cifrarse en reposo
- [DocumentDB.2] Los clústeres de Amazon DocumentDB deben tener un período de retención de copias de seguridad adecuado
- [DocumentDB.3] Las instantáneas de clústeres manuales de Amazon DocumentDB no deben ser públicas
- [DocumentDB.4] Los clústeres de Amazon DocumentDB deben publicar los registros de auditoría en Logs CloudWatch
- [DocumentDB.5] Los clústeres de Amazon DocumentDB deben tener habilitada la protección contra eliminaciones
- [DocumentDB.6] Los clústeres de Amazon DocumentDB deben cifrarse en tránsito
- [DynamoDB.3] Los clústeres de DynamoDB Accelerator (DAX) deben cifrarse en reposo
- [DynamoDB.7] Los clústeres de DynamoDB Accelerator deben cifrarse en tránsito
- [EC2.20] Ambos túneles VPN para un AWS Site-to-Site La conexión VPN debería estar activa

- [EC2.24] No se deben utilizar los tipos de instancias paravirtuales de Amazon EC2
- [EC2.58] Las VPC deben configurarse con un punto final de interfaz para los contactos de Systems Manager Incident Manager
- [EC2.60] Las VPC deben configurarse con un punto final de interfaz para Systems Manager Incident Manager
- [EC2.173] Las solicitudes de EC2 Spot Fleet con parámetros de lanzamiento deberían permitir el cifrado de los volúmenes de EBS adjuntos
- [EC2.183] Las conexiones VPN de EC2 deben utilizar el protocolo IKEv2
- [ECR.4] Los repositorios públicos de ECR deben etiquetarse
- [ECR.5] Los repositorios de ECR deben estar cifrados y ser gestionados por el cliente AWS KMS keys
- [ECS.17] Las definiciones de tareas de ECS no deben usar el modo de red host
- [EKS.9] Los grupos de nodos de EKS deben ejecutarse en una versión de Kubernetes compatible
- [ELB.17] Los balanceadores de cargas de aplicaciones y redes con oyentes deben usar las políticas de seguridad recomendadas
- [EventBridge.4] los puntos finales EventBridge globales deberían tener habilitada la replicación de eventos
- [FraudDetector.1] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.2] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas
- [FraudDetector.3] Los resultados de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.4] Las variables de Amazon Fraud Detector deben estar etiquetadas
- [FSx.3] FSx para sistemas de archivos OpenZFS debe configurarse para su implementación Multi-AZ
- [FSx.4] FSx para sistemas de archivos NetApp ONTAP debe configurarse para su implementación Multi-AZ
- [FSx.5] Los sistemas de archivos FSx for Windows File Server deben configurarse para Multi-AZ su implementación
- [GlobalAccelerator.1] Los aceleradores de Global Accelerator deben estar etiquetados
- [Glue.4]AWS GlueLos trabajos de Spark deberían ejecutarse en versiones compatibles deAWS Glue
- [GuardDuty.11] La monitorización del GuardDuty tiempo de ejecución debe estar habilitada

- [GuardDuty.12] La monitorización del tiempo de ejecución de GuardDuty ECS debe estar habilitada
- [GuardDuty.13] La monitorización del tiempo de ejecución de GuardDuty EC2 debe estar habilitada
- [IAM.26] SSL/TLS Los certificados caducados gestionados en IAM deben eliminarse
- [Inspector.3] El escaneo de código Lambda de Amazon Inspector Lambda debe estar activado
- [IoTSiteWise.1]AWSLos modelos SiteWise de activos de IoT deben estar etiquetados
- [IoTSiteWise.2]AWS SiteWise Los paneles de IoT deben estar etiquetados
- [IoTSiteWise.3]AWS SiteWise Las pasarelas de IoT deben estar etiquetadas
- [IoTSiteWise.4]AWS SiteWise Los portales de IoT deben estar etiquetados
- [IoTSiteWise.5]AWS SiteWise Los proyectos de IoT deben estar etiquetados
- [IoTTwinMaker.1]AWSLos trabajos de TwinMaker sincronización de IoT deben estar etiquetados
- [IoTTwinMaker.2]AWS TwinMaker Los espacios de trabajo de IoT deben estar etiquetados
- [IoTTwinMaker.3]AWS TwinMaker Las escenas de IoT deben estar etiquetadas
- [IoTTwinMaker.4]AWS TwinMaker Las entidades de IoT deben estar etiquetadas
- [IoTWireless.1]AWSLos grupos de multidifusión de IoT Wireless deben estar etiquetados
- [IoTWireless.2]AWSLos perfiles de servicio de IoT Wireless deben estar etiquetados
- [IoTWireless.3]AWSLas tareas de IoT FUOTA deben estar etiquetadas
- [IVS.1] Los pares de teclas de reproducción IVS deben estar etiquetados
- [IVS.2] Las configuraciones de grabación de IVS deben estar etiquetadas
- [IVS.3] Los canales IVS deben estar etiquetados
- [MSK.3] Los conectores MSK Connect deben estar cifrados en tránsito
- [MSK.5] Los conectores MSK deben tener el registro activado
- [NetworkFirewall.10] Los firewalls de Network Firewall deben tener habilitada la protección contra cambios de subred
- [RDS.14] Los clústeres de Amazon Aurora deben tener habilitado el retroceso
- [RDS.31] Los grupos de seguridad de la base de datos de RDS deben etiquetarse
- [RDS.41] Las instancias de base de datos de RDS para SQL Server deben cifrarse en tránsito
- [RDS.42] Las instancias de base de datos de RDS para MariaDB deben publicar los registros en Logs CloudWatch

- [RDS.43] Los proxies de bases de datos de RDS deben requerir el cifrado TLS para las conexiones
- [RDS.44] Las instancias de base de datos de RDS para MariaDB deben cifrarse durante el tránsito
- [RDS.45] Los clústeres de bases de datos Aurora MySQL deben tener habilitado el registro de auditoría
- [RDS.46] Las instancias de base de datos de RDS no deben implementarse en subredes públicas con rutas a pasarelas de Internet
- [RDS.51] Los clústeres globales de RDS deben ejecutarse en una versión compatible de Aurora MySQL
- [RedshiftServerless.1] Los grupos de trabajo sin servidor de Amazon Redshift deberían utilizar un enrutamiento de VPC mejorado
- [RedshiftServerless.2] Las conexiones a los grupos de trabajo sin servidor de Redshift deberían ser obligatorias para usar SSL
- [RedshiftServerless.3] Los grupos de trabajo sin servidor de Redshift deberían prohibir el acceso público
- [RedshiftServerless.4] Los espacios de nombres de Redshift Serverless deben cifrarse y administrarse por el clienteAWS KMS keys
- [RedshiftServerless.5] Los espacios de nombres Redshift Serverless no deben usar el nombre de usuario de administrador predeterminado
- [RedshiftServerless.6] Los espacios de nombres Redshift Serverless deberían exportar los registros a los registros CloudWatch
- [Route53.1] Los controles de salud de Route 53 deben estar etiquetados
- [Route53.2] Las zonas alojadas públicas de Route 53 deberían registrar las consultas de DNS
- [S3.24] Los puntos de Multi-Region acceso S3 deben tener habilitada la configuración de bloqueo del acceso público
- [S3.25] Los buckets de directorio de S3 deben tener configuraciones de ciclo de vida
- [SageMaker.8] las instancias de SageMaker notebooks deben ejecutarse en plataformas compatibles
- SageMaker Los modelos [SageMaker.16] deben usar un registro privado en la VPC para los contenedores principales
- [SageMaker.17] SageMaker Las tiendas offline de los grupos de funciones deben cifrarse con AWS KMS claves

- [SageMaker.18] las tiendas en línea de grupos de SageMaker funciones con almacenamiento estándar deben cifrarse con AWS KMS claves
- [SageMaker.19] SageMaker los modelos deben usar un registro privado en la VPC para las canalizaciones de inferencia de varios contenedores
- [SQS.3] Las políticas de acceso a las colas de SQS no deberían permitir el acceso público
- [Transfer.3] Los conectores Transfer Family deben tener habilitado el registro
- [WAF.1]AWS WAFEl registro de ACL web global clásico debe estar habilitado
- [WAF.6]AWS WAFLas reglas globales clásicas deben tener al menos una condición
- [WAF.7]AWS WAFLos grupos de reglas globales clásicos deben tener al menos una regla
- [WAF.8]AWS WAFLas ACL web globales clásicas deben tener al menos una regla o grupo de reglas
- [WorkSpaces.1] los volúmenes de WorkSpaces usuarios deben cifrarse en reposo
- [WorkSpaces.2] los volúmenes WorkSpaces raíz deben cifrarse en reposo

Medio Oriente (EAU)

Los siguientes controles no se admiten en la región Medio Oriente (EAU).

- [APIGateway.8] Las rutas de API Gateway deben especificar un tipo de autorización
- [APIGateway.9] El registro de acceso debe configurarse para las etapas V2 de API Gateway
- [APIGateway.11] Los nombres de dominio de API Gateway deben usar las políticas de seguridad recomendadas
- [Amplify.1] Las aplicaciones Amplify deben estar etiquetadas
- [Amplify.2] Amplify branches debe estar etiquetado
- [AppConfig.1]AWS AppConfiglas aplicaciones deben estar etiquetadas
- [AppConfig.2]AWS AppConfiglos perfiles de configuración deben estar etiquetados
- [AppConfig.3]AWS AppConfiglos entornos deben estar etiquetados
- [AppFlow.1] AppFlow Los flujos de Amazon deben estar etiquetados
- [AppRunner.1] Los servicios de App Runner deben estar etiquetados
- [AppRunner.2] Los conectores VPC de App Runner deben estar etiquetados
- [AppSync.1]AWS AppSyncLas cachés de las API deben estar cifradas en reposo

- [AppSync.6]AWS AppSyncLas cachés de las API deben cifrarse en tránsito
- [Backup.1]AWS Backuplos puntos de recuperación deben estar cifrados en reposo
- [Backup.4]AWS Backuplos planes de informes deben estar etiquetados
- [BedrockAgentCore.1] Los AgentCore tiempos de ejecución de Bedrock deben configurarse con el modo de red VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways debería requerir autorización para las solicitudes entrantes
- [BedrockAgentCore.3] Bedrock AgentCore Memory debe estar cifrada y gestionada por el clienteAWS KMSclaves
- [BedrockAgentCore.4] Bedrock AgentCore Gateway debe cifrarse de forma que sea gestionada por el clienteAWS KMSclaves
- [BedrockAgentCore.5] Los navegadores AgentCore personalizados de Bedrock no deberían usar el modo de red pública
- [BedrockAgentCore.6] Los navegadores AgentCore personalizados de Bedrock deberían tener habilitada la grabación de sesiones
- [CloudFormation.3] las CloudFormation pilas deben tener habilitada la protección de terminación
- [CloudFormation.4] las CloudFormation pilas deben tener funciones de servicio asociadas
- [CloudFront.1] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado
- [CloudFront.3] CloudFront las distribuciones deben requerir el cifrado durante el tránsito
- [CloudFront.4] CloudFront las distribuciones deben tener configurada la conmutación por error de origen
- [CloudFront.5] CloudFront las distribuciones deben tener habilitado el registro
- [CloudFront.6] CloudFront las distribuciones deben tener WAF activado
- [CloudFront.7] CloudFront las distribuciones deben usar certificados personalizados SSL/TLS
- [CloudFront.8] CloudFront las distribuciones deben usar el SNI para atender las solicitudes HTTPS
- [CloudFront.9] CloudFront las distribuciones deben cifrar el tráfico para convertirlo en orígenes personalizados
- [CloudFront.10] CloudFront las distribuciones no deben usar protocolos SSL obsoletos entre ubicaciones de borde y orígenes personalizados
- [CloudFront.12] CloudFront las distribuciones no deben apuntar a orígenes de S3 inexistentes

- [CloudFront.13] CloudFront las distribuciones deben usar el control de acceso al origen
- [CloudFront.14] CloudFront las distribuciones deben estar etiquetadas
- [CloudFront.15] CloudFront las distribuciones deben usar la política de seguridad TLS recomendada
- [CloudFront.16] CloudFront las distribuciones deben usar el control de acceso de origen para los orígenes de las URL de las funciones de Lambda
- [CloudFront.17] CloudFront las distribuciones deben usar grupos de claves confiables para las URL y cookies firmadas
- [CloudTrail.6] Asegúrese de que el depósito de S3 que se utiliza para almacenar CloudTrail los registros no sea de acceso público
- [CodeArtifact.1] CodeArtifact los repositorios deben estar etiquetados
- [CodeGuruProfiler.1] Los grupos CodeGuru de creación de perfiles de Profiler deben estar etiquetados
- [CodeGuruReviewer.1] Las asociaciones de repositorios de CodeGuru Reviewer deben estar etiquetadas
- [Cognito.1] Los grupos de usuarios de Cognito deben tener activada la protección contra amenazas y el modo de aplicación con todas las funciones para la autenticación estándar
- [Cognito.2] Los grupos de identidades de Cognito no deben permitir identidades no autenticadas
- [Connect.1] Los tipos de objetos de los perfiles de clientes de Amazon Connect deben estar etiquetados
- [Connect.2] Las instancias de Connect Customer deben tener el CloudWatch registro habilitado
- [Detective.1] Los gráficos de comportamiento de los detectives deben estar etiquetados
- [DMS.2] Los certificados DMS deben estar etiquetados
- [DMS.3] Las suscripciones a eventos de DMS deben estar etiquetadas
- [DMS.4] Las instancias de replicación de DMS deben estar etiquetadas
- [DMS.5] Los grupos de subredes de replicación del DMS deben estar etiquetados
- [DMS.6] Las instancias de replicación de DMS deben tener habilitada la actualización automática de las versiones secundarias
- [DMS.7] Las tareas de replicación del DMS para la base de datos de destino deben tener el registro habilitado
- [DMS.8] Las tareas de replicación del DMS para la base de datos de origen deben tener el registro activado

- [DMS.9] Los puntos finales del DMS deben usar SSL
- [DMS.10] Los puntos finales de DMS para las bases de datos de Neptune deben tener habilitada la autorización de IAM
- [DMS.11] Los puntos finales de DMS para MongoDB deben tener un mecanismo de autenticación habilitado
- [DMS.12] Los puntos finales de DMS para Redis OSS deben tener el TLS habilitado
- [DMS.13] Las instancias de replicación de DMS deben configurarse para usar varias zonas de disponibilidad
- [DynamoDB.3] Los clústeres de DynamoDB Accelerator (DAX) deben cifrarse en reposo
- [DynamoDB.7] Los clústeres de DynamoDB Accelerator deben cifrarse en tránsito
- [EC2.4] Las instancias EC2 detenidas deben eliminarse después de un período de tiempo específico
- [EC2.14] Los grupos de seguridad no deberían permitir la entrada desde la versión 0.0.0. 0/0 o: :/0 al puerto 3389
- [EC2.22] Deben eliminarse los grupos de seguridad de Amazon EC2 no utilizados
- [EC2.24] No se deben utilizar los tipos de instancias paravirtuales de Amazon EC2
- [EC2.25] Las plantillas de lanzamiento de Amazon EC2 no deben asignar direcciones IP públicas a las interfaces de red
- [EC2.51] Los puntos finales EC2 Client VPN deben tener habilitado el registro de conexiones de clientes
- [EC2.58] Las VPC deben configurarse con un punto final de interfaz para los contactos de Systems Manager Incident Manager
- [EC2.60] Las VPC deben configurarse con un punto final de interfaz para Systems Manager Incident Manager
- [EC2.170] Las plantillas de lanzamiento de EC2 deben utilizar la versión 2 del servicio de metadatos de instancias (IMDSv2)
- [EC2.173] Las solicitudes de EC2 Spot Fleet con parámetros de lanzamiento deberían permitir el cifrado de los volúmenes de EBS adjuntos
- [EC2.175] Las plantillas de lanzamiento de EC2 deben estar etiquetadas
- [EC2.177] Las sesiones de réplica de tráfico de EC2 deben etiquetarse
- [EC2.179] Los objetivos del espejo de tráfico de EC2 deben estar etiquetados

- [EC2.180] Las interfaces de red EC2 deberían tener habilitada source/destination la verificación
- [EC2.181] Las plantillas de lanzamiento de EC2 deberían permitir el cifrado de los volúmenes de EBS adjuntos
- [EC2.183] Las conexiones VPN de EC2 deben utilizar el protocolo IKEv2
- [ECR.4] Los repositorios públicos de ECR deben etiquetarse
- [EFS.1] Elastic File System debe configurarse para cifrar los datos de los archivos en reposo mediante AWS KMS
- [EFS.2] Los volúmenes de Amazon EFS deben figurar en los planes de copia de seguridad
- [EKS.9] Los grupos de nodos de EKS deben ejecutarse en una versión de Kubernetes compatible
- [ELB.14] El balanceador de carga clásico debe configurarse con el modo defensivo o de mitigación de desincronización más estricto
- [ELB.17] Los balanceadores de cargas de aplicaciones y redes con oyentes deben usar las políticas de seguridad recomendadas
- [ELB.18] Los oyentes del balanceador de cargas de red y aplicaciones deben usar protocolos seguros para cifrar los datos en tránsito
- [ElastiCache.1] ElastiCache (Redis OSS) los clústeres deben tener habilitadas las copias de seguridad automáticas
- [ElastiCache.2] ElastiCache los clústeres deberían tener habilitadas las actualizaciones automáticas de las versiones secundarias
- [ElastiCache.3] los grupos de ElastiCache replicación deberían tener habilitada la conmutación por error automática
- [ElastiCache.4] los grupos de ElastiCache replicación deben cifrarse en reposo
- [ElastiCache.5] los grupos de ElastiCache replicación deben cifrarse en tránsito
- [ElastiCache.6] ElastiCache (Redis OSS) Los grupos de replicación de versiones anteriores deberían tener habilitada la autenticación de Redis OSS
- [ElastiCache.7] los ElastiCache clústeres no deben usar el grupo de subredes predeterminado
- [ElasticBeanstalk.1] Los entornos de Elastic Beanstalk deberían tener habilitados los informes de estado mejorados
- [ElasticBeanstalk.2] Las actualizaciones de la plataforma gestionada de Elastic Beanstalk deben estar habilitadas
- [ElasticBeanstalk.3] Elastic Beanstalk debería transmitir los registros a CloudWatch

- [EMR.1] Los nodos principales del clúster de Amazon EMR no deben tener direcciones IP públicas
- [EventBridge.4] los puntos finales EventBridge globales deberían tener habilitada la replicación de eventos
- [FraudDetector.1] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.2] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas
- [FraudDetector.3] Los resultados de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.4] Las variables de Amazon Fraud Detector deben estar etiquetadas
- [GlobalAccelerator.1] Los aceleradores de Global Accelerator deben estar etiquetados
- [Glue.4]AWS GlueLos trabajos de Spark deberían ejecutarse en versiones compatibles deAWS Glue
- GuardDuty Los filtros [GuardDuty.2] deben estar etiquetados
- [IAM.1] Las políticas de IAM no deberían permitir todos los privilegios administrativos «*»
- [IAM.2] Los usuarios de IAM no deberían tener políticas de IAM adjuntas
- [IAM.3] Las claves de acceso de los usuarios de IAM deben rotarse cada 90 días o menos
- [IAM.4] La clave de acceso del usuario raíz de IAM no debería existir
- [IAM.5] La MFA debe estar habilitada para todos los usuarios de IAM que tengan una contraseña de consola
- [IAM.6] La MFA de hardware debe estar habilitada para el usuario root
- [IAM.8] Se deben eliminar las credenciales de usuario de IAM no utilizadas
- [IAM.9] La MFA debe estar habilitada para el usuario root
- [IAM.18] Asegúrese de que se haya creado una función de soporte para gestionar los incidentes conAWS Support
- [IAM.19] La MFA debe estar habilitada para todos los usuarios de IAM
- [IAM.21] Las políticas de IAM gestionadas por el cliente que cree no deberían permitir acciones comodín en los servicios
- [IAM.22] Se deben eliminar las credenciales de usuario de IAM que no se hayan utilizado durante 45 días
- [IAM.24] Las funciones de IAM deben estar etiquetadas
- [IAM.25] Los usuarios de IAM deben estar etiquetados
- [IAM.26] SSL/TLS Los certificados caducados gestionados en IAM deben eliminarse

- [IAM.27] Las identidades de IAM no deberían tener la AWSCloudShellFullAccess política adjunta
- [Inspector.1] El escaneo EC2 de Amazon Inspector debe estar activado
- [Inspector.2] El escaneo ECR de Amazon Inspector debe estar activado
- [Inspector.3] El escaneo de código Lambda de Amazon Inspector Lambda debe estar activado
- [Inspector.4] El escaneo estándar de Amazon Inspector Lambda debe estar activado
- [IoTSiteWise.1]AWSLos modelos SiteWise de activos de IoT deben estar etiquetados
- [IoTSiteWise.2]AWS SiteWise Los paneles de IoT deben estar etiquetados
- [IoTSiteWise.3]AWS SiteWise Las pasarelas de IoT deben estar etiquetadas
- [IoTSiteWise.4]AWS SiteWise Los portales de IoT deben estar etiquetados
- [IoTSiteWise.5]AWS SiteWise Los proyectos de IoT deben estar etiquetados
- [IoTTwinMaker.1]AWSLos trabajos de TwinMaker sincronización de IoT deben estar etiquetados
- [IoTTwinMaker.2]AWS TwinMaker Los espacios de trabajo de IoT deben estar etiquetados
- [IoTTwinMaker.3]AWS TwinMaker Las escenas de IoT deben estar etiquetadas
- [IoTTwinMaker.4]AWS TwinMaker Las entidades de IoT deben estar etiquetadas
- [IoTWireless.1]AWSLos grupos de multidifusión de IoT Wireless deben estar etiquetados
- [IoTWireless.2]AWSLos perfiles de servicio de IoT Wireless deben estar etiquetados
- [IoTWireless.3]AWSLas tareas de IoT FUOTA deben estar etiquetadas
- [IVS.1] Los pares de teclas de reproducción IVS deben estar etiquetados
- [IVS.2] Las configuraciones de grabación de IVS deben estar etiquetadas
- [IVS.3] Los canales IVS deben estar etiquetados
- [Keyspaces.1] Los espacios clave de Amazon Keyspaces deben estar etiquetados
- [KMS.1] Las políticas gestionadas por los clientes de IAM no deberían permitir acciones de descifrado en todas las claves de KMS
- [KMS.2] Los directores de IAM no deberían tener políticas integradas de IAM que permitan realizar acciones de descifrado en todas las claves de KMS
- [Lambda.7] Las funciones de Lambda deberían tener AWS X-Ray el rastreo activo está habilitado
- [Macie.1] Amazon Macie debería estar activado
- [Macie.2] La detección automática de datos confidenciales por parte de Macie debería estar habilitada
- [MSK.3] Los conectores MSK Connect deben estar cifrados en tránsito

- [MSK.4] Los clústeres de MSK deben tener el acceso público deshabilitado
- [MSK.5] Los conectores MSK deben tener el registro activado
- [MSK.6] Los clústeres de MSK deberían deshabilitar el acceso no autenticado
- [Opensearch.1] OpenSearch los dominios deben tener activado el cifrado en reposo
- [Opensearch.2] OpenSearch los dominios no deben ser de acceso público
- [Opensearch.3] OpenSearch los dominios deben cifrar los datos enviados entre nodos
- [Opensearch.4] El registro de errores de OpenSearch dominio en Logs debe estar habilitado CloudWatch
- [Opensearch.5] OpenSearch los dominios deben tener activado el registro de auditoría
- [Opensearch.6] OpenSearch los dominios deben tener al menos tres nodos de datos
- [Opensearch.7] OpenSearch los dominios deben tener habilitado un control de acceso detallado
- [Opensearch.8] Las conexiones a los OpenSearch dominios deben cifrarse con la última política de seguridad de TLS
- [Opensearch.9] OpenSearch los dominios deben estar etiquetados
- [Opensearch.10] OpenSearch los dominios deben tener instalada la última actualización de software
- [Opensearch.11] OpenSearch los dominios deben tener al menos tres nodos principales dedicados
- [RDS.14] Los clústeres de Amazon Aurora deben tener habilitado el retroceso
- [RDS.31] Los grupos de seguridad de la base de datos de RDS deben etiquetarse
- [RDS.35] Los clústeres de bases de datos de RDS deben tener habilitada la actualización automática de versiones secundarias
- [RDS.51] Los clústeres globales de RDS deben ejecutarse en una versión compatible de Aurora MySQL
- [Redshift.18] Los clústeres de Redshift deberían tener Multi-AZ las implementaciones habilitadas
- [RedshiftServerless.1] Los grupos de trabajo sin servidor de Amazon Redshift deberían utilizar un enrutamiento de VPC mejorado
- [RedshiftServerless.2] Las conexiones a los grupos de trabajo sin servidor de Redshift deberían ser obligatorias para usar SSL
- [Route53.1] Los controles de salud de Route 53 deben estar etiquetados
- [Route53.2] Las zonas alojadas públicas de Route 53 deberían registrar las consultas de DNS

- [S3.24] Los puntos de Multi-Region acceso S3 deben tener habilitada la configuración de bloqueo del acceso público
- [S3.25] Los buckets de directorio de S3 deben tener configuraciones de ciclo de vida
- [SageMaker.1] Las instancias de Amazon SageMaker Notebook no deberían tener acceso directo a Internet
- [SageMaker.2] las instancias de SageMaker cuadernos deben lanzarse en una VPC personalizada
- [SageMaker.3] Los usuarios no deben tener acceso root a las instancias de los SageMaker cuadernos
- SageMaker Los modelos [SageMaker.5] deben tener habilitado el aislamiento de red
- [SageMaker.9] las definiciones de trabajos de calidad de los SageMaker datos deben tener habilitado el cifrado del tráfico entre contenedores
- [SageMaker.10] Las definiciones de trabajos de explicabilidad del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores
- [SageMaker.11] las definiciones de trabajos SageMaker de calidad de los datos deben tener habilitado el aislamiento de red
- [SageMaker.12] las definiciones de trabajo basadas en el sesgo del SageMaker modelo deben tener habilitado el aislamiento de red
- [SageMaker.13] las definiciones de trabajos de calidad del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores
- [SageMaker.14] los programas SageMaker de monitoreo deben tener habilitado el aislamiento de la red
- [SageMaker.15] Las definiciones de trabajo basadas en el sesgo del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores
- SageMaker Los modelos [SageMaker.16] deben usar un registro privado en la VPC para los contenedores principales
- [SageMaker.17] SageMaker Las tiendas offline de los grupos de funciones deben cifrarse con AWS KMS claves
- [SageMaker.18] las tiendas en línea de grupos de SageMaker funciones con almacenamiento estándar deben cifrarse con AWS KMS claves
- [SageMaker.19] SageMaker los modelos deben usar un registro privado en la VPC para las canalizaciones de inferencia de varios contenedores
- [SES.1] Las listas de contactos de SES deben estar etiquetadas
- [SES.2] Los conjuntos de configuración de SES deben estar etiquetados

- [SES.3] Los conjuntos de configuración de SES deben tener el TLS habilitado para enviar correos electrónicos
- [SQS.1] Las colas de Amazon SQS deben cifrarse en reposo
- [SQS.2] Las colas de SQS deben estar etiquetadas
- [SQS.3] Las políticas de acceso a las colas de SQS no deberían permitir el acceso público
- [SSM.6] SSM Automation debería tener el registro habilitado CloudWatch
- [SSM.7] Los documentos SSM deben tener habilitada la configuración de bloqueo para compartir en público
- [WAF.1]AWS WAFEl registro de ACL web global clásico debe estar habilitado
- [WAF.3]AWS WAFLos grupos de reglas regionales clásicos deben tener al menos una regla
- [WAF.6]AWS WAFLas reglas globales clásicas deben tener al menos una condición
- [WAF.7]AWS WAFLos grupos de reglas globales clásicos deben tener al menos una regla
- [WAF.8]AWS WAFLas ACL web globales clásicas deben tener al menos una regla o grupo de reglas
- [WAF.10]AWS WAFLas ACL web deben tener al menos una regla o grupo de reglas
- [WorkSpaces.1] los volúmenes de WorkSpaces usuarios deben cifrarse en reposo
- [WorkSpaces.2] los volúmenes WorkSpaces raíz deben cifrarse en reposo

América del Sur (São Paulo)

Los siguientes controles no se admiten en la región América del Sur (São Paulo).

- [AppRunner.1] Los servicios de App Runner deben estar etiquetados
- [AppRunner.2] Los conectores VPC de App Runner deben estar etiquetados
- [BedrockAgentCore.1] Los AgentCore tiempos de ejecución de Bedrock deben configurarse con el modo de red VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways debería requerir autorización para las solicitudes entrantes
- [BedrockAgentCore.3] Bedrock AgentCore Memory debe estar cifrada y gestionada por el clienteAWS KMSclaves
- [BedrockAgentCore.4] Bedrock AgentCore Gateway debe cifrarse de forma que sea gestionada por el clienteAWS KMSclaves

- [BedrockAgentCore.5] Los navegadores AgentCore personalizados de Bedrock no deberían usar el modo de red pública
- [BedrockAgentCore.6] Los navegadores AgentCore personalizados de Bedrock deberían tener habilitada la grabación de sesiones
- [CloudFront.1] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado
- [CloudFront.3] CloudFront las distribuciones deben requerir el cifrado durante el tránsito
- [CloudFront.4] CloudFront las distribuciones deben tener configurada la conmutación por error de origen
- [CloudFront.5] CloudFront las distribuciones deben tener habilitado el registro
- [CloudFront.6] CloudFront las distribuciones deben tener WAF activado
- [CloudFront.7] CloudFront las distribuciones deben usar certificados personalizados SSL/TLS
- [CloudFront.8] CloudFront las distribuciones deben usar el SNI para atender las solicitudes HTTPS
- [CloudFront.9] CloudFront las distribuciones deben cifrar el tráfico para convertirlo en orígenes personalizados
- [CloudFront.10] CloudFront las distribuciones no deben usar protocolos SSL obsoletos entre ubicaciones de borde y orígenes personalizados
- [CloudFront.12] CloudFront las distribuciones no deben apuntar a orígenes de S3 inexistentes
- [CloudFront.13] CloudFront las distribuciones deben usar el control de acceso al origen
- [CloudFront.14] CloudFront las distribuciones deben estar etiquetadas
- [CloudFront.15] CloudFront las distribuciones deben usar la política de seguridad TLS recomendada
- [CloudFront.16] CloudFront las distribuciones deben usar el control de acceso de origen para los orígenes de las URL de las funciones de Lambda
- [CloudFront.17] CloudFront las distribuciones deben usar grupos de claves confiables para las URL y cookies firmadas
- [CodeArtifact.1] CodeArtifact los repositorios deben estar etiquetados
- [CodeGuruProfiler.1] Los grupos CodeGuru de creación de perfiles de Profiler deben estar etiquetados
- [CodeGuruReviewer.1] Las asociaciones de repositorios de CodeGuru Reviewer deben estar etiquetadas
- [Cognito.5] La MFA debe estar habilitada para los grupos de usuarios de Cognito

- [Connect.1] Los tipos de objetos de los perfiles de clientes de Amazon Connect deben estar etiquetados
- [Connect.2] Las instancias de Connect Customer deben tener el CloudWatch registro habilitado
- [EC2.173] Las solicitudes de EC2 Spot Fleet con parámetros de lanzamiento deberían permitir el cifrado de los volúmenes de EBS adjuntos
- [ECR.4] Los repositorios públicos de ECR deben etiquetarse
- [FraudDetector.1] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.2] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas
- [FraudDetector.3] Los resultados de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.4] Las variables de Amazon Fraud Detector deben estar etiquetadas
- [GlobalAccelerator.1] Los aceleradores de Global Accelerator deben estar etiquetados
- [IAM.26] SSL/TLS Los certificados caducados gestionados en IAM deben eliminarse
- [Inspector.3] El escaneo de código Lambda de Amazon Inspector Lambda debe estar activado
- [IoT.1]AWS IoT Device Defenderlos perfiles de seguridad deben estar etiquetados
- [IoT.2]AWS IoT Corelas acciones de mitigación deben estar etiquetadas
- [IoT.3]AWS IoT Corelas dimensiones deben estar etiquetadas
- [IoTSiteWise.1]AWSLos modelos SiteWise de activos de IoT deben estar etiquetados
- [IoTSiteWise.2]AWS SiteWise Los paneles de IoT deben estar etiquetados
- [IoTSiteWise.3]AWS SiteWise Las pasarelas de IoT deben estar etiquetadas
- [IoTSiteWise.4]AWS SiteWise Los portales de IoT deben estar etiquetados
- [IoTSiteWise.5]AWS SiteWise Los proyectos de IoT deben estar etiquetados
- [IoTTwinMaker.1]AWSLos trabajos de TwinMaker sincronización de IoT deben estar etiquetados
- [IoTTwinMaker.2]AWS TwinMaker Los espacios de trabajo de IoT deben estar etiquetados
- [IoTTwinMaker.3]AWS TwinMaker Las escenas de IoT deben estar etiquetadas
- [IoTTwinMaker.4]AWS TwinMaker Las entidades de IoT deben estar etiquetadas
- [IVS.1] Los pares de teclas de reproducción IVS deben estar etiquetados
- [IVS.2] Las configuraciones de grabación de IVS deben estar etiquetadas
- [IVS.3] Los canales IVS deben estar etiquetados
- [RDS.14] Los clústeres de Amazon Aurora deben tener habilitado el retroceso

- [RedshiftServerless.1] Los grupos de trabajo sin servidor de Amazon Redshift deberían utilizar un enrutamiento de VPC mejorado
- [RedshiftServerless.2] Las conexiones a los grupos de trabajo sin servidor de Redshift deberían ser obligatorias para usar SSL
- [Route53.1] Los controles de salud de Route 53 deben estar etiquetados
- [Route53.2] Las zonas alojadas públicas de Route 53 deberían registrar las consultas de DNS
- [S3.24] Los puntos de Multi-Region acceso S3 deben tener habilitada la configuración de bloqueo del acceso público
- [S3.25] Los buckets de directorio de S3 deben tener configuraciones de ciclo de vida
- [WAF.1]AWS WAFEl registro de ACL web global clásico debe estar habilitado
- [WAF.6]AWS WAFLas reglas globales clásicas deben tener al menos una condición
- [WAF.7]AWS WAFLos grupos de reglas globales clásicos deben tener al menos una regla
- [WAF.8]AWS WAFLas ACL web globales clásicas deben tener al menos una regla o grupo de reglas

AWS GovCloud (US-East)

Los siguientes controles no son compatibles en la AWS GovCloud (US-East) región.

- [ACM.2] Los certificados RSA gestionados por ACM deben utilizar una longitud de clave de al menos 2048 bits
- [Account.1] La información de contacto de seguridad debe proporcionarse para unCuenta de AWS
- [Account.2]Cuentas de AWSdebe formar parte de unAWS Organizationsorganización
- [APIGateway.2] Las etapas de la API REST de API Gateway deben configurarse para usar certificados SSL para la autenticación de backend
- [APIGateway.8] Las rutas de API Gateway deben especificar un tipo de autorización
- [APIGateway.9] El registro de acceso debe configurarse para las etapas V2 de API Gateway
- [APIGateway.10] Las integraciones de API Gateway V2 deben usar HTTPS para las conexiones privadas
- [APIGateway.11] Los nombres de dominio de API Gateway deben usar las políticas de seguridad recomendadas
- [Amplify.1] Las aplicaciones Amplify deben estar etiquetadas

- [Amplify.2] Amplify branches debe estar etiquetado
- [AppConfig.1]AWS AppConfiglas aplicaciones deben estar etiquetadas
- [AppConfig.2]AWS AppConfiglos perfiles de configuración deben estar etiquetados
- [AppConfig.3]AWS AppConfiglos entornos deben estar etiquetados
- [AppConfig.4]AWS AppConfiglas asociaciones de extensiones deben estar etiquetadas
- [AppFlow.1] AppFlow Los flujos de Amazon deben estar etiquetados
- [AppRunner.1] Los servicios de App Runner deben estar etiquetados
- [AppRunner.2] Los conectores VPC de App Runner deben estar etiquetados
- [AppSync.1]AWS AppSyncLas cachés de las API deben estar cifradas en reposo
- [AppSync.2]AWS AppSyncdebe tener habilitado el registro a nivel de campo
- [AppSync.4]AWS AppSyncLas API de GraphQL deben estar etiquetadas
- [AppSync.5]AWS AppSyncLas API de GraphQL no deben autenticarse con claves de API
- [AppSync.6]AWS AppSyncLas cachés de las API deben cifrarse en tránsito
- [AutoScaling.2] El grupo Amazon EC2 Auto Scaling debe cubrir varias zonas de disponibilidad
- [AutoScaling.3] Las configuraciones de lanzamiento grupal de Auto Scaling deberían configurar las instancias EC2 para que requieran la versión 2 del Servicio de Metadatos de Instancia (IMDSv2)
- [AutoScaling.6] Los grupos de Auto Scaling deben usar varios tipos de instancias en múltiples zonas de disponibilidad
- [AutoScaling.9] Los grupos de Amazon EC2 Auto Scaling deben utilizar las plantillas de lanzamiento de Amazon EC2
- [Backup.4]AWS Backuplos planes de informes deben estar etiquetados
- [Batch.1] Las colas de trabajos por lotes deben estar etiquetadas
- [Batch.2] Las políticas de programación de lotes deben estar etiquetadas
- [Batch.3] Los entornos de procesamiento por lotes deben etiquetarse
- [Batch.4] Las propiedades de los recursos de cómputo en los entornos de cómputo por lotes gestionados deben estar etiquetadas
- [BedrockAgentCore.1] Los AgentCore tiempos de ejecución de Bedrock deben configurarse con el modo de red VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways debería requerir autorización para las solicitudes entrantes

- [BedrockAgentCore.3] Bedrock AgentCore Memory debe estar cifrada y gestionada por el clienteAWS KMSclaves
- [BedrockAgentCore.4] Bedrock AgentCore Gateway debe cifrarse de forma que sea gestionada por el clienteAWS KMSclaves
- [BedrockAgentCore.5] Los navegadores AgentCore personalizados de Bedrock no deberían usar el modo de red pública
- [BedrockAgentCore.6] Los navegadores AgentCore personalizados de Bedrock deberían tener habilitada la grabación de sesiones
- [CloudFront.1] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado
- [CloudFront.3] CloudFront las distribuciones deben requerir el cifrado durante el tránsito
- [CloudFront.4] CloudFront las distribuciones deben tener configurada la conmutación por error de origen
- [CloudFront.5] CloudFront las distribuciones deben tener habilitado el registro
- [CloudFront.6] CloudFront las distribuciones deben tener WAF activado
- [CloudFront.7] CloudFront las distribuciones deben usar certificados personalizados SSL/TLS
- [CloudFront.8] CloudFront las distribuciones deben usar el SNI para atender las solicitudes HTTPS
- [CloudFront.9] CloudFront las distribuciones deben cifrar el tráfico para convertirlo en orígenes personalizados
- [CloudFront.10] CloudFront las distribuciones no deben usar protocolos SSL obsoletos entre ubicaciones de borde y orígenes personalizados
- [CloudFront.12] CloudFront las distribuciones no deben apuntar a orígenes de S3 inexistentes
- [CloudFront.13] CloudFront las distribuciones deben usar el control de acceso al origen
- [CloudFront.14] CloudFront las distribuciones deben estar etiquetadas
- [CloudFront.15] CloudFront las distribuciones deben usar la política de seguridad TLS recomendada
- [CloudFront.16] CloudFront las distribuciones deben usar el control de acceso de origen para los orígenes de las URL de las funciones de Lambda
- [CloudFront.17] CloudFront las distribuciones deben usar grupos de claves confiables para las URL y cookies firmadas
- [CloudWatch.17] las acciones CloudWatch de alarma deben estar activadas

- [CodeArtifact.1] CodeArtifact los repositorios deben estar etiquetados
- [CodeBuild.3] Los registros de CodeBuild S3 deben estar cifrados
- [CodeBuild.4] los entornos de CodeBuild proyectos deben tener un registroAWS ConfigDuración
- [CodeGuruProfiler.1] Los grupos CodeGuru de creación de perfiles de Profiler deben estar etiquetados
- [CodeGuruReviewer.1] Las asociaciones de repositorios de CodeGuru Reviewer deben estar etiquetadas
- [Cognito.1] Los grupos de usuarios de Cognito deben tener activada la protección contra amenazas y el modo de aplicación con todas las funciones para la autenticación estándar
- [Cognito.2] Los grupos de identidades de Cognito no deben permitir identidades no autenticadas
- [Cognito.3] Las políticas de contraseñas para los grupos de usuarios de Cognito deben tener configuraciones sólidas
- [Cognito.4] Los grupos de usuarios de Cognito deben tener activada la protección contra amenazas y el modo de aplicación con todas las funciones para la autenticación personalizada
- [Cognito.5] La MFA debe estar habilitada para los grupos de usuarios de Cognito
- [Cognito.6] Los grupos de usuarios de Cognito deben tener habilitada la protección contra la eliminación
- [Connect.1] Los tipos de objetos de los perfiles de clientes de Amazon Connect deben estar etiquetados
- [Connect.2] Las instancias de Connect Customer deben tener el CloudWatch registro habilitado
- [DataSync.2] DataSync las tareas deben estar etiquetadas
- [DMS.2] Los certificados DMS deben estar etiquetados
- [DMS.6] Las instancias de replicación de DMS deben tener habilitada la actualización automática de las versiones secundarias
- [DMS.7] Las tareas de replicación del DMS para la base de datos de destino deben tener el registro habilitado
- [DMS.8] Las tareas de replicación del DMS para la base de datos de origen deben tener el registro activado
- [DMS.9] Los puntos finales del DMS deben usar SSL
- [DocumentDB.1] Los clústeres de Amazon DocumentDB deben cifrarse en reposo
- [DocumentDB.2] Los clústeres de Amazon DocumentDB deben tener un período de retención de copias de seguridad adecuado

- [DocumentDB.3] Las instantáneas de clústeres manuales de Amazon DocumentDB no deben ser públicas
- [DocumentDB.4] Los clústeres de Amazon DocumentDB deben publicar los registros de auditoría en Logs CloudWatch
- [DocumentDB.5] Los clústeres de Amazon DocumentDB deben tener habilitada la protección contra eliminaciones
- [DynamoDB.3] Los clústeres de DynamoDB Accelerator (DAX) deben cifrarse en reposo
- [DynamoDB.7] Los clústeres de DynamoDB Accelerator deben cifrarse en tránsito
- [EC2.21] Las ACL de red no deberían permitir la entrada desde la versión 0.0.0. 0/0 al puerto 22 o al puerto 3389
- [EC2.22] Deben eliminarse los grupos de seguridad de Amazon EC2 no utilizados
- [EC2.23] Amazon EC2 Transit Gateways no debe aceptar automáticamente las solicitudes de adjuntos de VPC
- [EC2.24] No se deben utilizar los tipos de instancias paravirtuales de Amazon EC2
- [EC2.25] Las plantillas de lanzamiento de Amazon EC2 no deben asignar direcciones IP públicas a las interfaces de red
- [EC2.47] Los servicios de punto final de Amazon VPC deben estar etiquetados
- [EC2.52] Las pasarelas de tránsito EC2 deben estar etiquetadas
- [EC2.58] Las VPC deben configurarse con un punto final de interfaz para los contactos de Systems Manager Incident Manager
- [EC2.60] Las VPC deben configurarse con un punto final de interfaz para Systems Manager Incident Manager
- [EC2.170] Las plantillas de lanzamiento de EC2 deben utilizar la versión 2 del servicio de metadatos de instancias (IMDSv2)
- [EC2.173] Las solicitudes de EC2 Spot Fleet con parámetros de lanzamiento deberían permitir el cifrado de los volúmenes de EBS adjuntos
- [EC2.174] Los conjuntos de opciones DHCP de EC2 deben estar etiquetados
- [EC2.175] Las plantillas de lanzamiento de EC2 deben estar etiquetadas
- [EC2.176] Las listas de prefijos de EC2 deben estar etiquetadas
- [EC2.177] Las sesiones de réplica de tráfico de EC2 deben etiquetarse
- [EC2.178] Los filtros espejo de tráfico EC2 deben estar etiquetados

- [EC2.179] Los objetivos del espejo de tráfico de EC2 deben estar etiquetados
- [ECR.1] Los repositorios privados de ECR deben tener configurado el escaneo de imágenes
- [ECR.2] Los repositorios privados de ECR deben tener configurada la inmutabilidad de etiquetas
- [ECR.3] Los repositorios de ECR deben tener configurada al menos una política de ciclo de vida
- [ECR.4] Los repositorios públicos de ECR deben etiquetarse
- [ECS.3] Las definiciones de tareas de ECS no deben compartir el espacio de nombres del proceso del host
- [ECS.4] Los contenedores ECS deben ejecutarse sin privilegios
- [ECS.5] Las definiciones de tareas de ECS deben configurar los contenedores para que se limiten al acceso de solo lectura a los sistemas de archivos raíz
- [ECS.8] Los secretos no deben transmitirse como variables de entorno de contenedores
- [ECS.9] Las definiciones de tareas de ECS deben tener una configuración de registro
- [ECS.10] Los servicios Fargate de ECS deberían ejecutarse en la última versión de la plataforma Fargate
- [ECS.12] Los clústeres de ECS deben usar Container Insights
- [EFS.3] Los puntos de acceso EFS deben exigir un directorio raíz
- [EFS.4] Los puntos de acceso EFS deben exigir la identidad del usuario
- [EKS.2] Los clústeres de EKS deben ejecutarse en una versión de Kubernetes compatible
- [EKS.8] Los clústeres de EKS deben tener habilitado el registro de auditoría
- [ELB.10] El balanceador de carga clásico debe abarcar varias zonas de disponibilidad
- [ELB.12] El balanceador de carga de aplicaciones debe configurarse con el modo defensivo o de mitigación de desincronización más estricto
- [ELB.13] Los balanceadores de carga de aplicaciones, redes y puertas de enlace deben abarcar varias zonas de disponibilidad
- [ELB.14] El balanceador de carga clásico debe configurarse con el modo defensivo o de mitigación de desincronización más estricto
- [ELB.21] Los grupos destinatarios de Application and Network Load Balancer deben utilizar protocolos de control de estado cifrados
- [ELB.22] Los grupos objetivo del ELB deben usar protocolos de transporte cifrados
- [ElastiCache.1] ElastiCache (Redis OSS) los clústeres deben tener habilitadas las copias de seguridad automáticas

- [ElastiCache.2] ElastiCache los clústeres deberían tener habilitadas las actualizaciones automáticas de las versiones secundarias
- [ElastiCache.3] los grupos de ElastiCache replicación deberían tener habilitada la conmutación por error automática
- [ElastiCache.4] los grupos de ElastiCache replicación deben cifrarse en reposo
- [ElastiCache.5] los grupos de ElastiCache replicación deben cifrarse en tránsito
- [ElastiCache.6] ElastiCache (Redis OSS) Los grupos de replicación de versiones anteriores deberían tener habilitada la autenticación de Redis OSS
- [ElastiCache.7] los ElastiCache clústeres no deben usar el grupo de subredes predeterminado
- [ElasticBeanstalk.1] Los entornos de Elastic Beanstalk deberían tener habilitados los informes de estado mejorados
- [ElasticBeanstalk.2] Las actualizaciones de la plataforma gestionada de Elastic Beanstalk deben estar habilitadas
- [ElasticBeanstalk.3] Elastic Beanstalk debería transmitir los registros a CloudWatch
- [EMR.2] La configuración de acceso público del bloque Amazon EMR debe estar habilitada
- [EMR.3] Las configuraciones de seguridad de Amazon EMR deben cifrarse en reposo
- [EMR.4] Las configuraciones de seguridad de Amazon EMR deben cifrarse en tránsito
- [ES.4] Debería estar habilitado el registro de errores de dominio de Elasticsearch en Logs CloudWatch
- [EventBridge.3] los autobuses de eventos EventBridge personalizados deben tener adjunta una política basada en los recursos
- [EventBridge.4] los puntos finales EventBridge globales deberían tener habilitada la replicación de eventos
- [FraudDetector.1] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.2] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas
- [FraudDetector.3] Los resultados de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.4] Las variables de Amazon Fraud Detector deben estar etiquetadas
- [FSx.1] FSx para sistemas de archivos OpenZFS debe configurarse para copiar etiquetas en copias de seguridad y volúmenes
- [FSx.2] Los sistemas de archivos FSx for Lustre deben configurarse para copiar etiquetas a las copias de seguridad

- [GlobalAccelerator.1] Los aceleradores de Global Accelerator deben estar etiquetados
- [Glue.3]AWS GlueLas transformaciones de aprendizaje automático deben cifrarse en reposo
- [GuardDuty.7] La monitorización del tiempo de ejecución de GuardDuty EKS debe estar habilitada
- [GuardDuty.8] La protección contra GuardDuty malware para EC2 debe estar habilitada
- [GuardDuty.9] La protección GuardDuty RDS debe estar habilitada
- [GuardDuty.11] La monitorización del GuardDuty tiempo de ejecución debe estar habilitada
- [GuardDuty.12] La monitorización del tiempo de ejecución de GuardDuty ECS debe estar habilitada
- [GuardDuty.13] La monitorización del tiempo de ejecución de GuardDuty EC2 debe estar habilitada
- [IAM.6] La MFA de hardware debe estar habilitada para el usuario root
- [IAM.9] La MFA debe estar habilitada para el usuario root
- [IAM.21] Las políticas de IAM gestionadas por el cliente que cree no deberían permitir acciones comodín en los servicios
- [IAM.24] Las funciones de IAM deben estar etiquetadas
- [IAM.25] Los usuarios de IAM deben estar etiquetados
- [IAM.26] SSL/TLS Los certificados caducados gestionados en IAM deben eliminarse
- [IAM.28] El analizador de acceso externo de IAM Access Analyzer debe estar habilitado
- [Inspector.3] El escaneo de código Lambda de Amazon Inspector Lambda debe estar activado
- [IoTSiteWise.1]AWSLos modelos SiteWise de activos de IoT deben estar etiquetados
- [IoTSiteWise.2]AWS SiteWise Los paneles de IoT deben estar etiquetados
- [IoTSiteWise.3]AWS SiteWise Las pasarelas de IoT deben estar etiquetadas
- [IoTSiteWise.4]AWS SiteWise Los portales de IoT deben estar etiquetados
- [IoTSiteWise.5]AWS SiteWise Los proyectos de IoT deben estar etiquetados
- [IoTTwinMaker.1]AWSLos trabajos de TwinMaker sincronización de IoT deben estar etiquetados
- [IoTTwinMaker.2]AWS TwinMaker Los espacios de trabajo de IoT deben estar etiquetados
- [IoTTwinMaker.3]AWS TwinMaker Las escenas de IoT deben estar etiquetadas
- [IoTTwinMaker.4]AWS TwinMaker Las entidades de IoT deben estar etiquetadas
- [IoTWireless.1]AWSLos grupos de multidifusión de IoT Wireless deben estar etiquetados
- [IoTWireless.2]AWSLos perfiles de servicio de IoT Wireless deben estar etiquetados

- [IoTWireless.3]AWSLas tareas de IoT FUOTA deben estar etiquetadas
- [IVS.1] Los pares de teclas de reproducción IVS deben estar etiquetados
- [IVS.2] Las configuraciones de grabación de IVS deben estar etiquetadas
- [IVS.3] Los canales IVS deben estar etiquetados
- [Keyspaces.1] Los espacios clave de Amazon Keyspaces deben estar etiquetados
- [Kinesis.1] Las transmisiones de Kinesis deben cifrarse en reposo
- [KMS.5] Las claves KMS no deben ser de acceso público
- [Lambda.5] Las funciones de VPC Lambda deben funcionar en varias zonas de disponibilidad
- [Macie.1] Amazon Macie debería estar activado
- [Macie.2] La detección automática de datos confidenciales por parte de Macie debería estar habilitada
- [MQ.5] Los corredores de ActiveMQ deberían usar el modo de implementación active/standby
- [MQ.6] Los corredores de RabbitMQ deberían usar el modo de despliegue de clústeres
- [MSK.1] Los clústeres de MSK deben cifrarse en tránsito entre los nodos de intermediación
- [MSK.2] Los clústeres de MSK deberían tener configurada una supervisión mejorada
- [MSK.3] Los conectores MSK Connect deben estar cifrados en tránsito
- [MSK.5] Los conectores MSK deben tener el registro activado
- [Neptune.1] Los clústeres de bases de datos de Neptune deben cifrarse en reposo
- [Neptune.2] Los clústeres de bases de datos de Neptune deberían publicar registros de auditoría en Logs CloudWatch
- [Neptune.3] Las instantáneas del clúster de base de datos de Neptune no deben ser públicas
- [Neptune.4] Los clústeres de base de datos de Neptune deben tener habilitada la protección contra eliminación
- [Neptune.5] Los clústeres de Neptune DB deberían tener habilitadas las copias de seguridad automatizadas
- [Neptune.6] Las instantáneas del clúster de base de datos de Neptune deben cifrarse en reposo
- [Neptune.7] Los clústeres de base de datos de Neptune deben tener habilitada la autenticación de bases de datos de IAM
- [Neptune.8] Los clústeres de bases de datos de Neptune deben configurarse para copiar etiquetas a las instantáneas

- [Neptune.9] Los clústeres de base de datos Neptune deben implementarse en varias zonas de disponibilidad
- [NetworkFirewall.1] Los firewalls de Network Firewall deben implementarse en varias zonas de disponibilidad
- [NetworkFirewall.2] El registro de Network Firewall debe estar habilitado
- [NetworkFirewall.3] Las políticas de Network Firewall deben tener asociado al menos un grupo de reglas
- [NetworkFirewall.4] La acción sin estado predeterminada para las políticas de Network Firewall debe ser eliminar o reenviar paquetes completos
- [NetworkFirewall.5] La acción sin estado predeterminada para las políticas de Network Firewall debe ser eliminar o reenviar paquetes fragmentados
- [NetworkFirewall.6] El grupo de reglas de Stateless Network Firewall no debe estar vacío
- [NetworkFirewall.9] Los firewalls de Network Firewall deben tener habilitada la protección de eliminación
- [Opensearch.1] OpenSearch los dominios deben tener activado el cifrado en reposo
- [Opensearch.2] OpenSearch los dominios no deben ser de acceso público
- [Opensearch.3] OpenSearch los dominios deben cifrar los datos enviados entre nodos
- [Opensearch.4] El registro de errores de OpenSearch dominio en Logs debe estar habilitado CloudWatch
- [Opensearch.5] OpenSearch los dominios deben tener activado el registro de auditoría
- [Opensearch.6] OpenSearch los dominios deben tener al menos tres nodos de datos
- [Opensearch.7] OpenSearch los dominios deben tener habilitado un control de acceso detallado
- [Opensearch.8] Las conexiones a los OpenSearch dominios deben cifrarse con la última política de seguridad de TLS
- [PCA.1]AWS Privada CALa autoridad emisora de certificados raíz debe estar deshabilitada
- [PCA.2]AWSLas autoridades de certificación de CA privadas deben estar etiquetadas
- [RDS.14] Los clústeres de Amazon Aurora deben tener habilitado el retroceso
- [RDS.15] Los clústeres de bases de datos de RDS deben configurarse para varias zonas de disponibilidad
- [RDS.24] Los clústeres de bases de datos de RDS deben usar un nombre de usuario de administrador personalizado

- [RDS.25] Las instancias de bases de datos de RDS deben usar un nombre de usuario de administrador personalizado
- [RDS.27] Los clústeres de bases de datos de RDS deben cifrarse en reposo
- [RDS.31] Los grupos de seguridad de la base de datos de RDS deben etiquetarse
- [RDS.34] Los clústeres de bases de datos Aurora MySQL deben publicar los registros de auditoría en Logs CloudWatch
- [RDS.35] Los clústeres de bases de datos de RDS deben tener habilitada la actualización automática de versiones secundarias
- [RDS.43] Los proxies de bases de datos de RDS deben requerir el cifrado TLS para las conexiones
- [RDS.45] Los clústeres de bases de datos Aurora MySQL deben tener habilitado el registro de auditoría
- [RDS.47] Los clústeres de bases de datos de RDS para PostgreSQL deben configurarse para copiar las etiquetas a las instantáneas de bases de datos
- [RDS.48] Los clústeres de bases de datos de RDS para MySQL deben configurarse para copiar etiquetas a las instantáneas de bases de datos
- [RDS.50] Los clústeres de bases de datos de RDS deben tener un período de retención de copias de seguridad suficiente
- [RDS.51] Los clústeres globales de RDS deben ejecutarse en una versión compatible de Aurora MySQL
- [Redshift.8] Los clústeres de Amazon Redshift no deben usar el nombre de usuario de administrador predeterminado
- [Redshift.10] Los clústeres de Redshift deben cifrarse en reposo
- [Redshift.17] Los grupos de parámetros del clúster de Redshift deben estar etiquetados
- [RedshiftServerless.1] Los grupos de trabajo sin servidor de Amazon Redshift deberían utilizar un enrutamiento de VPC mejorado
- [RedshiftServerless.2] Las conexiones a los grupos de trabajo sin servidor de Redshift deberían ser obligatorias para usar SSL
- [RedshiftServerless.3] Los grupos de trabajo sin servidor de Redshift deberían prohibir el acceso público
- [RedshiftServerless.6] Los espacios de nombres Redshift Serverless deberían exportar los registros a los registros CloudWatch

- [Route53.1] Los controles de salud de Route 53 deben estar etiquetados
- [Route53.2] Las zonas alojadas públicas de Route 53 deberían registrar las consultas de DNS
- [S3.10] Los cubos de uso general de S3 con el control de versiones habilitado deben tener configuraciones de ciclo de vida
- [S3.11] Los cubos de uso general de S3 deben tener habilitadas las notificaciones de eventos
- [S3.12] Las ACL no deben usarse para administrar el acceso de los usuarios a los cubos de uso general de S3
- [S3.13] Los cubos de uso general de S3 deben tener configuraciones de ciclo de vida
- [S3.20] Los cubos de uso general de S3 deben tener habilitada la eliminación de MFA
- [S3.24] Los puntos de Multi-Region acceso S3 deben tener habilitada la configuración de bloqueo del acceso público
- [S3.25] Los buckets de directorio de S3 deben tener configuraciones de ciclo de vida
- [SageMaker.1] Las instancias de Amazon SageMaker Notebook no deberían tener acceso directo a Internet
- [SageMaker.2] las instancias de SageMaker cuadernos deben lanzarse en una VPC personalizada
- [SageMaker.3] Los usuarios no deben tener acceso root a las instancias de los SageMaker cuadernos
- SageMaker Los modelos [SageMaker.5] deben tener habilitado el aislamiento de red
- [SageMaker.6] las configuraciones de imagen de la SageMaker aplicación deben estar etiquetadas
- [SageMaker.7] SageMaker las imágenes deben estar etiquetadas
- [SageMaker.9] las definiciones de trabajos de calidad de los SageMaker datos deben tener habilitado el cifrado del tráfico entre contenedores
- [SageMaker.10] Las definiciones de trabajos de explicabilidad del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores
- [SageMaker.11] las definiciones de trabajos SageMaker de calidad de los datos deben tener habilitado el aislamiento de red
- [SageMaker.12] las definiciones de trabajo basadas en el sesgo del SageMaker modelo deben tener habilitado el aislamiento de red
- [SageMaker.13] las definiciones de trabajos de calidad del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores
- [SageMaker.14] los programas SageMaker de monitoreo deben tener habilitado el aislamiento de la red

- [SageMaker.15] Las definiciones de trabajo basadas en el sesgo del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores
- SageMaker Los modelos [SageMaker.16] deben usar un registro privado en la VPC para los contenedores principales
- [SageMaker.17] SageMaker Las tiendas offline de los grupos de funciones deben cifrarse con AWS KMS claves
- [SageMaker.18] las tiendas en línea de grupos de SageMaker funciones con almacenamiento estándar deben cifrarse con AWS KMS claves
- [SageMaker.19] SageMaker los modelos deben usar un registro privado en la VPC para las canalizaciones de inferencia de varios contenedores
- [SES.1] Las listas de contactos de SES deben estar etiquetadas
- [SES.2] Los conjuntos de configuración de SES deben estar etiquetados
- [SES.3] Los conjuntos de configuración de SES deben tener el TLS habilitado para enviar correos electrónicos
- [SNS.4] Las políticas de acceso a los temas de SNS no deberían permitir el acceso público
- [SQS.3] Las políticas de acceso a las colas de SQS no deberían permitir el acceso público
- [SSM.4] Los documentos SSM no deben ser públicos
- [SSM.5] Los documentos SSM deben estar etiquetados
- [SSM.6] SSM Automation debería tener el registro habilitado CloudWatch
- [StepFunctions.1] Step Functions indica que las máquinas deben tener el registro activado
- [StepFunctions.2] Las actividades de Step Functions deben estar etiquetadas
- [Transfer.4] Los acuerdos Transfer Family deben estar etiquetados
- [Transfer.5] Los certificados Transfer Family deben estar etiquetados
- [Transfer.6] Los conectores Transfer Family deben estar etiquetados
- [Transfer.7] Los perfiles de Transfer Family deben estar etiquetados
- [WAF.1]AWS WAFEl registro de ACL web global clásico debe estar habilitado
- [WAF.2]AWS WAFLas reglas regionales clásicas deben tener al menos una condición
- [WAF.3]AWS WAFLos grupos de reglas regionales clásicos deben tener al menos una regla
- [WAF.4]AWS WAFLas ACL web regionales clásicas deben tener al menos una regla o grupo de reglas

- [WAF.6]AWS WAFLas reglas globales clásicas deben tener al menos una condición
- [WAF.7]AWS WAFLos grupos de reglas globales clásicos deben tener al menos una regla
- [WAF.8]AWS WAFLas ACL web globales clásicas deben tener al menos una regla o grupo de reglas
- [WAF.10]AWS WAFLas ACL web deben tener al menos una regla o grupo de reglas
- [WAF.12]AWS WAFlas reglas deben tener CloudWatch las métricas habilitadas
- [WorkSpaces.1] los volúmenes de WorkSpaces usuarios deben cifrarse en reposo
- [WorkSpaces.2] los volúmenes WorkSpaces raíz deben cifrarse en reposo

AWS GovCloud (US-West)

Los siguientes controles no son compatibles en la AWS GovCloud (US-West) región.

- [ACM.2] Los certificados RSA gestionados por ACM deben utilizar una longitud de clave de al menos 2048 bits
- [Account.1] La información de contacto de seguridad debe proporcionarse para unCuenta de AWS
- [Account.2]Cuentas de AWSdebe formar parte de unAWS Organizationsorganización
- [APIGateway.2] Las etapas de la API REST de API Gateway deben configurarse para usar certificados SSL para la autenticación de backend
- [APIGateway.8] Las rutas de API Gateway deben especificar un tipo de autorización
- [APIGateway.9] El registro de acceso debe configurarse para las etapas V2 de API Gateway
- [APIGateway.10] Las integraciones de API Gateway V2 deben usar HTTPS para las conexiones privadas
- [APIGateway.11] Los nombres de dominio de API Gateway deben usar las políticas de seguridad recomendadas
- [Amplify.1] Las aplicaciones Amplify deben estar etiquetadas
- [Amplify.2] Amplify branches debe estar etiquetado
- [AppConfig.1]AWS AppConfiglas aplicaciones deben estar etiquetadas
- [AppConfig.2]AWS AppConfiglos perfiles de configuración deben estar etiquetados
- [AppConfig.3]AWS AppConfiglos entornos deben estar etiquetados
- [AppConfig.4]AWS AppConfiglas asociaciones de extensiones deben estar etiquetadas

- [AppFlow.1] AppFlow Los flujos de Amazon deben estar etiquetados
- [AppRunner.1] Los servicios de App Runner deben estar etiquetados
- [AppRunner.2] Los conectores VPC de App Runner deben estar etiquetados
- [AppSync.1]AWS AppSyncLas cachés de las API deben estar cifradas en reposo
- [AppSync.2]AWS AppSyncdebe tener habilitado el registro a nivel de campo
- [AppSync.4]AWS AppSyncLas API de GraphQL deben estar etiquetadas
- [AppSync.5]AWS AppSyncLas API de GraphQL no deben autenticarse con claves de API
- [AppSync.6]AWS AppSyncLas cachés de las API deben cifrarse en tránsito
- [AutoScaling.2] El grupo Amazon EC2 Auto Scaling debe cubrir varias zonas de disponibilidad
- [AutoScaling.3] Las configuraciones de lanzamiento grupal de Auto Scaling deberían configurar las instancias EC2 para que requieran la versión 2 del Servicio de Metadatos de Instancia (IMDSv2)
- [AutoScaling.6] Los grupos de Auto Scaling deben usar varios tipos de instancias en múltiples zonas de disponibilidad
- [AutoScaling.9] Los grupos de Amazon EC2 Auto Scaling deben utilizar las plantillas de lanzamiento de Amazon EC2
- [Backup.4]AWS Backuplos planes de informes deben estar etiquetados
- [Batch.1] Las colas de trabajos por lotes deben estar etiquetadas
- [Batch.2] Las políticas de programación de lotes deben estar etiquetadas
- [Batch.3] Los entornos de procesamiento por lotes deben etiquetarse
- [Batch.4] Las propiedades de los recursos de cómputo en los entornos de cómputo por lotes gestionados deben estar etiquetadas
- [BedrockAgentCore.1] Los AgentCore tiempos de ejecución de Bedrock deben configurarse con el modo de red VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways debería requerir autorización para las solicitudes entrantes
- [BedrockAgentCore.3] Bedrock AgentCore Memory debe estar cifrada y gestionada por el clienteAWS KMSclaves
- [BedrockAgentCore.4] Bedrock AgentCore Gateway debe cifrarse de forma que sea gestionada por el clienteAWS KMSclaves
- [BedrockAgentCore.5] Los navegadores AgentCore personalizados de Bedrock no deberían usar el modo de red pública

- [BedrockAgentCore.6] Los navegadores AgentCore personalizados de Bedrock deberían tener habilitada la grabación de sesiones
- [CloudFront.1] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado
- [CloudFront.3] CloudFront las distribuciones deben requerir el cifrado durante el tránsito
- [CloudFront.4] CloudFront las distribuciones deben tener configurada la conmutación por error de origen
- [CloudFront.5] CloudFront las distribuciones deben tener habilitado el registro
- [CloudFront.6] CloudFront las distribuciones deben tener WAF activado
- [CloudFront.7] CloudFront las distribuciones deben usar certificados personalizados SSL/TLS
- [CloudFront.8] CloudFront las distribuciones deben usar el SNI para atender las solicitudes HTTPS
- [CloudFront.9] CloudFront las distribuciones deben cifrar el tráfico para convertirlo en orígenes personalizados
- [CloudFront.10] CloudFront las distribuciones no deben usar protocolos SSL obsoletos entre ubicaciones de borde y orígenes personalizados
- [CloudFront.12] CloudFront las distribuciones no deben apuntar a orígenes de S3 inexistentes
- [CloudFront.13] CloudFront las distribuciones deben usar el control de acceso al origen
- [CloudFront.14] CloudFront las distribuciones deben estar etiquetadas
- [CloudFront.15] CloudFront las distribuciones deben usar la política de seguridad TLS recomendada
- [CloudFront.16] CloudFront las distribuciones deben usar el control de acceso de origen para los orígenes de las URL de las funciones de Lambda
- [CloudFront.17] CloudFront las distribuciones deben usar grupos de claves confiables para las URL y cookies firmadas
- [CloudWatch.17] las acciones CloudWatch de alarma deben estar activadas
- [CodeArtifact.1] CodeArtifact los repositorios deben estar etiquetados
- [CodeBuild.3] Los registros de CodeBuild S3 deben estar cifrados
- [CodeBuild.4] los entornos de CodeBuild proyectos deben tener un registroAWS ConfigDuración
- [CodeGuruProfiler.1] Los grupos CodeGuru de creación de perfiles de Profiler deben estar etiquetados
- [CodeGuruReviewer.1] Las asociaciones de repositorios de CodeGuru Reviewer deben estar etiquetadas

- [Cognito.1] Los grupos de usuarios de Cognito deben tener activada la protección contra amenazas y el modo de aplicación con todas las funciones para la autenticación estándar
- [Cognito.3] Las políticas de contraseñas para los grupos de usuarios de Cognito deben tener configuraciones sólidas
- [Cognito.4] Los grupos de usuarios de Cognito deben tener activada la protección contra amenazas y el modo de aplicación con todas las funciones para la autenticación personalizada
- [Cognito.5] La MFA debe estar habilitada para los grupos de usuarios de Cognito
- [Cognito.6] Los grupos de usuarios de Cognito deben tener habilitada la protección contra la eliminación
- [Connect.1] Los tipos de objetos de los perfiles de clientes de Amazon Connect deben estar etiquetados
- [DataSync.2] DataSync las tareas deben estar etiquetadas
- [DMS.2] Los certificados DMS deben estar etiquetados
- [DMS.6] Las instancias de replicación de DMS deben tener habilitada la actualización automática de las versiones secundarias
- [DMS.7] Las tareas de replicación del DMS para la base de datos de destino deben tener el registro habilitado
- [DMS.8] Las tareas de replicación del DMS para la base de datos de origen deben tener el registro activado
- [DMS.9] Los puntos finales del DMS deben usar SSL
- [DocumentDB.1] Los clústeres de Amazon DocumentDB deben cifrarse en reposo
- [DocumentDB.2] Los clústeres de Amazon DocumentDB deben tener un período de retención de copias de seguridad adecuado
- [DocumentDB.3] Las instantáneas de clústeres manuales de Amazon DocumentDB no deben ser públicas
- [DocumentDB.4] Los clústeres de Amazon DocumentDB deben publicar los registros de auditoría en Logs CloudWatch
- [DocumentDB.5] Los clústeres de Amazon DocumentDB deben tener habilitada la protección contra eliminaciones
- [DynamoDB.3] Los clústeres de DynamoDB Accelerator (DAX) deben cifrarse en reposo
- [DynamoDB.7] Los clústeres de DynamoDB Accelerator deben cifrarse en tránsito

- [EC2.21] Las ACL de red no deberían permitir la entrada desde la versión 0.0.0. 0/0 al puerto 22 o al puerto 3389
- [EC2.22] Deben eliminarse los grupos de seguridad de Amazon EC2 no utilizados
- [EC2.23] Amazon EC2 Transit Gateways no debe aceptar automáticamente las solicitudes de adjuntos de VPC
- [EC2.24] No se deben utilizar los tipos de instancias paravirtuales de Amazon EC2
- [EC2.25] Las plantillas de lanzamiento de Amazon EC2 no deben asignar direcciones IP públicas a las interfaces de red
- [EC2.28] Los volúmenes de EBS deben estar cubiertos por un plan de respaldo
- [EC2.38] Las instancias EC2 deben estar etiquetadas
- [EC2.58] Las VPC deben configurarse con un punto final de interfaz para los contactos de Systems Manager Incident Manager
- [EC2.60] Las VPC deben configurarse con un punto final de interfaz para Systems Manager Incident Manager
- [EC2.170] Las plantillas de lanzamiento de EC2 deben utilizar la versión 2 del servicio de metadatos de instancias (IMDSv2)
- [EC2.173] Las solicitudes de EC2 Spot Fleet con parámetros de lanzamiento deberían permitir el cifrado de los volúmenes de EBS adjuntos
- [EC2.174] Los conjuntos de opciones DHCP de EC2 deben estar etiquetados
- [EC2.175] Las plantillas de lanzamiento de EC2 deben estar etiquetadas
- [EC2.176] Las listas de prefijos de EC2 deben estar etiquetadas
- [EC2.177] Las sesiones de réplica de tráfico de EC2 deben etiquetarse
- [EC2.178] Los filtros espejo de tráfico EC2 deben estar etiquetados
- [EC2.179] Los objetivos del espejo de tráfico de EC2 deben estar etiquetados
- [ECR.1] Los repositorios privados de ECR deben tener configurado el escaneo de imágenes
- [ECR.2] Los repositorios privados de ECR deben tener configurada la inmutabilidad de etiquetas
- [ECR.3] Los repositorios de ECR deben tener configurada al menos una política de ciclo de vida
- [ECR.4] Los repositorios públicos de ECR deben etiquetarse
- [ECS.3] Las definiciones de tareas de ECS no deben compartir el espacio de nombres del proceso del host
- [ECS.4] Los contenedores ECS deben ejecutarse sin privilegios

- [ECS.5] Las definiciones de tareas de ECS deben configurar los contenedores para que se limiten al acceso de solo lectura a los sistemas de archivos raíz
- [ECS.8] Los secretos no deben transmitirse como variables de entorno de contenedores
- [ECS.9] Las definiciones de tareas de ECS deben tener una configuración de registro
- [ECS.10] Los servicios Fargate de ECS deberían ejecutarse en la última versión de la plataforma Fargate
- [ECS.12] Los clústeres de ECS deben usar Container Insights
- [EFS.3] Los puntos de acceso EFS deben exigir un directorio raíz
- [EFS.4] Los puntos de acceso EFS deben exigir la identidad del usuario
- [EKS.2] Los clústeres de EKS deben ejecutarse en una versión de Kubernetes compatible
- [EKS.8] Los clústeres de EKS deben tener habilitado el registro de auditoría
- [ELB.10] El balanceador de carga clásico debe abarcar varias zonas de disponibilidad
- [ELB.12] El balanceador de carga de aplicaciones debe configurarse con el modo defensivo o de mitigación de desincronización más estricto
- [ELB.13] Los balanceadores de carga de aplicaciones, redes y puertas de enlace deben abarcar varias zonas de disponibilidad
- [ELB.14] El balanceador de carga clásico debe configurarse con el modo defensivo o de mitigación de desincronización más estricto
- [ELB.21] Los grupos destinatarios de Application and Network Load Balancer deben utilizar protocolos de control de estado cifrados
- [ELB.22] Los grupos objetivo del ELB deben usar protocolos de transporte cifrados
- [ElastiCache.1] ElastiCache (Redis OSS) los clústeres deben tener habilitadas las copias de seguridad automáticas
- [ElastiCache.2] ElastiCache los clústeres deberían tener habilitadas las actualizaciones automáticas de las versiones secundarias
- [ElastiCache.3] los grupos de ElastiCache replicación deberían tener habilitada la conmutación por error automática
- [ElastiCache.4] los grupos de ElastiCache replicación deben cifrarse en reposo
- [ElastiCache.5] los grupos de ElastiCache replicación deben cifrarse en tránsito
- [ElastiCache.6] ElastiCache (Redis OSS) Los grupos de replicación de versiones anteriores deberían tener habilitada la autenticación de Redis OSS

- [ElastiCache.7] los ElastiCache clústeres no deben usar el grupo de subredes predeterminado
- [ElasticBeanstalk.1] Los entornos de Elastic Beanstalk deberían tener habilitados los informes de estado mejorados
- [ElasticBeanstalk.2] Las actualizaciones de la plataforma gestionada de Elastic Beanstalk deben estar habilitadas
- [ElasticBeanstalk.3] Elastic Beanstalk debería transmitir los registros a CloudWatch
- [EMR.2] La configuración de acceso público del bloque Amazon EMR debe estar habilitada
- [EMR.3] Las configuraciones de seguridad de Amazon EMR deben cifrarse en reposo
- [EMR.4] Las configuraciones de seguridad de Amazon EMR deben cifrarse en tránsito
- [ES.4] Debería estar habilitado el registro de errores de dominio de Elasticsearch en Logs CloudWatch
- [EventBridge.3] los autobuses de eventos EventBridge personalizados deben tener adjunta una política basada en los recursos
- [EventBridge.4] los puntos finales EventBridge globales deberían tener habilitada la replicación de eventos
- [FraudDetector.1] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.2] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas
- [FraudDetector.3] Los resultados de Amazon Fraud Detector deben estar etiquetados
- [FraudDetector.4] Las variables de Amazon Fraud Detector deben estar etiquetadas
- [FSx.1] FSx para sistemas de archivos OpenZFS debe configurarse para copiar etiquetas en copias de seguridad y volúmenes
- [FSx.2] Los sistemas de archivos FSx for Lustre deben configurarse para copiar etiquetas a las copias de seguridad
- [GlobalAccelerator.1] Los aceleradores de Global Accelerator deben estar etiquetados
- [GuardDuty.7] La monitorización del tiempo de ejecución de GuardDuty EKS debe estar habilitada
- [GuardDuty.8] La protección contra GuardDuty malware para EC2 debe estar habilitada
- [GuardDuty.9] La protección GuardDuty RDS debe estar habilitada
- [GuardDuty.11] La monitorización del GuardDuty tiempo de ejecución debe estar habilitada
- [GuardDuty.12] La monitorización del tiempo de ejecución de GuardDuty ECS debe estar habilitada

- [GuardDuty.13] La monitorización del tiempo de ejecución de GuardDuty EC2 debe estar habilitada
- [IAM.6] La MFA de hardware debe estar habilitada para el usuario root
- [IAM.9] La MFA debe estar habilitada para el usuario root
- [IAM.21] Las políticas de IAM gestionadas por el cliente que cree no deberían permitir acciones comodín en los servicios
- [IAM.24] Las funciones de IAM deben estar etiquetadas
- [IAM.25] Los usuarios de IAM deben estar etiquetados
- [IAM.28] El analizador de acceso externo de IAM Access Analyzer debe estar habilitado
- [Inspector.3] El escaneo de código Lambda de Amazon Inspector Lambda debe estar activado
- [IoTSiteWise.1]AWSLos modelos SiteWise de activos de IoT deben estar etiquetados
- [IoTSiteWise.2]AWS SiteWise Los paneles de IoT deben estar etiquetados
- [IoTSiteWise.3]AWS SiteWise Las pasarelas de IoT deben estar etiquetadas
- [IoTSiteWise.4]AWS SiteWise Los portales de IoT deben estar etiquetados
- [IoTSiteWise.5]AWS SiteWise Los proyectos de IoT deben estar etiquetados
- [IoTTwinMaker.1]AWSLos trabajos de TwinMaker sincronización de IoT deben estar etiquetados
- [IoTTwinMaker.2]AWS TwinMaker Los espacios de trabajo de IoT deben estar etiquetados
- [IoTTwinMaker.3]AWS TwinMaker Las escenas de IoT deben estar etiquetadas
- [IoTTwinMaker.4]AWS TwinMaker Las entidades de IoT deben estar etiquetadas
- [IoTWireless.1]AWSLos grupos de multidifusión de IoT Wireless deben estar etiquetados
- [IoTWireless.2]AWSLos perfiles de servicio de IoT Wireless deben estar etiquetados
- [IoTWireless.3]AWSLas tareas de IoT FUOTA deben estar etiquetadas
- [IVS.1] Los pares de teclas de reproducción IVS deben estar etiquetados
- [IVS.2] Las configuraciones de grabación de IVS deben estar etiquetadas
- [IVS.3] Los canales IVS deben estar etiquetados
- [Keyspaces.1] Los espacios clave de Amazon Keyspaces deben estar etiquetados
- [Kinesis.1] Las transmisiones de Kinesis deben cifrarse en reposo
- [KMS.5] Las claves KMS no deben ser de acceso público
- [Lambda.5] Las funciones de VPC Lambda deben funcionar en varias zonas de disponibilidad
- [Macie.1] Amazon Macie debería estar activado

- [Macie.2] La detección automática de datos confidenciales por parte de Macie debería estar habilitada
- [MQ.5] Los corredores de ActiveMQ deberían usar el modo de implementación active/standby
- [MQ.6] Los corredores de RabbitMQ deberían usar el modo de despliegue de clústeres
- [MSK.1] Los clústeres de MSK deben cifrarse en tránsito entre los nodos de intermediación
- [MSK.2] Los clústeres de MSK deberían tener configurada una supervisión mejorada
- [MSK.3] Los conectores MSK Connect deben estar cifrados en tránsito
- [MSK.5] Los conectores MSK deben tener el registro activado
- [Neptune.1] Los clústeres de bases de datos de Neptune deben cifrarse en reposo
- [Neptune.2] Los clústeres de bases de datos de Neptune deberían publicar registros de auditoría en Logs CloudWatch
- [Neptune.3] Las instantáneas del clúster de base de datos de Neptune no deben ser públicas
- [Neptune.4] Los clústeres de base de datos de Neptune deben tener habilitada la protección contra eliminación
- [Neptune.5] Los clústeres de Neptune DB deberían tener habilitadas las copias de seguridad automatizadas
- [Neptune.6] Las instantáneas del clúster de base de datos de Neptune deben cifrarse en reposo
- [Neptune.7] Los clústeres de base de datos de Neptune deben tener habilitada la autenticación de bases de datos de IAM
- [Neptune.8] Los clústeres de bases de datos de Neptune deben configurarse para copiar etiquetas a las instantáneas
- [Neptune.9] Los clústeres de base de datos Neptune deben implementarse en varias zonas de disponibilidad
- [NetworkFirewall.1] Los firewalls de Network Firewall deben implementarse en varias zonas de disponibilidad
- [NetworkFirewall.2] El registro de Network Firewall debe estar habilitado
- [NetworkFirewall.3] Las políticas de Network Firewall deben tener asociado al menos un grupo de reglas
- [NetworkFirewall.4] La acción sin estado predeterminada para las políticas de Network Firewall debe ser eliminar o reenviar paquetes completos
- [NetworkFirewall.5] La acción sin estado predeterminada para las políticas de Network Firewall debe ser eliminar o reenviar paquetes fragmentados

- [NetworkFirewall.6] El grupo de reglas de Stateless Network Firewall no debe estar vacío
- [NetworkFirewall.9] Los firewalls de Network Firewall deben tener habilitada la protección de eliminación
- [Opensearch.1] OpenSearch los dominios deben tener activado el cifrado en reposo
- [Opensearch.2] OpenSearch los dominios no deben ser de acceso público
- [Opensearch.3] OpenSearch los dominios deben cifrar los datos enviados entre nodos
- [Opensearch.4] El registro de errores de OpenSearch dominio en Logs debe estar habilitado CloudWatch
- [Opensearch.5] OpenSearch los dominios deben tener activado el registro de auditoría
- [Opensearch.6] OpenSearch los dominios deben tener al menos tres nodos de datos
- [Opensearch.7] OpenSearch los dominios deben tener habilitado un control de acceso detallado
- [Opensearch.8] Las conexiones a los OpenSearch dominios deben cifrarse con la última política de seguridad de TLS
- [PCA.1]AWS Privada CALa autoridad emisora de certificados raíz debe estar deshabilitada
- [PCA.2]AWSLas autoridades de certificación de CA privadas deben estar etiquetadas
- [RDS.14] Los clústeres de Amazon Aurora deben tener habilitado el retroceso
- [RDS.15] Los clústeres de bases de datos de RDS deben configurarse para varias zonas de disponibilidad
- [RDS.24] Los clústeres de bases de datos de RDS deben usar un nombre de usuario de administrador personalizado
- [RDS.25] Las instancias de bases de datos de RDS deben usar un nombre de usuario de administrador personalizado
- [RDS.27] Los clústeres de bases de datos de RDS deben cifrarse en reposo
- [RDS.34] Los clústeres de bases de datos Aurora MySQL deben publicar los registros de auditoría en Logs CloudWatch
- [RDS.35] Los clústeres de bases de datos de RDS deben tener habilitada la actualización automática de versiones secundarias
- [RDS.43] Los proxies de bases de datos de RDS deben requerir el cifrado TLS para las conexiones
- [RDS.45] Los clústeres de bases de datos Aurora MySQL deben tener habilitado el registro de auditoría

- [RDS.47] Los clústeres de bases de datos de RDS para PostgreSQL deben configurarse para copiar las etiquetas a las instantáneas de bases de datos
- [RDS.48] Los clústeres de bases de datos de RDS para MySQL deben configurarse para copiar etiquetas a las instantáneas de bases de datos
- [RDS.50] Los clústeres de bases de datos de RDS deben tener un período de retención de copias de seguridad suficiente
- [RDS.51] Los clústeres globales de RDS deben ejecutarse en una versión compatible de Aurora MySQL
- [Redshift.7] Los clústeres de Redshift deberían utilizar un enrutamiento de VPC mejorado
- [Redshift.8] Los clústeres de Amazon Redshift no deben usar el nombre de usuario de administrador predeterminado
- [Redshift.10] Los clústeres de Redshift deben cifrarse en reposo
- [Redshift.11] Los clústeres de Redshift deben estar etiquetados
- [Redshift.13] Las instantáneas del clúster de Redshift deben estar etiquetadas
- [Redshift.17] Los grupos de parámetros del clúster de Redshift deben estar etiquetados
- [RedshiftServerless.1] Los grupos de trabajo sin servidor de Amazon Redshift deberían utilizar un enrutamiento de VPC mejorado
- [RedshiftServerless.2] Las conexiones a los grupos de trabajo sin servidor de Redshift deberían ser obligatorias para usar SSL
- [RedshiftServerless.3] Los grupos de trabajo sin servidor de Redshift deberían prohibir el acceso público
- [RedshiftServerless.6] Los espacios de nombres Redshift Serverless deberían exportar los registros a los registros CloudWatch
- [Route53.1] Los controles de salud de Route 53 deben estar etiquetados
- [Route53.2] Las zonas alojadas públicas de Route 53 deberían registrar las consultas de DNS
- [S3.10] Los cubos de uso general de S3 con el control de versiones habilitado deben tener configuraciones de ciclo de vida
- [S3.11] Los cubos de uso general de S3 deben tener habilitadas las notificaciones de eventos
- [S3.12] Las ACL no deben usarse para administrar el acceso de los usuarios a los cubos de uso general de S3
- [S3.13] Los cubos de uso general de S3 deben tener configuraciones de ciclo de vida

- [S3.20] Los cubos de uso general de S3 deben tener habilitada la eliminación de MFA
- [S3.24] Los puntos de Multi-Region acceso S3 deben tener habilitada la configuración de bloqueo del acceso público
- [S3.25] Los buckets de directorio de S3 deben tener configuraciones de ciclo de vida
- [SageMaker.2] las instancias de SageMaker cuadernos deben lanzarse en una VPC personalizada
- [SageMaker.3] Los usuarios no deben tener acceso root a las instancias de los SageMaker cuadernos
- SageMaker Los modelos [SageMaker.5] deben tener habilitado el aislamiento de red
- [SageMaker.6] las configuraciones de imagen de la SageMaker aplicación deben estar etiquetadas
- [SageMaker.7] SageMaker las imágenes deben estar etiquetadas
- [SageMaker.9] las definiciones de trabajos de calidad de los SageMaker datos deben tener habilitado el cifrado del tráfico entre contenedores
- [SageMaker.10] Las definiciones de trabajos de explicabilidad del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores
- [SageMaker.11] las definiciones de trabajos SageMaker de calidad de los datos deben tener habilitado el aislamiento de red
- [SageMaker.12] las definiciones de trabajo basadas en el sesgo del SageMaker modelo deben tener habilitado el aislamiento de red
- [SageMaker.13] las definiciones de trabajos de calidad del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores
- [SageMaker.14] los programas SageMaker de monitoreo deben tener habilitado el aislamiento de la red
- [SageMaker.15] Las definiciones de trabajo basadas en el sesgo del SageMaker modelo deben tener habilitado el cifrado del tráfico entre contenedores
- [SageMaker.17] SageMaker Las tiendas offline de los grupos de funciones deben cifrarse con AWS KMS claves
- [SageMaker.18] las tiendas en línea de grupos de SageMaker funciones con almacenamiento estándar deben cifrarse con AWS KMS claves
- [SES.3] Los conjuntos de configuración de SES deben tener el TLS habilitado para enviar correos electrónicos
- [SNS.4] Las políticas de acceso a los temas de SNS no deberían permitir el acceso público

- [SQS.3] Las políticas de acceso a las colas de SQS no deberían permitir el acceso público
- [SSM.4] Los documentos SSM no deben ser públicos
- [SSM.5] Los documentos SSM deben estar etiquetados
- [StepFunctions.1] Step Functions indica que las máquinas deben tener el registro activado
- [StepFunctions.2] Las actividades de Step Functions deben estar etiquetadas
- [Transfer.4] Los acuerdos Transfer Family deben estar etiquetados
- [Transfer.5] Los certificados Transfer Family deben estar etiquetados
- [Transfer.6] Los conectores Transfer Family deben estar etiquetados
- [Transfer.7] Los perfiles de Transfer Family deben estar etiquetados
- [WAF.1]AWS WAFEl registro de ACL web global clásico debe estar habilitado
- [WAF.2]AWS WAFLas reglas regionales clásicas deben tener al menos una condición
- [WAF.3]AWS WAFLos grupos de reglas regionales clásicos deben tener al menos una regla
- [WAF.4]AWS WAFLas ACL web regionales clásicas deben tener al menos una regla o grupo de reglas
- [WAF.6]AWS WAFLas reglas globales clásicas deben tener al menos una condición
- [WAF.7]AWS WAFLos grupos de reglas globales clásicos deben tener al menos una regla
- [WAF.8]AWS WAFLas ACL web globales clásicas deben tener al menos una regla o grupo de reglas
- [WAF.10]AWS WAFLas ACL web deben tener al menos una regla o grupo de reglas
- [WAF.12]AWS WAFlas reglas deben tener CloudWatch las métricas habilitadas

Creación de recursos CSPM de Security Hub con CloudFormation

AWSSecurity Hub con el que se integra CSPMAWS CloudFormation, un servicio que le ayuda a modelar y configurar sus AWS recursos para que pueda dedicar menos tiempo a crear y administrar sus recursos e infraestructura. Cree una plantilla que describa todos los AWS recursos que desee (como las reglas de automatización) y CloudFormation aprovisione y configure esos recursos por usted.

Cuando la utiliceCloudFormation, podrá reutilizar la plantilla para configurar los recursos de CSPM de su Security Hub de forma coherente y repetida. Describa sus recursos una vez y, a continuación, aprovisione los mismos recursos una y otra vez en varias regionesCuentas de AWS.

Security Hub (CSPM) yCloudFormationplantillas

Para aprovisionar y configurar los recursos del CSPM de Security Hub y los servicios relacionados, debe entender cómo funcionan las plantillas de CloudFormation. Las plantillas son archivos de texto en formato JSON o YAML. Estas plantillas describen los recursos que desea aprovisionar en sus CloudFormation pilas.

Si no estás familiarizado con JSON o YAML, puedes usar CloudFormation Designer para ayudarte a empezar con CloudFormation las plantillas. Para obtener más información, consulta ¿Qué es CloudFormation Designer? en la Guía AWS CloudFormation del usuario.

Puede crear CloudFormation plantillas para los siguientes tipos de recursos CSPM de Security Hub:

- Habilitación del CSPM de Security Hub
- Designación del administrador delegado del CSPM de Security Hub para una organización
- Especificación de la forma en que está configurada la organización en el CSPM de Security Hub
- Habilitación de un estándar de seguridad
- Habilitación de agregación entre regiones
- Creación de una política de configuración centralizada y asociación a cuentas, unidades organizativas (OU) o a la raíz de la organización
- Creación de hallazgos personalizados
- Creación de una regla de automatización
- Personalización de parámetros de control
- Suscripción a una integración de productos de terceros

Para obtener más información, incluidos ejemplos de plantillas JSON y YAML para recursos, consulte la Referencia del tipo de recurso del CSPM de AWS Security Hub en la Guía del usuario de AWS CloudFormation.

Obtenga más información sobreCloudFormation

Para obtener más informaciónCloudFormation, consulte los siguientes recursos:

- AWS CloudFormation
- AWS CloudFormationGuía del usuario

- CloudFormationReferencia de la API
- AWS CloudFormationGuía del usuario de la interfaz de línea de comandos

Suscripción a los anuncios del CSPM de Security Hub con Amazon SNS

En esta sección se proporciona información sobre cómo suscribirse a los AWS anuncios de CSPM de Security Hub con Amazon Simple Notification Service (Amazon SNS) para recibir notificaciones sobre Security Hub CSPM.

Tras suscribirse, recibirá notificaciones sobre los siguientes eventos (tenga en cuenta el `AnnouncementType` correspondiente a cada evento):

- `NEW_STANDARDS_CONTROLS`: se han agregado nuevos controles o estándares del CSPM de Security Hub.
- `RETIRED_STANDARDS_CONTROLS`: se han retirado controles o estándares existentes del CSPM de Security Hub.

Las notificaciones están disponibles en todos los formatos que admite Amazon SNS. Puede suscribirse a los anuncios del CSPM de Security Hub en todas las Regiones de AWS en las que el CSPM de Security Hub se encuentra disponible.

Un usuario debe disponer de permisos de `Subscribe` para suscribirse a un tema de Amazon SNS. Puede lograrlo con las políticas de Amazon SNS, las políticas de IAM o ambas. Para obtener más información, consulte Uso en conjunto de políticas y roles de IAM y Amazon SNS en la Guía para desarrolladores de Amazon Simple Notification Service.

> **Note**
>
> El CSPM de Security Hub envía anuncios de Amazon SNS sobre actualizaciones del servicio del CSPM de Security Hub a cualquier Cuenta de AWS suscrita. Para recibir notificaciones sobre los resultados del CSPM de Security Hub, consulte Revisión de detalles e historial de resultados en el CSPM de Security Hub.

Puede suscribirse a una cola de Amazon Simple Queue Service (Amazon SQS) sobre un tema de Amazon SNS, pero debe utilizar un tema de Amazon SNS nombre de recurso de Amazon (ARN) que

se encuentre en la misma región. Para obtener más información, consulte Suscripción a una cola de un tema de Amazon SNS en la Guía para desarrolladores de Amazon Simple Queue Service.

También puede utilizar una AWS Lambda función para invocar eventos cuando reciba notificaciones. Para obtener más información, incluido un ejemplo de código de función, consulte el Tutorial: Uso AWS Lambda con Amazon Simple Notification Service en la Guía para AWS Lambda desarrolladores.

Los ARN de tema de Amazon SNS para cada región son los siguientes.

Región de AWS	ARN del tema de Amazon SNS
Este de EE. UU. (Ohio)	`arn:aws:sns:us-east-2:291342846459:SecurityHubAnnouncements`
Este de EE. UU. (Norte de Virginia)	`arn:aws:sns:us-east-1:088139225913:SecurityHubAnnouncements`
Oeste de EE. UU. (Norte de California)	`arn:aws:sns:us-west-1:137690824926:SecurityHubAnnouncements`
Oeste de EE. UU. (Oregón)	`arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements`
África (Ciudad del Cabo)	`arn:aws:sns:af-south-1:463142546776:SecurityHubAnnouncements`
Asia-Pacífico (Hong Kong)	`arn:aws:sns:ap-east-1:464812404305:SecurityHubAnnouncements`
Asia-Pacífico (Hyderabad)	`arn:aws:sns:ap-south-2:849907286123:SecurityHubAnnouncements`

Región de AWS	ARN del tema de Amazon SNS
Asia-Pacífico (Yakarta)	`arn:aws:sns:ap-southeast-3:627843640627:SecurityHubAnnouncements`
Asia-Pacífico (Mumbai)	`arn:aws:sns:ap-south-1:707356269775:SecurityHubAnnouncements`
Asia-Pacífico (Osaka)	`arn:aws:sns:ap-northeast-3:633550238216:SecurityHubAnnouncements`
Asia-Pacífico (Seúl)	`arn:aws:sns:ap-northeast-2:374299265323:SecurityHubAnnouncements`
Asia-Pacífico (Singapur)	`arn:aws:sns:ap-southeast-1:512267288502:SecurityHubAnnouncements`
Asia-Pacífico (Sídney)	`arn:aws:sns:ap-southeast-2:475730049140:SecurityHubAnnouncements`
Asia-Pacífico (Tokio)	`arn:aws:sns:ap-northeast-1:592469075483:SecurityHubAnnouncements`
Canadá (centro)	`arn:aws:sns:ca-central-1:137749997395:SecurityHubAnnouncements`
China (Pekín)	`arn:aws-cn:sns:cn-north-1:672341567257:SecurityHubAnnouncements`

Región de AWS	ARN del tema de Amazon SNS
China (Ningxia)	`arn:aws-cn:sns:cn-northwest-1:672534482217:SecurityHubAnnouncements`
Europa (Fráncfort)	`arn:aws:sns:eu-central-1:871975303681:SecurityHubAnnouncements`
Europa (Irlanda)	`arn:aws:sns:eu-west-1:705756202095:SecurityHubAnnouncements`
Europa (Londres)	`arn:aws:sns:eu-west-2:883600840440:SecurityHubAnnouncements`
Europa (Milán)	`arn:aws:sns:eu-south-1:151363035580:SecurityHubAnnouncements`
Europa (París)	`arn:aws:sns:eu-west-3:313420042571:SecurityHubAnnouncements`
Europa (España)	`arn:aws:sns:eu-south-2:777487947751:SecurityHubAnnouncements`
Europa (Estocolmo)	`arn:aws:sns:eu-north-1:191971010772:SecurityHubAnnouncements`
Europa (Zúrich)	`arn:aws:sns:eu-central-2:704347005078:SecurityHubAnnouncements`

Región de AWS	ARN del tema de Amazon SNS
Israel (Tel Aviv)	`arn:aws:sns:il-central-1:726652212146:SecurityHubAnnouncements`
Middle East (Bahrain)	`arn:aws:sns:me-south-1:585146626860:SecurityHubAnnouncements`
Medio Oriente (EAU)	`arn:aws:sns:me-central-1:431548502100:SecurityHubAnnouncements`
América del Sur (São Paulo)	`arn:aws:sns:sa-east-1:359811883282:SecurityHubAnnouncements`
AWS GovCloud (US-East)	`arn:aws-us-gov:sns:us-gov-east-1:239368469855:SecurityHubAnnouncements`
AWS GovCloud (US-West)	`arn:aws-us-gov:sns:us-gov-west-1:239334163374:SecurityHubAnnouncements`

Los mensajes suelen ser los mismos en todas las regiones de una partición, por lo que puede suscribirse a una región de cada partición para recibir anuncios que afecten a todas las regiones de esa partición. Los anuncios asociados a las cuentas miembro no se replican en la cuenta de administrador. Como resultado, cada cuenta, incluida la cuenta de administrador, tendrá una única copia de cada anuncio. Puede decidir qué cuenta quiere usar para suscribirse a los anuncios del CSPM de Security Hub.

Para conocer el costo de suscribirse a los anuncios del CSPM de Security Hub, consulte la página de precios de Amazon SNS.

Suscripción a los anuncios del CSPM de Security Hub (consola)

1. Abra la consola de Amazon SNS en https://console.aws.amazon.com/sns/v3/home.
2. En la lista de regiones, seleccione la región en la que desea suscribirse a los anuncios del CSPM de Security Hub. En este ejemplo se utiliza la región `us-west-2`.
3. En el panel de navegación, seleccione Suscripciones y, a continuación, elija Crear suscripción.
4. Escriba el ARN del tema en el cuadro de texto ARN del tema. Por ejemplo, `arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements`.
5. En Protocolo, seleccione cómo desea recibir los anuncios sobre el CSPM de Security Hub. Si elige Correo electrónico, en Punto de conexión, introduzca la dirección de correo electrónico que desee usar para recibir anuncios.
6. Seleccione Crear suscripción.
7. Confirme la suscripción. Por ejemplo, si ha elegido un protocolo de correo electrónico, Amazon SNS enviará un mensaje de confirmación de la suscripción a la dirección de correo electrónico facilitada.

Suscribirse a los anuncios de CSPM de Security Hub (AWS CLI)

1. Use el siguiente comando:

```
 aws  sns --region us-west-2 subscribe --topic-arn arn:aws:sns:us-
west-2:393883065485:SecurityHubAnnouncements --protocol email --notification-
endpoint your_email@your_domain.com
```

2. Confirme la suscripción. Por ejemplo, si ha elegido un protocolo de correo electrónico, Amazon SNS enviará un mensaje de confirmación de la suscripción a la dirección de correo electrónico facilitada.

Formato de los mensajes de Amazon SNS

Los siguientes ejemplos muestran anuncios del CSPM de Security Hub desde Amazon SNS sobre la incorporación de nuevos controles de seguridad. El contenido de los mensajes varía según el tipo de anuncio, pero el formato es el mismo para todos los tipos de anuncios. Opcionalmente, se puede incluir un campo de `Link` que proporcione detalles sobre el anuncio.

Ejemplo: anuncio del CSPM de Security Hub sobre nuevos controles (protocolo de correo electrónico)

```
{
"AnnouncementType":"NEW_STANDARDS_CONTROLS",
"Title":"[New Controls] 36 new Security Hub CSPM controls added to theAWSFoundational
 Security Best Practices standard",
"Description":"We have added 36 new controls to theAWSFoundational Security Best
 Practices standard. These include controls for Amazon Auto Scaling (AutoScaling.3,
 AutoScaling.4, AutoScaling.6),CloudFormation(CloudFormation.1), Amazon CloudFront
 (CloudFront.10), Amazon Elastic Compute Cloud (Amazon EC2) (EC2.23, EC2.24, EC2.27),
 Amazon Elastic Container Registry (Amazon ECR) (ECR.1, ECR.2), Amazon Elastic
 Container Service (Amazon ECS) (ECS.3, ECS.4, ECS.5, ECS.8, ECS.10, ECS.12), Amazon
 Elastic File System (Amazon EFS) (EFS.3, EFS.4), Amazon Elastic Kubernetes Service
 (Amazon EKS) (EKS.2), Elastic Load Balancing (ELB.12, ELB.13, ELB.14), Amazon
 Kinesis (Kinesis.1),AWS Network Firewall(NetworkFirewall.3, NetworkFirewall.4,
 NetworkFirewall.5), Amazon OpenSearch Service (OpenSearch.7), Amazon Redshift
 (Redshift.9),
Amazon Simple Storage Service (Amazon S3) (S3.13), Amazon Simple Notification
 Service (SNS.2),AWS WAF(WAF.2, WAF.3, WAF.4, WAF.6, WAF.7, WAF.8). If you enabled
 theAWSFoundational Security Best Practices standard in an account and configured
 Security Hub CSPM to automatically enable new controls, these controls are enabled by
 default. Availability of controls can vary by Region. "
}
```

Ejemplo: anuncio del CSPM de Security Hub sobre nuevos controles (protocolo JSON por correo electrónico)

```
{
  "Type" : "Notification",
  "MessageId" : "d124c9cf-326a-5931-9263-92a92e7af49f",
  "TopicArn" : "arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements",
  "Message" : "{\"AnnouncementType\":\"NEW_STANDARDS_CONTROLS\",\"Title\":
\"[New Controls] 36 new Security Hub CSPM controls added to theAWSFoundational
 Security Best Practices standard\",\"Description\":\"We have added 36 new
 controls to theAWSFoundational Security Best Practices standard. These
 include controls for Amazon Auto Scaling (AutoScaling.3, AutoScaling.4,
 AutoScaling.6),CloudFormation(CloudFormation.1), Amazon CloudFront (CloudFront.10),
 Amazon Elastic Compute Cloud (Amazon EC2) (EC2.23, EC2.24, EC2.27), Amazon Elastic
 Container Registry (Amazon ECR) (ECR.1, ECR.2), Amazon Elastic Container Service
 (Amazon ECS) (ECS.3, ECS.4, ECS.5, ECS.8, ECS.10, ECS.12), Amazon Elastic File System
 (Amazon EFS) (EFS.3, EFS.4), Amazon Elastic Kubernetes Service (Amazon EKS) (EKS.2),
 Elastic Load Balancing (ELB.12, ELB.13, ELB.14), Amazon Kinesis (Kinesis.1),AWS
 Network Firewall(NetworkFirewall.3, NetworkFirewall.4, NetworkFirewall.5), Amazon
 OpenSearch Service (OpenSearch.7), Amazon Redshift (Redshift.9),
```

```
Amazon Simple Storage Service (Amazon S3) (S3.13), Amazon Simple Notification
 Service (SNS.2),AWS WAF(WAF.2, WAF.3, WAF.4, WAF.6, WAF.7, WAF.8). If you enabled
 theAWSFoundational Security Best Practices standard in an account and configured
 Security Hub CSPM to automatically enable new controls, these controls are enabled by
 default. Availability of controls can vary by Region. \"}",
  "Timestamp" : "2022-08-04T19:11:12.652Z",
  "SignatureVersion" : "1",
  "Signature" :
 "HTHgNFRYMetCvisulgLM4CVySvK9qCXFPHQDxYl9tuCFQuIrd7YO4m4YFR28XKMgzqrF20YP
+EilipUm2SOTpEEtOTekU5bn74+YmNZfwr4aPFx0vUuQCVOshmHl37hjkiLjhCg/t53QQiLfP7MH
+MTXIUPR37k5SuFCXvjpRQ8ynV532AH3Wpv0HmojDLMg+eg51V1fUsOG8yiJVCBEJhJ1yS
+gkwJdhRk2UQab9RcAmE6COK3hRWcjDwqTXz5nR6Ywv1ZqZfLIl7gYKslt+jsyd/k+7kOqGmOJRDr7qhE7H
+7vaGRLOptsQnbW8VmeYnDbahEO8FV+Mp1rpV+7Qg==",
  "SigningCertURL" : "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-56e67fcb41f6fec09b0196692625d385.pem",
  "UnsubscribeURL" : "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:393883065485:SecurityHubAnnouncements:9d0230d7-d582-451d-9f15-0c32818bf61f"
}
```


Cómo desactivar el CSPM de Security Hub

Puede deshabilitar el CSPM de AWS Security Hub mediante la consola CSPM de Security Hub o la API de Security Hub. Si deshabilita el CSPM de Security Hub, puede habilitarlo de nuevo más adelante.

Si la organización utiliza una configuración centralizada, el administrador delegado del CSPM de Security Hub puede crear políticas de configuración que desactiven el CSPM de Security Hub para cuentas y unidades organizativas (UO) específicas, y mantener el CSPM de Security Hub habilitado para otras. Las políticas de configuración afectan tanto a la región principal como a todas las regiones vinculadas. Para obtener más información, consulte Descripción de la configuración central en el CSPM de Security Hub.

Si desactiva el CSPM de Security Hub para una cuenta, ocurre lo siguiente:

- Todos los estándares y controles del CSPM de Security Hub se deshabilitan para la cuenta.
- El CSPM de Security Hub deja de generar, actualizar e ingerir resultados para la cuenta.
- Después de 30 días, el CSPM de Security Hub elimina de forma permanente todos los resultados archivados existentes de la cuenta. Los resultados no se pueden recuperar mediante el uso del CSPM de Security Hub.

- Después de 90 días, el CSPM de Security Hub elimina de forma permanente todos los resultados activos existentes de la cuenta. Los resultados no se pueden recuperar mediante el uso del CSPM de Security Hub.
- Después de 90 días, el CSPM de Security Hub elimina de forma permanente toda la información existente y la configuración del CSPM de Security Hub correspondiente a la cuenta. Los datos y la configuración no se pueden recuperar.

Para retener los resultados existentes, puede exportarlos a un bucket de S3 antes de deshabilitar el CSPM de Security Hub. Puedes hacerlo mediante una acción personalizada con una EventBridge regla de Amazon. Para obtener más información, consulte Uso EventBridge para respuesta y remediación automatizadas.

Si vuelve a habilitar el CSPM de Security Hub en un plazo de 90 días tras haberlo deshabilitado en una cuenta, recuperará el acceso a los resultados activos existentes, así como a la información y a la configuración del CSPM de Security Hub para la cuenta. Si vuelve a habilitar el CSPM de Security Hub en un plazo de 30 días, también recuperará el acceso a los resultados archivados existentes de la cuenta. Sin embargo, los resultados existentes pueden ser inexactos porque reflejarán el estado de su AWS entorno cuando deshabilitó Security Hub CSPM. Además, al volver a habilitar los estándares y controles individuales, Security Hub CSPM podría generar inicialmente resultados duplicados para AWS recursos específicos, en función de los estándares y controles que habilite. Por estas razones, recomendamos que realice una de las siguientes acciones:

- Cambie el estado del flujo de trabajo de todos los resultados existentes a `RESOLVED` antes de deshabilitar el CSPM de Security Hub. Para obtener más información, consulte Configuración del estado de flujo de trabajo de los resultados.
- Deshabilite todos los estándares al menos seis días antes de deshabilitar el CSPM de Security Hub. El CSPM de Security Hub archiva todos los resultados existentes dentro de lo posible, normalmente en un plazo de tres a cinco días. Para obtener más información, consulte Desactivación de un estándar.

No puede desactivar el CSPM de Security Hub en los siguientes casos:

- La cuenta es la cuenta de administrador delegado del CSPM de Security Hub para una organización. Si usa configuración centralizada, no puede asociar una política de configuración que desactive el CSPM de Security Hub para la cuenta de administrador delegado. La asociación puede funcionar para otras cuentas, pero el CSPM de Security Hub no aplica la política a la cuenta de administrador delegado.

- La cuenta es una cuenta de administrador del CSPM de Security Hub por invitación y tiene cuentas de miembro. Antes de poder desactivar el CSPM de Security Hub, debe desasociar todas las cuentas de miembro. Para aprender a hacerlo, consulte the section called “Desasociación de cuentas miembro”.

Antes de que el propietario de una cuenta de miembro pueda desactivar el CSPM de Security Hub, la cuenta se debe desasociar de la cuenta de administrador. Para una cuenta de organización, solo la cuenta de administrador puede desvincular una cuenta de miembro. Para obtener más información, consulte the section called “Desasociación de cuentas de la organización como cuentas de miembro”. En el caso de cuentas invitadas manualmente, la cuenta de administrador o la cuenta de miembro pueden desasociar la cuenta. Para obtener más información, consulte the section called “Desasociación de cuentas miembro” o the section called “Desvinculación de una cuenta de administrador”. No es necesario desasociar si usa la configuración centralizada, ya que el administrador del CSPM de Security Hub puede crear una política que desactive el CSPM de Security Hub para cuentas de miembro específicas.

Cuando inhabilitas el CSPM de Security Hub para una cuenta, solo se inhabilita en la cuenta actual. Región de AWS Sin embargo, si usa la configuración centralizada para desactivar el CSPM de Security Hub para cuentas específicas, este se desactiva en la región de inicio y en todas las regiones vinculadas.

Para desactivar el CSPM de Security Hub, elija el método que prefiera y siga los pasos.

Security Hub CSPM console

Siga estos pasos para utilizar la consola para desactivar el CSPM de Security Hub.

Para desactivar el CSPM de Security Hub

1. Abra la consola CSPM de AWS Security Hub en. https://console.aws.amazon.com/securityhub/
2. En el panel de navegación, en Configuración, seleccione General.
3. En la sección Desactivar Security Hub CSPM, elija Desactivar Security Hub CSPM.
4. Cuando se solicite confirmación, elija Desactivar el CSPM de Security Hub.

Security Hub API

Para deshabilitar el CSPM de Security Hub mediante programación, utilice el DisableSecurityHubfuncionamiento de la API de Security HubAWS. O bien, si está utilizando el, ejecute el comando AWS CLI disable-security-hub. Por ejemplo, el siguiente comando desactiva el CSPM de Security Hub en la versión actual: Región de AWS

```
$ aws securityhub disable-security-hub
```

Seguridad en AWS Security Hub CSPM

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, se beneficia de una arquitectura de red y centro de datos diseñada para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre usted AWS y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la AWS nube. AWS también le proporciona servicios que puede usar de forma segura. Third-partylos auditores prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los programas de AWS cumplimiento. Para obtener más información sobre los programas de conformidad que se aplican a AWS Security Hub CSPM, consulte Servicios de AWS en el ámbito del programa de conformidad.
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. También es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y la normativa aplicables.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida al usar Security Hub CSPM. En los siguientes temas se muestra cómo configurar el CSPM de Security Hub para cumplir sus objetivos de seguridad y cumplimiento. También aprenderá a usar otros AWS servicios que le ayudan a supervisar y proteger sus recursos de CSPM de Security Hub.

Temas

- Protección de datos en AWS Security Hub CSPM
- AWS Administración de identidades y accesos para Security Hub CSPM

- Validación de conformidad para AWS Security Hub CSPM
- Resiliencia en AWS Centro de seguridad
- Seguridad de la infraestructura en AWS Security Hub CSPM
- AWS Security Hub CSPM y puntos finales de interfaz de VPC (AWS PrivateLink)

Protección de datos en AWS Security Hub CSPM

El modelo de responsabilidad compartida de AWS se aplica a la protección de datos en AWS Security Hub CSPM. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta todo el. Nube de AWS Eres responsable de mantener el control sobre el contenido alojado en esta infraestructura. También eres responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulte las Preguntas frecuentes sobre la privacidad de los datos y las condiciones legales de la región de . Para obtener más información sobre la protección de datos en Europa, consulte el Centro del Reglamento General de Protección de Datos (RGPD).

Con fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure los usuarios individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utiliza la autenticación multifactor (MFA) en cada cuenta.
- Úselo SSL/TLS para comunicarse con AWS los recursos. Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Configure el registro de actividad de los usuarios y de la API con AWS CloudTrail. Para obtener información sobre el uso de CloudTrail rutas para capturar AWS actividades, consulte Cómo trabajar con CloudTrail rutas en la Guía del AWS CloudTrail usuario.
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados que contiene Servicios de AWS.
- Utiliza servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger la información confidencial almacenada en Amazon S3.
- Si necesita módulos criptográficos validados por la FIPS 140-3 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información

sobre los puntos de conexión de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-3.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabajas con Security Hub CSPM u otro sistema Servicios de AWS mediante la consola, la API o los SDK. AWS CLI AWS Cualquier dato que introduzca en etiquetas o campos de formato libre utilizados para los nombres se pueden emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya información de credenciales en la URL a fin de validar la solicitud para ese servidor.

Security Hub CSPM es una oferta de servicios para varios usuarios. Para garantizar la protección de los datos, Security Hub CSPM cifra los datos en reposo y los datos en tránsito entre los servicios de los componentes.

AWS Administración de identidades y accesos para Security Hub CSPM

AWS Identity and Access Management (IAM) ayuda al administrador a controlar de forma segura el acceso a los recursos. Servicio de AWS AWS Los administradores de IAM controlan quién puede estar autenticado (ha iniciado sesión) y autorizado (tiene permisos) para utilizar recursos de Security Hub. IAM es un Servicio de AWS servicio que puede utilizar sin coste adicional.

Temas

- Público
- Autenticación con identidades
- Administración del acceso con políticas
- Cómo funciona Security Hub con IAM
- Identity-based ejemplos de políticas para AWS Security Hub CSPM
- Service-linked roles para AWS Security Hub CSPM
- AWS políticas administradas para Security Hub
- Resolución de problemas AWS Security Hub CSPM identidad y acceso

Público

La forma en que usas AWS Identity and Access Management (IAM) difiere según tu función:

- Usuario del servicio: solicite permisos al administrador si no puede acceder a las características (consulte Resolución de problemas AWS Security Hub CSPM identidad y acceso).
- Administrador del servicio: determine el acceso de los usuarios y envíe las solicitudes de permiso (consulte Cómo funciona Security Hub con IAM).
- Administrador de IAM: escribe las políticas para administrar el acceso (consulte Identity-based ejemplos de políticas para AWS Security Hub CSPM).

Autenticación con identidades

La autenticación es la forma en que inicias sesión AWS con tus credenciales de identidad. Debe autenticarse como usuario de Usuario raíz de la cuenta de AWS IAM o asumiendo una función de IAM.

Puedes iniciar sesión como una identidad federada con credenciales de una fuente de identidad, como AWS IAM Identity Center (el centro de identidad de IAM), la autenticación de inicio de sesión único o las credenciales. Google/Facebook Para obtener más información sobre el inicio de sesión, consulte Cómo iniciar sesión en la Cuenta de AWS en la Guía del usuario de AWS Sign-In .

Para el acceso programático, AWS proporciona un SDK y una CLI para firmar criptográficamente las solicitudes. Para obtener más información, consulte AWS Signature Version 4 para solicitudes de API en la Guía del usuario de IAM.

Cuenta de AWS usuario raíz

Cuando creas una Cuenta de AWS, comienzas con una identidad de inicio de sesión denominada usuario Cuenta de AWS raíz que tiene acceso total a todos los recursos. Servicios de AWS Se recomiendaencarecidamente que no utilice el usuario raíz para las tareas diarias. Para ver las tareas que requieren credenciales de usuario raíz, consulte Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Identidad federada

Como práctica recomendada, exija a los usuarios humanos que utilicen la federación con un proveedor de identidad para acceder Servicios de AWS mediante credenciales temporales.

Una identidad federada es un usuario de su directorio empresarial, proveedor de identidad web o Directory Service que accede Servicios de AWS mediante credenciales de una fuente de identidad. Las identidades federadas asumen roles que proporcionan credenciales temporales.

Para una administración de acceso centralizada, se recomienda AWS IAM Identity Center. Para obtener más información, consulte ¿Qué es el Centro de identidades de IAM? en la Guía del usuario de AWS IAM Identity Center .

Usuarios y grupos de IAM

Un usuario de IAM es una identidad con permisos específicos para una sola persona o aplicación. Recomendamos el uso de credenciales temporales en lugar de usuarios de IAM con credenciales de larga duración. Para obtener más información, consulte Exigir a los usuarios humanos que utilicen la federación con un proveedor de identidad para acceder AWS mediante credenciales temporales en la Guía del usuario de IAM.

Un grupo de IAM especifica un conjunto de usuarios de IAM y facilita la administración de los permisos para grupos grandes de usuarios. Para obtener más información, consulte Casos de uso para usuarios de IAM en la Guía del usuario de IAM.

Roles de IAM

Un Rol de IAM es una identidad con permisos específicos que proporciona credenciales temporales. Puede asumir un rol cambiando de un rol de usuario a uno de IAM (consola) o llamando a una AWS CLI operación de AWS API. Para obtener más información, consulte Métodos para asumir un rol en la Guía del usuario de IAM.

Los roles de IAM son útiles para el acceso de usuario federado, los permisos de usuario de IAM temporales, el acceso entre cuentas, el acceso entre servicios y las aplicaciones que se ejecutan en Amazon EC2. Para obtener más información, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Administración del acceso con políticas

Puedes controlar el acceso AWS creando políticas y adjuntándolas a AWS identidades o recursos. Una política define los permisos cuando se asocian a una identidad o un recurso. AWS evalúa estas políticas cuando un director hace una solicitud. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre los documentos de políticas de JSON, consulte Información general de políticas de JSON en la Guía del usuario de IAM.

Mediante las políticas, los administradores especifican quién tiene acceso a qué, definiendo qué entidad principal puede realizar acciones sobre qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Un administrador de IAM crea políticas de IAM y las agrega a roles, que los usuarios pueden asumir posteriormente. Las políticas de IAM definen permisos independientemente del método que se utilice para realizar la operación.

Identity-based políticas

Identity-based las políticas son documentos de política de permisos de JSON que se adjuntan a una identidad (usuario, grupo o rol). Estas políticas controlan qué acciones pueden realizar las identidades, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en la identidad, consulte Definición de permisos de IAM personalizados con políticas administradas por el cliente en la Guía del usuario de IAM.

Identity-based las políticas pueden ser políticas en línea (integradas directamente en una sola identidad) o políticas administradas (políticas independientes asociadas a varias identidades). Para obtener información sobre cómo elegir entre políticas administradas e insertadas, consulte Selección entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Resource-based políticas

Resource-based las políticas son documentos de políticas JSON que se adjuntan a un recurso. Los ejemplos incluyen las Políticas de confianza de roles de IAM y las Políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Debe especificar una entidad principal en una política basada en recursos.

Resource-based las políticas son políticas en línea que se encuentran en ese servicio. No puede usar políticas AWS administradas de IAM en una política basada en recursos.

Otros tipos de políticas

AWS admite tipos de políticas adicionales que pueden establecer los permisos máximos que otorgan los tipos de políticas más comunes:

- Límites de permisos: establecen los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM. Para obtener más información, consulte Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.
- Políticas de control de servicios (SCP): especifican los permisos máximos para una organización o unidad organizativa en AWS Organizations. Para obtener más información, consulte Políticas de control de servicios en la Guía del usuario de AWS Organizations .

- Políticas de control de recursos (RCP): definen los permisos máximos disponibles para los recursos de las cuentas. Para obtener más información, consulte Políticas de control de recursos (RCP) en la Guía del usuario de AWS Organizations .
- Políticas de sesión: políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal para un rol o un usuario federado. Para obtener más información, consulte Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo se AWS determina si se permite una solicitud cuando se trata de varios tipos de políticas, consulte la lógica de evaluación de políticas en la guía del usuario de IAM.

Cómo funciona Security Hub con IAM

Antes de usar AWS Identity and Access Management (IAM) para administrar el acceso AWS Security Hub CSPM, averigüe qué funciones de IAM están disponibles para su uso con Security Hub CSPM.

Funciones de IAM con las que puede usar AWS Security Hub CSPM

Característica de IAM	Compatibilidad con Security Hub CSPM
Identity-based políticas	Sí
Resource-based políticas	No
Acciones de políticas	Sí
Recursos de políticas	No
Claves de condición de política	Sí
Listas de control de acceso (ACL)	No
Attribute-based control de acceso (ABAC): etiquetas en las políticas	Sí
Credenciales temporales	Sí

Característica de IAM	Compatibilidad con Security Hub CSPM
Sesiones de acceso directo (FAS)	Sí
Roles de servicio	No
Service-linked roles	Sí

Para obtener una visión general de cómo Servicios de AWS funcionan Security Hub CSPM y otros con la mayoría de las funciones de IAM, consulte la sección sobre cómo Servicios de AWS funciona con IAM en la Guía del usuario de IAM.

Identity-based políticas para Security Hub CSPM

Compatibilidad con las políticas basadas en identidad: sí

Identity-based las políticas son documentos de política de permisos de JSON que puede adjuntar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en la identidad, consulte Definición de permisos de IAM personalizados con políticas administradas por el cliente en la Guía del usuario de IAM.

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. Para obtener más información sobre los elementos que puede utilizar en una política de JSON, consulte Referencia de los elementos de la política de JSON de IAM en la Guía del usuario de IAM.

El CSPM de Security Hub admite políticas basadas en la identidad. Para obtener más información, consulte Identity-based ejemplos de políticas para AWS Security Hub CSPM.

Resource-based políticas para Security Hub CSPM

Admite políticas basadas en recursos: no

Resource-based las políticas son documentos de políticas JSON que se adjuntan a un recurso. Los ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad

principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política basada en recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Para habilitar el acceso entre cuentas, puede especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. Para obtener más información, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Security Hub CSPM no admite políticas basadas en recursos. No puede adjuntar una política de IAM directamente a un recurso de CSPM de Security Hub.

Acciones de política para Security Hub CSPM

Compatibilidad con las acciones de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Las acciones de política en Security Hub CSPM utilizan el siguiente prefijo antes de la acción:

```
securityhub:
```

Por ejemplo, para conceder a un usuario permiso para habilitar el CSPM de Security Hub, que es una acción que corresponde al `EnableSecurityHub` funcionamiento de la API de CSPM de Security Hub, incluya la acción en su política. `securityhub:EnableSecurityHub` Las instrucciones de la política deben incluir un elemento `Action` o un elemento `NotAction`. El CSPM de Security Hub define su propio conjunto de acciones que describen las tareas que puede realizar con este servicio.

```
"Action": "securityhub:EnableSecurityHub"
```

Para especificar varias acciones en una única instrucción, sepárelas con comas. Por ejemplo:

```
"Action": [
      "securityhub:EnableSecurityHub",
      "securityhub:BatchEnableStandards"
```

También puede utilizar caracteres comodín para especificar varias acciones (*). Por ejemplo, para especificar todas las acciones que comiencen con la palabra `Get`, incluya la siguiente acción:

```
"Action": "securityhub:Get*"
```

Sin embargo, recomendamos que las políticas se creen según el principio de privilegios mínimos. En otras palabras, debe crear políticas que incluyan solo los permisos necesarios para realizar una tarea específica.

El usuario debe tener acceso a la operación `DescribeStandardsControl` para poder acceder a `BatchGetSecurityControls`, `BatchGetStandardsControlAssociations` y `ListStandardsControlAssociations`.

El usuario debe tener acceso a la operación `UpdateStandardsControls` para poder acceder a `BatchUpdateStandardsControlAssociations` y `UpdateSecurityControl`.

Para obtener una lista de las acciones de CSPM de Security Hub, consulte Acciones definidas por AWS Security Hub CSPM en la referencia de autorización del servicio. Para ver ejemplos de políticas que especifican las acciones de CSPM de Security Hub, consulte. Identity-based ejemplos de políticas para AWS Security Hub CSPM

Recursos de políticas para Security Hub CSPM

Compatibilidad con recursos de políticas: no

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). En el caso de las acciones que no admiten permisos por recurso, utilice un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

```
"Resource": "*"
```

El CSPM de Security Hub define los siguientes tipos de recursos:

- Hub
- Producto
- Agregador de resultados, también denominado agregador entre regiones

- Regla de automatización
- Configuración de políticas

Puede especificar estos tipos de recursos en políticas utilizando los ARN.

Para obtener una lista de los tipos de recursos de CSPM de Security Hub y la sintaxis ARN de cada uno de ellos, consulte los tipos de recursos definidos AWS Security Hub CSPM en la Referencia de autorización de servicios. Para saber qué acciones puede especificar para cada tipo de recurso, consulte Acciones definidas por AWS Security Hub CSPM en la Referencia de autorizaciones de servicio. Para ver ejemplos de políticas que especifican recursos, consulte Identity-based ejemplos de políticas para AWS Security Hub CSPM.

Claves de condiciones de política para el CSPM de Security Hub

Compatibilidad con claves de condición de políticas específicas del servicio: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` especifica cuándo se ejecutan las instrucciones en función de criterios definidos. Puede crear expresiones condicionales que utilizan operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud. Para ver todas las claves de condiciones AWS globales, consulte las claves de contexto de condiciones AWS globales en la guía del usuario de IAM.

Para obtener una lista de las claves de condición de CSPM de Security Hub, consulte las claves de condición que aparecen AWS Security Hub CSPM en la referencia de autorización de servicio. Para obtener más información acerca de las acciones y los recursos con los que puede utilizar una clave de condición, consulte Acciones definidas por AWS Security Hub CSPM. Para ver ejemplos de políticas que utilizan claves de condición, consulte Identity-based ejemplos de políticas para AWS Security Hub CSPM.

Listas de control de acceso (ACL) en Security Hub CSPM

Compatibilidad con ACL: no

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

El CSPM de Security Hub no admite las ACL, lo que significa que no puede adjuntar una ACL a un recurso de CSPM de Security Hub.

Attribute-based control de acceso (ABAC) con Security Hub CSPM

Admite ABAC (etiquetas en las políticas): sí

Attribute-based el control de acceso (ABAC) es una estrategia de autorización que define los permisos en función de atributos denominados etiquetas. Puede adjuntar etiquetas a las entidades y AWS los recursos de IAM y, a continuación, diseñar políticas de ABAC para permitir las operaciones cuando la etiqueta del principal coincida con la etiqueta del recurso.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información sobre ABAC, consulte Definición de permisos con la autorización de ABAC en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulte Uso del control de acceso basado en atributos (ABAC) en la Guía del usuario de IAM.

Puede adjuntar etiquetas a los recursos de CSPM de Security Hub. También puede controlar el acceso a los recursos proporcionando información sobre las etiquetas en el elemento `Condition` de una política.

Para obtener información sobre cómo etiquetar los recursos de CSPM de Security Hub, consulte. Etiquetado de recursos de Security Hub Para obtener un ejemplo de política basada en identidad que controla el acceso a un recurso basado en etiquetas, consulte Identity-based ejemplos de políticas para AWS Security Hub CSPM.

Uso de credenciales temporales con Security Hub CSPM

Compatibilidad con credenciales temporales: sí

Las credenciales temporales proporcionan acceso a corto plazo a AWS los recursos y se crean automáticamente al usar la federación o al cambiar de rol. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para obtener más información, consulte Credenciales de seguridad temporales en IAM y Servicios de AWS que funcionan con IAM en la Guía del usuario de IAM.

Puede utilizar credenciales temporales para iniciar sesión con federación, asumir un rol de IAM o asumir un rol de acceso entre cuentas. Las credenciales de seguridad temporales se obtienen llamando a operaciones de AWS STS API como AssumeRole o GetFederationToken.

Security Hub CSPM admite el uso de credenciales temporales.

Sesiones de acceso directo para Security Hub CSPM

Admite sesiones de acceso directo (FAS): sí

Las sesiones de acceso directo (FAS) utilizan los permisos de la persona principal que llama a una Servicio de AWS, junto con la solicitud Servicio de AWS para realizar solicitudes a los servicios descendentes. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Sesiones de acceso directo.

Por ejemplo, el CSPM de Security Hub hace que las solicitudes de FAS sean descendentes Servicios de AWS cuando se integra el CSPM de Security Hub AWS Organizations y cuando se designa la cuenta de administrador de CSPM delegada de Security Hub para una organización en Organizations.

Para otras tareas, el CSPM de Security Hub usa una función vinculada a un servicio para realizar acciones en su nombre. Para obtener más información sobre este rol, consulte Service-linked roles para AWS Security Hub CSPM.

Funciones de servicio para Security Hub CSPM

El CSPM de Security Hub no asume ni usa funciones de servicio. Para realizar acciones en su nombre, el CSPM de Security Hub usa una función vinculada a un servicio. Para obtener más información sobre este rol, consulte Service-linked roles para AWS Security Hub CSPM.

> **Warning**
>
> Cambiar los permisos de un rol de servicio puede crear problemas operativos con el uso del CSPM de Security Hub. Edite las funciones de servicio solo cuando el CSPM de Security Hub le brinde instrucciones para hacerlo.

Service-linked roles para Security Hub (CSPM)

Compatible con roles vinculados al servicio: sí

Un rol vinculado a un servicio es un tipo de rol de servicio que está vinculado a un. Servicio de AWS El servicio puede asumir la función de realizar una acción en su nombre. Service-linked las funciones aparecen en su nombre Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

El CSPM de Security Hub usa un rol vinculado a un servicio para realizar acciones en su nombre. Para obtener más información sobre este rol, consulte Service-linked roles para AWS Security Hub CSPM.

Identity-based ejemplos de políticas para AWS Security Hub CSPM

De forma predeterminada, los usuarios y los roles no tienen permiso para crear o modificar los recursos de CSPM de Security Hub. Tampoco pueden realizar tareas mediante la API o Consola de administración de AWS AWS la AWS CLI API. Un administrador debe crear políticas de IAM que concedan permisos a los usuarios y a los roles para realizar operaciones de la API concretas en los recursos especificados que necesiten. El administrador debe adjuntar esas políticas a los usuarios o grupos que necesiten esos permisos.

Para obtener información acerca de cómo crear una política basada en identidad de IAM con estos documentos de políticas JSON de ejemplo, consulte Creación de políticas en la pestaña JSON en la Guía del usuario de IAM.

Temas

- Prácticas recomendadas relativas a políticas
- Uso de la consola CSPM de Security Hub
- Ejemplo: Permitir que los usuarios vean sus propios permisos
- Ejemplo: Permitir a los usuarios crear y administrar una política de configuración
- Ejemplo: Permitir a los usuarios ver los resultados
- Ejemplo: Permitir a los usuarios crear y administrar reglas de automatización

Prácticas recomendadas relativas a políticas

Identity-based las políticas determinan si alguien puede crear los recursos de Security Hub de tu cuenta, acceder a ellos o eliminarlos. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos en muchos casos de uso comunes. Están disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por los AWS clientes que sean específicas para sus casos de uso. Con el fin de obtener más información, consulte las políticas administradas por AWS o las políticas administradas por AWS para funciones de tarea en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulte Políticas y permisos en IAM en la Guía del usuario de IAM.
- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder acceso a las acciones de servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo CloudFormation. Para obtener más información, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utiliza el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte Validación de políticas con el Analizador de acceso de IAM en la Guía del usuario de IAM.
- Exigir la autenticación multifactor (MFA): si tienes una situación en la que se requieren usuarios de IAM o un usuario raíz Cuenta de AWS, activa la MFA para aumentar la seguridad. Para exigir la MFA cuando se invoquen las operaciones de la API, añada condiciones de MFA a sus políticas. Para más información, consulte Acceso seguro a la API con MFA en la Guía del usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.

Uso de la consola CSPM de Security Hub

Para acceder a la AWS Security Hub CSPM consola, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle enumerar y ver detalles sobre los recursos de CSPM de Security Hub que tiene. Cuenta de AWS Si crea una política basada en identidades que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles) que tengan esa política.

No es necesario que concedas permisos mínimos de consola a los usuarios que solo realizan llamadas a la API AWS CLI o a la AWS API. En su lugar, permita el acceso únicamente a las acciones que coincidan con la operación de API que intentan realizar.

Para garantizar que esos usuarios y roles puedan usar la consola CSPM de Security Hub, adjunte también la siguiente política AWS administrada a la entidad. Para obtener más información, consulte Agregar de permisos a un usuario en la Guía del usuario de IAM:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "securityhub:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "securityhub.amazonaws.com"
                }
            }
        }
    ]
}
```

Ejemplo: Permitir que los usuarios vean sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a los usuarios de IAM ver las políticas administradas e insertadas que se asocian a la identidad de sus usuarios. Esta política incluye permisos para completar esta acción en la consola o mediante programación mediante la API or. AWS CLI AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Ejemplo: Permitir a los usuarios crear y administrar una política de configuración

En este ejemplo, se muestra cómo crear una política de IAM que permita a un usuario crear, ver, actualizar y eliminar políticas de configuración. En este ejemplo de política, también se permite al usuario iniciar, detener y ver asociaciones de políticas. Para que esta política de IAM funcione, el usuario debe ser el administrador delegado de CSPM de Security Hub de una organización.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "CreateAndUpdateConfigurationPolicy",
            "Effect": "Allow",
            "Action": [
                "securityhub:CreateConfigurationPolicy",
                "securityhub:UpdateConfigurationPolicy"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ViewConfigurationPolicy",
            "Effect": "Allow",
            "Action": [
                "securityhub:GetConfigurationPolicy",
                "securityhub:ListConfigurationPolicies"
            ],
            "Resource": "*"
        },
        {
            "Sid": "DeleteConfigurationPolicy",
            "Effect": "Allow",
            "Action": [
                "securityhub:DeleteConfigurationPolicy"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ViewConfigurationPolicyAssociation",
            "Effect": "Allow",
            "Action": [
```

```
                "securityhub:BatchGetConfigurationPolicyAssociations",
                "securityhub:GetConfigurationPolicyAssociation",
                "securityhub:ListConfigurationPolicyAssociations"
            ],
            "Resource": "*"
        },
        {
            "Sid": "UpdateConfigurationPolicyAssociation",
            "Effect": "Allow",
            "Action": [
                "securityhub:StartConfigurationPolicyAssociation",
                "securityhub:StartConfigurationPolicyDisassociation"
            ],
            "Resource": "*"
        }
    ]
}
```

Ejemplo: Permitir a los usuarios ver los resultados

En este ejemplo se muestra cómo puede crear una política de IAM que permita a un usuario ver las conclusiones del CSPM de Security Hub.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ReviewFindings",
            "Effect": "Allow",
            "Action": [
                "securityhub:GetFindings"
            ],
            "Resource": "*"
        }
    ]
}
```

Ejemplo: Permitir a los usuarios crear y administrar reglas de automatización

En este ejemplo se muestra cómo puede crear una política de IAM que permita a un usuario crear, ver, actualizar y eliminar las reglas de automatización de CSPM de Security Hub. Para que esta política de IAM funcione, el usuario debe ser un administrador de CSPM de Security Hub. Para limitar los permisos (por ejemplo, para permitir que un usuario solo vea las reglas de automatización), puede eliminar los permisos de creación, actualización y eliminación.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "CreateAndUpdateAutomationRules",
            "Effect": "Allow",
            "Action": [
                "securityhub:CreateAutomationRule",
                "securityhub:BatchUpdateAutomationRules"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ViewAutomationRules",
            "Effect": "Allow",
            "Action": [
                "securityhub:BatchGetAutomationRules",
                "securityhub:ListAutomationRules"
            ],
            "Resource": "*"
        },
        {
            "Sid": "DeleteAutomationRules",
            "Effect": "Allow",
            "Action": [
                "securityhub:BatchDeleteAutomationRules"
            ],
            "Resource": "*"
        }
    ]
}
```

Service-linked roles para AWS Security Hub CSPM

AWS Security Hub CSPM usa una función vinculada a un AWS Identity and Access Management servicio (IAM) denominada. https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_terms-and-concepts.html#iam-term-service-linked-role `AWSServiceRoleForSecurityHub` Este rol vinculado a un servicio es un rol de IAM que está vinculado directamente al CSPM de Security Hub. Está predefinida por el CSPM de Security Hub e incluye todos los permisos que el CSPM de Security Hub necesita para llamar a otros recursos y supervisarlos en su nombre. Servicios de AWS AWS El CSPM de Security Hub usa esta función vinculada a servicios en todos los lugares en los que el CSPM de Security Hub está disponible. Regiones de AWS

Una función vinculada a un servicio facilita la configuración del CSPM de Security Hub, ya que no es necesario agregar manualmente los permisos necesarios. El CSPM de Security Hub define los permisos de su función vinculada a un servicio y, a menos que se defina lo contrario, solo el CSPM de Security Hub puede asumir la función. Los permisos definidos incluyen las políticas de confianza y de permisos, y no puede asociar esa política de permisos a ninguna otra entidad de IAM.

Para revisar los detalles de la función vinculada a un servicio, puede usar la consola CSPM de Security Hub. En el panel de navegación, elija General en Configuración. Luego, en la sección Permisos del servicio, elija Ver permisos del servicio.

Puede eliminar el rol vinculado al servicio CSPM de Security Hub solo después de deshabilitar el CSPM de Security Hub en todas las regiones en las que esté habilitado. Esto protege sus recursos de CSPM de Security Hub, ya que no puede eliminar inadvertidamente los permisos de acceso a ellos.

Para obtener información sobre otros servicios que admiten funciones vinculadas a servicios, consulte los AWS servicios que funcionan con IAM en la guía del usuario de IAM y busque los servicios que tienen la palabra Sí en la columna de funciones. Service-linked Seleccione una opción Sí con una conexión para revisar la documentación acerca del rol vinculado a un servicio en cuestión.

Temas

- Service-linked permisos de rol para Security Hub (CSPM)
- Crear un rol vinculado a un servicio para Security Hub CSPM
- Editar un rol vinculado a un servicio para Security Hub CSPM
- Eliminar un rol vinculado a un servicio para Security Hub CSPM

Service-linked permisos de rol para Security Hub (CSPM)

El CSPM de Security Hub usa el rol vinculado al servicio denominado. `AWSServiceRoleForSecurityHub` Es un rol vinculado a un servicio que se requiere para acceder a sus recursos. AWS Security Hub CSPM Esta función vinculada a un servicio permite al CSPM de Security Hub realizar tareas como recibir los hallazgos de otras personas Servicios de AWS y configurar la AWS Config infraestructura necesaria para ejecutar las comprobaciones de seguridad de los controles. El rol vinculado a servicios `AWSServiceRoleForSecurityHub` confía en el servicio `securityhub.amazonaws.com` para asumir el rol.

El rol vinculado al servicio `AWSServiceRoleForSecurityHub` utiliza la política administrada de `AWSSecurityHubServiceRolePolicy`.

Debe conceder permisos para permitir a una identidad de IAM (como un rol, grupo o usuario) crear, editar o eliminar un rol vinculado a un servicio. Para que la función `AWSServiceRoleForSecurityHub` vinculada a un servicio se cree correctamente, la identidad de IAM que utilice para acceder al CSPM de Security Hub debe tener los permisos necesarios. Para conceder los permisos necesarios, asocie la siguiente política a la identidad de IAM.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "securityhub:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "securityhub.amazonaws.com"
                }
            }
        }
    ]
```

```
}
```

Crear un rol vinculado a un servicio para Security Hub CSPM

El rol `AWSServiceRoleForSecurityHub` vinculado a un servicio se crea automáticamente cuando habilita el CSPM de Security Hub por primera vez o cuando habilita el CSPM de Security Hub en una región en la que no lo haya habilitado anteriormente. También puede crear manualmente el rol vinculado al servicio de `AWSServiceRoleForSecurityHub` por medio de la consola de IAM, la CLI de IAM o la API de IAM. Para obtener más información acerca de cómo crear un rol manualmente, consulte Crear un rol vinculado a un servicio en la Guía del usuario de IAM.

> **Important**
>
> La función vinculada a un servicio que se crea para una cuenta de administrador de CSPM de Security Hub no se aplica a las cuentas de miembros de CSPM de Security Hub asociadas.

Editar un rol vinculado a un servicio para Security Hub CSPM

El CSPM de Security Hub no permite editar el rol vinculado a un servicio. `AWSServiceRoleForSecurityHub` Después de crear un rol vinculado a un servicio, no puede cambiarle el nombre, ya que varias entidades pueden hacer referencia a él. Sin embargo, puede editar la descripción del rol mediante IAM. Para obtener más información, consulte Edición de un rol vinculado a un servicio en la Guía del usuario de IAM.

Eliminar un rol vinculado a un servicio para Security Hub CSPM

Si ya no necesita utilizar una característica o servicio que requiere un rol vinculado a un servicio, le recomendamos que elimine el rol. De esta forma, no tendrá una entidad no utilizada cuya supervisión o mantenimiento no se realizan de forma activa.

Al deshabilitar el CSPM de Security Hub, el CSPM de Security Hub no elimina automáticamente el rol vinculado al servicio. `AWSServiceRoleForSecurityHub` Si vuelve a habilitar el CSPM de Security Hub, el servicio puede volver a utilizar el rol vinculado al servicio existente. Si ya no necesita usar el CSPM de Security Hub, puede eliminar manualmente el rol vinculado al servicio.

> **Important**
>
> Antes de eliminar el rol `AWSServiceRoleForSecurityHub` vinculado a un servicio, primero debe deshabilitar el CSPM de Security Hub en todas las regiones en las que esté habilitado. Para obtener más información, consulte Cómo desactivar el CSPM de Security Hub. Si el CSPM de Security Hub no está desactivado al intentar eliminar el rol vinculado al servicio, la eliminación fallará.

Para eliminar el rol vinculado al servicio de `AWSServiceRoleForSecurityHub`, puede usar la consola de IAM, la CLI de IAM o la API de IAM. Para obtener más información, consulte Eliminación de un rol vinculado a servicios en la Guía del usuario de IAM.

AWS políticas administradas para Security Hub

Una política AWS administrada es una política independiente creada y administrada por. AWS AWS las políticas administradas están diseñadas para proporcionar permisos para muchos casos de uso comunes, de modo que pueda empezar a asignar permisos a usuarios, grupos y funciones.

Ten en cuenta que es posible que las políticas AWS administradas no otorguen permisos con privilegios mínimos para tus casos de uso específicos, ya que están disponibles para que los usen todos los AWS clientes. Se recomienda definir políticas administradas por el cliente específicas para sus casos de uso a fin de reducir aún más los permisos.

No puedes cambiar los permisos definidos en AWS las políticas administradas. Si AWS actualiza los permisos definidos en una política AWS administrada, la actualización afecta a todas las identidades principales (usuarios, grupos y roles) a las que está asociada la política. AWS es más probable que actualice una política AWS administrada cuando Servicio de AWS se lance una nueva o cuando haya nuevas operaciones de API disponibles para los servicios existentes.

Para obtener más información, consulte Políticas administradas por AWS en la Guía del usuario de IAM.

AWS política gestionada: AWSSecurityHubFullAccess

Puede asociar la política `AWSSecurityHubFullAccess` a las identidades de IAM.

Esta política otorga permisos administrativos que permiten a una entidad principal obtener acceso completo a todas las acciones del CSPM de Security Hub. Esta política se debe asociar a una entidad principal antes de habilitar manualmente el CSPM de Security Hub para la cuenta. Por

ejemplo, las entidades principales con estos permisos pueden tanto ver como actualizar el estado de los resultados. También pueden configurar resultados de información personalizados, habilitar integraciones, y habilitar o deshabilitar estándares y controles. Las entidades principales de una cuenta de administrador también pueden administrar cuentas miembro.

Detalles de los permisos

Esta política incluye los permisos siguientes:

- `securityhub`: concede a las entidades principales acceso completo a todas las acciones del CSPM de Security Hub.
- `guardduty`— Permite a los directores gestionar todo el ciclo de vida de un detector, gestionar los administradores de la organización, gestionar las cuentas de los miembros y configurar toda la organización en Amazon. GuardDuty Esto incluye las acciones de la API: GetDetector,, ListDetector, CreateDetector,, UpdateDetector, DeleteDetector, EnableOrganizationAdminAccount, ListOrganizationAdminAccounts. CreateMembers UpdateOrganizationConfiguration DescribeOrganizationConfiguration
- `iam`— Permite a los directores crear un rol vinculado a un servicio para Security Hub, CSPM y Security Hub, y obtener los roles, las políticas y las versiones de las políticas.
- `inspector`— Permite a los directores obtener información sobre el estado de la cuenta, habilitarla o deshabilitarla, delegar la administración administrativa y gestionar la configuración de la organización en Amazon Inspector. Esto incluye las acciones de la API: habilitar BatchGetAccountStatus, deshabilitar, EnableDelegatedAdminAccount, DisableDelegatedAdminAccount, ListDelegatedAdminAccounts UpdateOrganizationConfiguration, DescribeOrganizationConfiguration.
- `pricing`— Permite a los directores obtener una lista de precios Servicios de AWS y productos.
- `account`— Permite a los directores obtener información sobre las regiones de las cuentas para facilitar la administración de las regiones en Security Hub.

Para revisar los permisos de esta política, consulte AWSSecurityHubFullAccess en la Guía de referencia de la política administrada de AWS .

AWS política gestionada: AWSSecurityHubReadOnlyAccess

Puede asociar la política `AWSSecurityHubReadOnlyAccess` a las identidades de IAM.

Esta política otorga permisos de solo lectura que permiten a los usuarios ver información en el CSPM de Security Hub. Las entidades principales con esta política asociada no pueden realizar

ninguna actualización en el CSPM de Security Hub. Por ejemplo, las entidades principales con estos permisos pueden ver la lista de resultados asociados a su cuenta, pero no pueden cambiar el estado de un resultado. Pueden ver los resultados de las informaciones, pero no pueden crear ni configurar informaciones personalizadas. No pueden configurar controles ni integraciones de productos.

Detalles de los permisos

Esta política incluye los permisos siguientes:

- `securityhub`: permite a los usuarios realizar acciones que devuelven una lista de elementos o detalles sobre un elemento. Esto incluye las operaciones de la API que comienzan con `Get`, `List` o `Describe`.

Para revisar los permisos de esta política, consulte AWSSecurityHubReadOnlyAccess en la Guía de referencia de la política administrada de AWS .

AWS política gestionada: AWSSecurityHubOrganizationsAccess

Puede asociar la política `AWSSecurityHubOrganizationsAccess` a las identidades de IAM.

Esta política otorga permisos administrativos para habilitar y administrar Security Hub, Security Hub CSPM, Amazon GuardDuty y Amazon Inspector para una organización en. AWS Organizations Los permisos de esta política permiten a la cuenta de administración de la organización designar la cuenta de administrador delegado para Security Hub, Security Hub CSPM, Amazon y Amazon GuardDuty Inspector. También permiten que la cuenta de administrador delegado habilite las cuentas de la organización como cuentas de miembro.

Esta política solo proporciona permisos para. AWS Organizations La cuenta de administración de la organización y la cuenta de administrador delegado también requieren permisos para las acciones asociadas. Estos permisos se pueden conceder mediante la política administrada de `AWSSecurityHubFullAccess`.

La creación o actualización de una política de administrador delegado en una cuenta de administración requiere permisos adicionales que no se proporcionan en esta política. Para realizar estas acciones, se recomienda agregar permisos `organizations:PutResourcePolicy` o adjuntar la AWSOrganizationsFullAccess política.

Detalles de los permisos

Esta política incluye los permisos siguientes:

- `organizations:ListAccounts`: permite a las entidades principales recuperar la lista de cuentas que pertenecen a una organización.
- `organizations:DescribeOrganization`: permite a las entidades principales recuperar información sobre la organización.
- `organizations:ListRoots`: permite a las entidades principales enumerar la raíz de una organización.
- `organizations:ListDelegatedAdministrators`: permite a las entidades principales enumerar el administrador delegado de una organización.
- `organizations:ListAWSServiceAccessForOrganization`— Permite a los directores enumerar los Servicios de AWS que usa una organización.
- `organizations:ListOrganizationalUnitsForParent`: permite a las entidades principales enumerar las unidades organizativas (OU) secundarias de una unidad organizativa principal.
- `organizations:ListAccountsForParent`: permite a las entidades principales enumerar las cuentas secundarias de una unidad organizativa principal.
- `organizations:ListParents`: enumera las unidades raíz u organizativas (UO) que sirven como unidad principal inmediata de la UO secundaria o cuenta especificada.
- `organizations:DescribeAccount`: permite a las entidades principales recuperar información de sobre una cuenta en una organización.
- `organizations:DescribeOrganizationalUnit`: permite a las entidades principales recuperar información sobre una unidad organizativa de la organización.
- `organizations:ListPolicies`: recupera la lista de todas las políticas de una organización de un tipo especificado.
- `organizations:ListPoliciesForTarget`: enumera las políticas que están asociadas directamente con la raíz de destino, la unidad organizativa (UO) o la cuenta especificada.
- `organizations:ListTargetsForPolicy`: enumera todas las raíces, las unidades organizativas (UO) y las cuentas a las que está asociada la política especificada.
- `organizations:EnableAWSServiceAccess`: permite que las entidades principales habiliten la integración con Organizations.
- `organizations:RegisterDelegatedAdministrator`: permite que las entidades principales designen la cuenta de administrador delegado.
- `organizations:DeregisterDelegatedAdministrator`: permite que las entidades principales eliminen la cuenta de administrador delegado.
- `organizations:DescribePolicy`: recupera información sobre una política.

- `organizations:DescribeEffectivePolicy`: devuelve el contenido de la política en vigor para el tipo de política y la cuenta especificados.
- `organizations:CreatePolicy`— Crea una política de un tipo específico que se puede adjuntar a una cuenta raíz, a una unidad organizativa (OU) o a una AWS cuenta individual.
- `organizations:UpdatePolicy`: actualiza una política existente con un nombre nuevo, una descripción nueva o contenido nuevo.
- `organizations:DeletePolicy`: elimina la política especificada de la organización.
- `organizations:AttachPolicy`: asocia una política a una raíz, una unidad organizativa (UO) o una cuenta individual.
- `organizations:DetachPolicy`: desasocia una política de una raíz de destino, una unidad organizativa (UO) o una cuenta.
- `organizations:EnablePolicyType`: habilita un tipo de política en una raíz.
- `organizations:DisablePolicyType`: deshabilita un tipo de política organizacional en una raíz.
- `organizations:TagResource`: agrega uno o más etiquetas a un recurso especificado.
- `organizations:UntagResource`: elimina cualquier etiqueta con las claves especificadas de un recurso indicado.
- `organizations:ListTagsForResource`: enumera las etiquetas asociadas a un recurso especificado.
- `organizations:DescribeResourcePolicy`— Recupera información sobre una política de recursos.

Para revisar los permisos de esta política, consulte AWSSecurityHubOrganizationsAccess en la Guía de referencia de la política administrada de AWS .

AWS política gestionada: AWSSecurityHubServiceRolePolicy

No puede asociar `AWSSecurityHubServiceRolePolicy` a sus entidades IAM. Esta política está asociada a un rol vinculado al servicio que permite al CSPM de Security Hub realizar acciones en su nombre. Para obtener más información, consulte the section called “Service-linked roles”.

Esta política otorga permisos administrativos que permiten que el rol vinculado al servicio realice tareas como ejecutar comprobaciones de seguridad para los controles del CSPM de Security Hub.

Detalles de los permisos

Esta política incluye los permisos siguientes:

- `cloudtrail`— Recuperar información sobre las CloudTrail rutas.
- `cloudwatch`— Recupere CloudWatch las alarmas actuales y las métricas de estado de los conectores.
- `logs`— Recuperar los filtros CloudWatch métricos de los registros.
- `sns`: recuperar la lista de suscripciones a un tema de SNS.
- `config`— Recuperar información sobre los registradores, los recursos y AWS Config las reglas de configuración. Administre los grabadores de configuración vinculados al servicio CSPM de Security Hub y los grabadores de configuración vinculados a servicios de terceros. Cree y elimine AWS Config reglas y ejecute evaluaciones comparándolas con las reglas. Enumere los registradores de configuración y obtenga información sobre los conectores para respaldar las integraciones en la nube de terceros.
- `iam`— Recupere y genere informes de credenciales para las cuentas y cree el rol vinculado al servicio para. AWS Config
- `organizations`: recuperar información de cuentas y unidades organizativas (OU) de una organización.
- `securityhub`: recuperar información sobre la configuración del servicio, los estándares y los controles del CSPM de Security Hub.
- `tag`: recuperar información sobre las etiquetas de recursos.

Para revisar los permisos de esta política, consulte AWSSecurityHubServiceRolePolicy en la Guía de referencia de la política administrada de AWS .

Security Hub se actualiza a AWS políticas administradas

La siguiente tabla proporciona detalles sobre las actualizaciones de las políticas AWS administradas para AWS Security Hub y Security Hub CSPM desde que este servicio comenzó a rastrear estos cambios. Para recibir alertas automáticas sobre actualizaciones en las políticas, suscríbase al canal RSS en la página del Historial de documentos de Security Hub.

Cambio	Descripción	Fecha
AWSSecurityHubServiceRolePolicy: política actualizada	Security Hub CSPM actualizó la política para permitir la integración de terceros. La actualización agrega los siguientes permisos: administrar grabadores de configuración de terceros, enumerar los registradores de configuración, obtener información sobre los conectores y recuperar las métricas de estado de los conectores.	30 de junio de 2026
AWSSecurityHubServiceRolePolicy: política actualizada	El CSPM de Security Hub actualizó la política para agregar permisos para administrar los grabadores de configuración vinculados al servicio de Security Hub CSPM y crear el rol vinculado al servicio. AWS Config	29 de abril de 2026
AWSSecurityHubOrganizationsAccess: política actualizada	Security Hub actualizó la política para agregar permisos a fin de describir las políticas de recursos a fin de respaldar las funciones de Security Hub. Security Hub se encuentra en versión preliminar y está sujeto a cambios.	12 de noviembre de 2025
AWSSecurityHubFullAccess: política actualizada	Security Hub actualizó la política para agregar funciones relacionadas con la administración GuardDuty	17 de noviembre de 2025

Cambio	Descripción	Fecha
	, Amazon Inspector y la administración de cuentas a fin de respaldar las funciones de Security Hub. Security Hub se encuentra en versión preliminar y está sujeto a cambios.	
AWSSecurityHubOrganizationsAccess: actualización de una política actual	Security Hub agregó nuevos permisos a la política. Estos permisos permiten que la administración de la organización habilite y administre Security Hub y el CSPM de Security Hub para una organización.	17 de junio de 2025
AWSSecurityHubFullAccess: actualización de una política actual	El CSPM de Security Hub agregó nuevos permisos que permiten a las entidades principales crear un rol vinculado al servicio para Security Hub.	17 de junio de 2025
AWSSecurityHubFullAccess— Actualización de una política existente	Security Hub CSPM actualizó la política para obtener información sobre los precios Servicios de AWS y los productos.	24 de abril de 2024
AWSSecurityHubReadOnlyAccess— Actualización de una política existente	El CSPM de Security Hub actualizó esta política administrada mediante la adición de un campo `Sid`.	22 de febrero de 2024

Cambio	Descripción	Fecha
AWSSecurityHubFullAccess— Actualización de una política existente	Security Hub CSPM actualizó la política para poder determinar si Amazon GuardDuty y Amazon Inspector están habilitados en una cuenta. Esto ayuda a los clientes a recopilar información relacionada con la seguridad de múltiples fuentes. Servicios de AWS	16 de noviembre de 2023
AWSSecurityHubOrganizationsAccess— Actualización de una política existente	El CSPM de Security Hub ha actualizado la política para conceder permisos adicionales a fin de permitir acceso de solo lectura a las funcionalidades de administrador delegado de AWS Organizations . Esto incluye detalles como la raíz, las unidades organizativas (OU), las cuentas, la estructura de la organización y el acceso a servicios.	16 de noviembre de 2023
AWSSecurityHubServiceRolePolicy: actualización de una política actual	El CSPM de Security Hub ha agregado los permisos `BatchGetSecurityControls` , `DisassociateFromAdministratorAccount` y `UpdateSecurityControl` para leer y actualizar las propiedades de control de seguridad personalizables.	26 de noviembre de 2023

Cambio	Descripción	Fecha
AWSSecurityHubServiceRolePolicy: actualización de una política actual	El CSPM de Security Hub agregó el permiso `tag:GetResources` para leer las etiquetas de recursos relacionadas con los resultados.	7 de noviembre de 2023
AWSSecurityHubServiceRolePolicy: actualización de una política actual	El CSPM de Security Hub agregó el permiso `BatchGetStandardsControlAssociations` para obtener información sobre el estado de habilitación de un control en un estándar.	27 de septiembre de 2023
AWSSecurityHubServiceRolePolicy: actualización de una política actual	Security Hub CSPM agregó nuevos permisos para obtener AWS Organizations datos y leer y actualizar las configuraciones de Security Hub CSPM, incluidos los estándares y los controles.	20 de septiembre de 2023
AWSSecurityHubServiceRolePolicy: actualización de una política actual	El CSPM de Security Hub trasladó el permiso `config:DescribeConfigRuleEvaluationStatus` existente a una instrucción diferente en la política. El permiso `config:DescribeConfigRuleEvaluationStatus` se aplica ahora a todos los recursos.	17 de marzo de 2023

Cambio	Descripción	Fecha
AWSSecurityHubServiceRolePolicy: actualización de una política actual	El CSPM de Security Hub trasladó el permiso `config:PutEvaluations` existente a una instrucción diferente en la política. El permiso `config:PutEvaluations` se aplica ahora a todos los recursos.	14 de julio de 2021
AWSSecurityHubServiceRolePolicy: actualización de una política actual	El CSPM de Security Hub agregó un nuevo permiso para permitir que el rol vinculado a un servicio entregue resultados de evaluación a AWS Config.	29 de junio de 2021
AWSSecurityHubServiceRolePolicy— Se agregó a la lista de políticas administradas	Se agregó información sobre la política administrada AWSSecurityHubServiceRolePolicy, que utiliza la función vinculada al servicio CSPM de Security Hub.	11 de junio de 2021
AWSSecurityHubOrganizationsAccess— Nueva política	El CSPM de Security Hub agregó una nueva política que otorga los permisos necesarios para la integración del CSPM de Security Hub con Organizations.	15 de marzo de 2021
El CSPM de Security Hub comenzó a hacer un seguimiento de los cambios	Security Hub CSPM comenzó a rastrear los cambios en sus políticas AWS administradas.	15 de marzo de 2021

Resolución de problemas AWS Security Hub CSPM identidad y acceso

Utilice la siguiente información como ayuda para diagnosticar y solucionar los problemas comunes que pueden surgir al trabajar con AWS Security Hub CSPM un IAM.

Temas

- No estoy autorizado a realizar ninguna acción en Security Hub (CSPM).
- No estoy autorizado a ejecutar iam: PassRole
- Quiero tener acceso programático a Security Hub (CSPM).
- Soy administrador y quiero permitir que otras personas accedan a Security Hub CSPM
- Quiero permitir la entrada de personas ajenas a mi Cuenta de AWS para acceder a mis recursos de CSPM de Security Hub

No estoy autorizado a realizar ninguna acción en Security Hub (CSPM).

Si Consola de administración de AWS le indica que no está autorizado a realizar una acción, debe ponerse en contacto con su administrador para obtener ayuda. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

El siguiente ejemplo de error se produce cuando el usuario `mateojackson` intenta usar la consola para ver los detalles de una *`widget`* pero no tiene `securityhub:`*`GetWidget`* permisos.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 securityhub:GetWidget on resource: my-example-widget
```

En este caso, Mateo pide a su administrador que actualice sus políticas de forma que pueda obtener acceso al recurso *`my-example-widget`* mediante la acción `securityhub:`*`GetWidget`*.

No estoy autorizado a ejecutar iam: PassRole

Si recibe un error que indica que no tiene autorización para realizar la acción `iam:PassRole`, se deben actualizar las políticas a fin de permitirle pasar un rol a Security Hub.

Algunas Servicios de AWS permiten transferir una función existente a ese servicio en lugar de crear una nueva función de servicio o una función vinculada a un servicio. Para ello, debe tener permisos para transferir el rol al servicio.

En el siguiente ejemplo, el error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en Security Hub. Sin embargo, la acción requiere

que el servicio cuente con permisos que otorguen un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con su AWS administrador. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero tener acceso programático a Security Hub (CSPM).

Los usuarios necesitan acceso programático si quieren interactuar con AWS personas ajenas al. Consola de administración de AWS La forma de conceder el acceso programático depende del tipo de usuario al que acceda. AWS

Para conceder acceso programático a los usuarios, elija una de las siguientes opciones.

¿Qué usuario necesita acceso programático?	Para	Mediante
IAM	(Recomendado) Usa las credenciales de la consola como credenciales temporales para firmar las solicitudes programáticas a los AWS CLI AWS SDK o las API. AWS	Siga las instrucciones de la interfaz que desea utilizar: • Para ello AWS CLI, consulte Inicio de sesión para el desarrollo AWS local en la Guía del AWS Command Line Interface usuario. • Para AWS los SDK, consulte Iniciar sesión para el desarrollo AWS local en la Guía de referencia AWS sobre los SDK y las herramientas.

¿Qué usuario necesita acceso programático?	Para	Mediante
Identidad del personal (Usuarios administrados en el IAM Identity Center)	Usa credenciales temporales para firmar las solicitudes programáticas a los AWS SDK o AWS CLI las API. AWS	Siga las instrucciones de la interfaz que desea utilizar: • Para ello AWS CLI, consulte Configuración AWS CLI para su uso AWS IAM Identity Center en la Guía del AWS Command Line Interface usuario. • Para ver AWS los SDK, las herramientas y las AWS API, consulte la autenticación del IAM Identity Center en la guía de referencia de AWS SDK y herramientas.
IAM	Utilice credenciales temporales para firmar las solicitudes programáticas a los AWS SDK o las AWS CLI API. AWS	Siga las instrucciones que aparecen en la Guía del usuario de IAM, que se indican en la sección Uso de credenciales temporales con los AWS recursos.

¿Qué usuario necesita acceso programático?	Para	Mediante
IAM	(No recomendado) Utilice credenciales a largo plazo para firmar las solicitud es programáticas a los AWS CLI AWS SDK o las API. AWS	Siga las instrucciones de la interfaz que desea utilizar: • Para ello AWS CLI, consulte Autenticación mediante credenciales de usuario de IAM en la Guía del usuario. AWS Command Line Interface • Para ver AWS los SDK y las herramientas, consulte Autenticar con credencia les de larga duración en la Guía de referencia sobre los AWS SDK y las herramien tas. • Para obtener informaci ón AWS sobre las API, consulte Administrar las claves de acceso para los usuarios de IAM en la Guía del usuario de IAM.

Soy administrador y quiero permitir que otras personas accedan a Security Hub CSPM

Para dar acceso, agregue permisos a los usuarios, grupos o roles:

- Usuarios y grupos en: AWS IAM Identity Center

  Cree un conjunto de permisos. Siga las instrucciones de Creación de un conjunto de permisos en la Guía del usuario de AWS IAM Identity Center .

- Usuarios gestionados en IAM a través de un proveedor de identidades:

Cree un rol para la federación de identidades. Siga las instrucciones descritas en Creación de un rol para un proveedor de identidad de terceros (federación) en la Guía del usuario de IAM.

- Usuarios de IAM:
  - Cree un rol que el usuario pueda aceptar. Siga las instrucciones descritas en Creación de un rol para un usuario de IAM en la Guía del usuario de IAM.
  - (No recomendado) Adjunte una política directamente a un usuario o agregue un usuario a un grupo de usuarios. Siga las instrucciones descritas en Adición de permisos a un usuario (consola) de la Guía del usuario de IAM.

Quiero permitir la entrada de personas ajenas a mi Cuenta de AWS para acceder a mis recursos de CSPM de Security Hub

Se puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Se puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que admitan las políticas basadas en recursos o las listas de control de acceso (ACL), puede utilizar dichas políticas para conceder a las personas acceso a sus recursos.

Para obtener más información, consulte lo siguiente:

- Para obtener información sobre la compatibilidad de Security Hub con estas características, consulte Cómo funciona Security Hub con IAM.
- Para obtener información sobre cómo proporcionar acceso a los recursos de su propiedad Cuentas de AWS , consulte Cómo proporcionar acceso a un usuario de IAM en otro Cuenta de AWS que sea de su propiedad en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta Cómo proporcionar acceso a los que Cuentas de AWS pertenecen a terceros en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulte Proporcionar acceso a usuarios autenticados externamente (identidad federada) en la Guía del usuario de IAM.
- Para conocer sobre la diferencia entre las políticas basadas en roles y en recursos para el acceso entre cuentas, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Validación de conformidad para AWS Security Hub CSPM

Nuestra nueva experiencia AWS de registro no está diseñada para cargas de trabajo reguladas. Si utilizas nuestra nueva experiencia de AWS registro, pero quieres utilizarla AWS para cargas de trabajo reguladas, puedes suscribirte a una versión AWS (avanzada) o activar funciones avanzadas para tu entorno. AWS

Para saber si una Servicio de AWS está dentro del ámbito de un programa de cumplimiento específico, consulte Servicios de AWS la sección Alcance por programa de cumplimiento y seleccione el programa de cumplimiento que le interese. Para obtener información general, consulte Programas AWS de cumplimiento Programas .

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descargar informes en AWS Artifact .

Su responsabilidad de cumplimiento al usarlos Servicios de AWS viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y normativas aplicables. Para obtener más información sobre su responsabilidad de cumplimiento al usarlos Servicios de AWS, consulte la documentación AWS de seguridad.

Resiliencia en AWS Centro de seguridad

La infraestructura AWS global se basa Regiones de AWS en zonas de disponibilidad. Las regiones proporcionan varias zonas de disponibilidad físicamente independientes y aisladas que se encuentran conectadas mediante redes con un alto nivel de rendimiento y redundancia, además de baja demora. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre las zonas sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de uno o varios centros de datos.

Para obtener más información sobre Regiones de AWS las zonas de disponibilidad, consulte Infraestructura AWS global.

Seguridad de la infraestructura en AWS Security Hub CSPM

Como servicio gestionado, AWS Security Hub CSPM está protegido por la seguridad de red AWS global. Para obtener información sobre los servicios de AWS seguridad y cómo AWS protege la infraestructura, consulta AWS Cloud Security. Para diseñar su AWS entorno utilizando las mejores

prácticas de seguridad de la infraestructura, consulte Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Las llamadas a la API AWS publicadas se utilizan para acceder al CSPM de Security Hub a través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Conjuntos de cifrado con un secreto directo perfecto (PFS), como el DHE (efímero) o el ECDHE (efímero de curva elíptica Diffie-Hellman). Diffie-Hellman La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

AWS Security Hub CSPM y puntos finales de interfaz de VPC (AWS PrivateLink)

Puede establecer una conexión privada entre su VPC y AWS Security Hub CSPM mediante la creación de un punto final de VPC de interfaz. Los puntos finales de la interfaz funcionan con una tecnología que le permite acceder de forma privada a las API de CSPM de Security Hub sin una puerta de enlace a Internet, un dispositivo NAT, una conexión VPN o una conexión Direct Connect. AWS PrivateLink AWS Las instancias de su VPC no necesitan direcciones IP públicas para comunicarse con las API de CSPM de Security Hub. El tráfico entre su VPC y el CSPM de Security Hub no sale de la red de Amazon.

Cada punto de conexión de la interfaz está representado por una o más interfaces de red elásticas en las subredes. Para obtener más información, consulte Acceso y Servicio de AWS uso de un punto final de VPC desde una interfaz en la Guía de Amazon Virtual Private Cloud.

Consideraciones sobre los puntos de enlace de la VPC CSPM de Security Hub

Antes de configurar un punto final de VPC de interfaz para Security Hub CSPM, asegúrese de revisar los requisitos previos y otra información en la Guía de nube privada virtual de Amazon. https://docs.aws.amazon.com/vpc/latest/privatelink/what-is-privatelink.html

El CSPM de Security Hub permite realizar llamadas a todas sus acciones de API desde su VPC.

Creación de un punto final de VPC de interfaz para Security Hub CSPM

Puede crear un punto de enlace de VPC para el servicio CSPM de Security Hub mediante la consola de Amazon VPC o el (). AWS Command Line Interface AWS CLI Para obtener más información, consulte Cómo crear un punto de conexión de VPC en la Guía de Amazon Virtual Private Cloud.

Cree un punto de enlace de VPC para Security Hub CSPM con el siguiente nombre de servicio:

`com.amazonaws.region.securityhub`

¿Dónde *region* está el código de región del correspondiente? Región de AWS

Si habilita el DNS privado para el punto final, puede realizar solicitudes de API al CSPM de Security Hub utilizando su nombre de DNS predeterminado para la región, por ejemplo, `securityhub.us-east-1.amazonaws.com` para la región de EE. UU. Este (norte de Virginia).

Crear una política de terminales de VPC para Security Hub CSPM

Puede adjuntar una política de puntos finales a su punto de enlace de VPC que controle el acceso al CSPM de Security Hub. La política especifica la siguiente información:

- La entidad principal que puede realizar acciones.
- Las acciones que se pueden realizar.
- Los recursos en los que se pueden llevar a cabo las acciones.

Para obtener más información, consulte Control del acceso a puntos de conexión de VPC mediante políticas de punto de conexión en la Guía de Amazon Virtual Private Cloud.

Ejemplo: política de puntos de conexión de VPC para las acciones de CSPM de Security Hub

El siguiente es un ejemplo de una política de punto final para Security Hub CSPM. Cuando se adjunta a un punto final, esta política otorga acceso a las acciones de CSPM de Security Hub enumeradas a todos los responsables de todos los recursos.

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "securityhub:getFindings",
            "securityhub:getEnabledStandards",
            "securityhub:getInsights"
         ],
         "Resource":"*"
      }
   ]
```

```
}
```

Subredes compartidas

No puede crear, describir, modificar ni eliminar puntos de conexión de VPC en subredes que se compartan con usted. No obstante, puede usar los puntos de conexión de VPC en las subredes que se compartan con usted. Para obtener información sobre el uso compartido de VPC, consulte Uso compartido de las subredes de la VPC con otras cuentas en la Guía de Amazon Virtual Private Cloud.

Registrar llamadas a la API de Security Hub con CloudTrail

AWSEI CSPM de Security Hub está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en el Security Hub CSPM. CloudTrail captura las llamadas a la API para Security Hub CSPM como eventos. Las llamadas capturadas incluyen llamadas desde la consola del CSPM de Security Hub y llamadas de código a las operaciones de la API del CSPM de Security Hub. Si crea una ruta, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos para Security Hub CSPM. Si no configura una ruta, podrá ver los eventos más recientes en la CloudTrail consola, en el historial de eventos. Con la información que CloudTrail recopila, puede determinar la solicitud que se realizó a Security Hub CSPM, la dirección IP desde la que se realizó la solicitud, quién la hizo, cuándo se realizó y detalles adicionales.

Para obtener más información CloudTrail, incluido cómo configurarlo y habilitarlo, consulte la Guía del AWS CloudTrailusuario.

Información sobre CSPM de Security Hub en CloudTrail

CloudTrail está activado en tu cuenta Cuenta de AWS al crear la cuenta. Cuando se produce una actividad de eventos admitida en Security Hub CSPM, esa actividad se registra en un CloudTrail evento junto con otros eventos de AWS servicio en el historial de eventos. Se puede ver, buscar y descargar los últimos eventos de la cuenta de . Para obtener más información, consulte Visualización de eventos con el historial de CloudTrail eventos.

Para mantener un registro continuo de los eventos de la cuenta, incluidos los eventos del CSPM de Security Hub, cree un registro de seguimiento. Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando se crea un registro de seguimiento en la consola, este se aplica a todas las regiones de AWS. La ruta registra los eventos

de todas las regiones de la AWS partición y envía los archivos de registro al bucket de Amazon S3 que especifique. Además, puede configurar otros AWS servicios para analizar más a fondo los datos de eventos recopilados en los CloudTrail registros y actuar en función de ellos. Para más información, consulte los siguientes temas:

- Introducción a la creación de registros de seguimiento
- CloudTrail servicios e integraciones compatibles
- Configuración de las notificaciones de Amazon SNS para CloudTrail
- Recibir archivos de CloudTrail registro de varias regiones y recibir archivos de CloudTrail registro de varias cuentas

El CSPM de Security Hub admite el registro de todas las acciones de la API CSPM de Security Hub como eventos en los registros. CloudTrail Para ver una lista de las operaciones del CSPM de Security Hub, consulte la Referencia de la API del CSPM de Security Hub.

Cuando se registra la actividad de las siguientes acciones CloudTrail, el valor de se establece en. `responseElements` `null` Esto garantiza que la información confidencial no se incluya en CloudTrail los registros.

- `BatchImportFindings`
- `GetFindings`
- `GetInsights`
- `GetMembers`
- `UpdateFindings`

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con credenciales de usuario root o AWS Identity and Access Management (IAM)
- si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado
- Si la solicitud la realizó otro servicio AWS

Para obtener más información, consulte el elemento userIdentity de CloudTrail .

Ejemplo: entradas de archivos de registro del CSPM de Security Hub

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una solicitud única de cualquier fuente e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un registro ordenado de las llamadas a la API pública, por lo que no aparecen en ningún orden específico.

En el siguiente ejemplo, se muestra una entrada de CloudTrail registro que demuestra la `CreateInsight` acción. En este ejemplo, se crea una información llamada `Test Insight`. Se especifica el atributo `ResourceId` como el agregador Agrupar por y no se especifican filtros opcionales para esta información. Para obtener más información acerca de las informaciones, consulte Visualización de productos de información en el CSPM de Security Hub.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAJK6U5DS22IAVUI7BW",
        "arn": "arn:aws:iam::012345678901:user/TestUser",
        "accountId": "012345678901",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "TestUser"
    },
    "eventTime": "2018-11-25T01:02:18Z",
    "eventSource": "securityhub.amazonaws.com",
    "eventName": "CreateInsight",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.179",
    "userAgent": "aws-cli/1.11.76 Python/2.7.10 Darwin/17.7.0 botocore/1.5.39",
    "requestParameters": {
        "Filters": {},
        "ResultField": "ResourceId",
        "Name": "Test Insight"
    },
    "responseElements": {
        "InsightArn": "arn:aws:securityhub:us-west-2:0123456789010:insight/custom/
f4c4890b-ac6b-4c26-95f9-e62cc46f3055"
    },
    "requestID": "c0fffccd-f04d-11e8-93fc-ddcd14710066",
    "eventID": "3dabcebf-35b0-443f-a1a2-26e186ce23bf",
```

```
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "012345678901"
}
```

Etiquetado de recursos de Security Hub

Una etiqueta es una etiqueta opcional que puede definir y asignar a AWS los recursos, incluidos ciertos tipos de recursos CSPM de AWS Security Hub. Las etiquetas pueden ayudarle a identificar, clasificar y administrar recursos de distintas formas, como por finalidad, propietario, entorno u otros criterios. Por ejemplo, puede usar etiquetas para distinguir entre los recursos, identificar recursos que admiten ciertos requisitos de conformidad o flujos de trabajo, o asignar costos.

Puede agregar etiquetas a los siguientes tipos de recursos del CSPM de Security Hub:

- Reglas de automatización
- Políticas de configuración
- Recurso de `Hub`

Conceptos básicos del etiquetado

Un recurso puede tener hasta 50 etiquetas. Cada etiqueta está formada por una clave de etiqueta y un valor de etiqueta opcional, ambos definidos por el usuario. Un clave de etiqueta es una etiqueta general que actúa como una categoría para un valor de etiqueta más específicos. Un valor de etiqueta actúa como descriptor de una clave de etiqueta.

Por ejemplo, si crea reglas de automatización diferentes para entornos diferentes (un conjunto de reglas de automatización para las cuentas de prueba y otro para las cuentas de producción), puede asignar una clave de etiqueta `Environment` a esas reglas. El valor de etiqueta asociado puede ser `Test` para las reglas asociadas a cuentas de prueba y `Prod` para las reglas asociadas a las cuentas de producción y unidades organizativas.

Al definir y asignar etiquetas a los recursos de CSPM de AWS Security Hub, tenga en cuenta lo siguiente:

- Cada recurso puede tener un máximo de 50 etiquetas.
- Para cada recurso, cada clave de etiqueta debe ser única y solo puede tener un valor.
- Las claves y los valores de las etiquetas distinguen entre mayúsculas y minúsculas. Le recomendamos que defina una estrategia de uso de mayúsculas y minúsculas en las etiquetas e implemente esa estrategia sistemáticamente en todos los recursos.

- Una clave de etiqueta puede tener un máximo de 128 UTF-8 caracteres. El valor de una etiqueta puede tener un máximo de 256 UTF-8 caracteres. Los caracteres pueden ser letras, números, espacios o los siguientes símbolos: _ . : / = + - @
- El `aws:` prefijo está reservado para su uso por parte AWS de. No puede usarlo en las claves o valores de etiqueta que defina. Además, las claves o valores de etiqueta que utilizan este prefijo no se pueden cambiar ni quitar. Las etiquetas que usan este prefijo no cuentan para la cuota de 50 etiquetas por recurso.
- Las etiquetas que asigne estarán disponibles solo para usted Cuenta de AWS y solo en el lugar Región de AWS en el que las asigne.
- Si asigna etiquetas a un recurso mediante el CSPM de Security Hub, las etiquetas se aplican solo al recurso almacenado directamente en el CSPM de Security Hub en la Región de AWS correspondiente. No se aplican a ningún recurso de apoyo asociado que el CSPM de Security Hub cree, utilice o mantenga en su nombre en otros Servicios de AWS. Por ejemplo, si asigna etiquetas a una regla de automatización que actualiza los resultados relacionados con Amazon Simple Storage Service (Amazon S3), las etiquetas se aplican únicamente a la regla de automatización en el CSPM de Security Hub para la región especificada. No se aplican a sus buckets de S3. Para asignar también etiquetas a un recurso asociado, puede usar Grupos de recursos de AWS o el Servicio de AWS que almacena el recurso, por ejemplo, Amazon S3 para un bucket de S3. La asignación de etiquetas a los recursos asociados resulta útil a la hora de identificar los recursos de apoyo de los recursos del CSPM de Security Hub.
- Si elimina un recurso, también se eliminará cualquier etiqueta asignada a dicho recurso.

> **Important**
>
> No almacene datos confidenciales ni de otro tipo en etiquetas. Se puede acceder a las etiquetas desde muchas Servicios de AWS de ellas, incluidas. Administración de facturación y costos de AWS No se diseñaron para utilizarse con datos confidenciales.

Para agregar y administrar etiquetas para los recursos CSPM de Security Hub, puede usar la consola CSPM de Security Hub, la API CSPM de Security Hub o la API de etiquetado. Grupos de recursos de AWS Con el CSPM de Security Hub, puede agregar etiquetas a un recurso en el momento en que se crea. También puede añadir y gestionar etiquetas para los recursos individuales existentes. Con Resource Groups, puede añadir y administrar etiquetas de forma masiva para varios recursos existentes que abarquen variosServicios de AWS, incluido Security Hub CSPM.

Para obtener consejos y prácticas recomendadas adicionales sobre el etiquetado, consulte Etiquetar los recursos en la Guía del usuario sobre cómo etiquetar AWS los recursos. AWS

Uso de etiquetas en políticas de IAM

Una vez que comience a etiquetar los recursos, puede definir permisos de recursos basados en etiquetas en las políticas de AWS Identity and Access Management (IAM). Al utilizar las etiquetas de este modo, puede implementar un control pormenorizado sobre qué usuarios y roles de su empresa Cuenta de AWS tienen permiso para crear y etiquetar recursos, y qué usuarios y roles tienen permiso para añadir, editar y eliminar etiquetas de forma más general. Para controlar el acceso basándose función de etiquetas, puede utilizar claves de condición relacionadas con las etiquetas en el elemento Condition de las políticas de IAM.

Por ejemplo, puede crear una política de IAM que permita a un usuario tener acceso completo a todos los recursos del CSPM de AWS Security Hub si la etiqueta `Owner` del recurso especifica su nombre de usuario:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ModifyResourceIfOwner",
            "Effect": "Allow",
            "Action": "securityhub:*",
            "Resource": "*",
            "Condition": {
                "StringEqualsIgnoreCase": {"aws:ResourceTag/Owner":
 "${aws:username}"}
            }
        }
    ]
}
```

Si define los permisos de nivel de recurso basados en etiquetas, estos entrarán en vigor inmediatamente. Esto significa que sus recursos están más seguros en cuanto se crean y que puede empezar a aplicar el uso de etiquetas de nuevos recursos rápidamente. También puede usar

permisos de nivel de recurso para controlar las claves y valores de etiqueta que se pueden asociar a recursos nuevos y existentes. Para obtener más información, consulte Controlar el acceso a AWS los recursos mediante etiquetas en la Guía del usuario de IAM.

Adición de etiquetas a los recursos del CSPM de Security Hub

Una etiqueta es una etiqueta que puede definir y asignar a AWS los recursos, incluidos ciertos tipos de recursos CSPM de AWS Security Hub. Con las etiquetas, puede identificar, clasificar y administrar recursos de distintas formas, como por finalidad, propietario, entorno u otros criterios. Por ejemplo, puede usar etiquetas para aplicar políticas, asignar costos, distinguir entre las versiones de los recursos o identificar los recursos que respaldan determinados requisitos de conformidad o flujos de trabajo.

Puede agregar etiquetas a los siguientes tipos de recursos del CSPM de Security Hub:

- Reglas de automatización
- Políticas de configuración
- Recurso de Hub

Un recurso puede tener hasta 50 etiquetas. Cada etiqueta consta de una clave de etiqueta necesaria y un valor de etiqueta opcional. Una clave de etiqueta es una etiqueta general que actúa como una categoría para un valor de etiqueta más específico. Un valor de etiqueta actúa como descriptor de una clave de etiqueta. Para obtener más información acerca de las opciones y los requisitos de etiquetado, consulte Conceptos básicos del etiquetado.

Para agregar etiquetas a un recurso del CSPM de Security Hub, puede utilizar la consola o la API del CSPM de Security Hub. Sin embargo, la consola no permite agregar etiquetas al recurso de Hub.

Después de agregar las etiquetas, puede editarlas y cambiar la clave o el valor.

Para agregar o editar las etiquetas de varios recursos del CSPM de Security Hub al mismo tiempo, utilice las operaciones de etiquetado de la API de etiquetado de Grupos de recursos de AWS.

> **Important**
>
> La adición de etiquetas a un recurso puede afectar al acceso al recurso. Antes de añadir una etiqueta a un recurso, revise las políticas AWS Identity and Access Management (de IAM) que puedan utilizar etiquetas para controlar el acceso a los recursos.

Console

Para agregar etiquetas a un recurso del CSPM de Security Hub (consola)

Cuando crea una regla de automatización o una política de configuración, la consola del CSPM de Security Hub ofrece opciones para agregarle etiquetas. Puede proporcionar la clave y el valor de la etiqueta en la sección Etiquetas.

Security Hub CSPM API

Para agregar etiquetas a un recurso del CSPM de Security Hub (API)

Para crear un recurso y añadirle una o más etiquetas mediante programación, utilice la operación adecuada para el tipo de recurso que desee crear:

- Para crear una política de configuración y añadirle una o más etiquetas, invoca la CreateConfigurationPolicyAPI o, si la utilizasAWS CLI, ejecuta el comando create-configuration-policy.
- Para crear una regla de automatización y añadirle una o más etiquetas, invoca la CreateAutomationRuleAPI o, si la utilizas, ejecuta el AWS CLI comando create-automation-rule.
- Para habilitar el CSPM de Security Hub y añadir una o más etiquetas a su Hub recurso, invoque la EnableSecurityHubAPI o, si utiliza AWS Command Line Interface (AWS CLI), ejecute el comando enable-security-hub.

En su solicitud, use el parámetro `tags` para especificar la clave de etiqueta y el valor de etiqueta opcional de cada etiqueta que quiera añadir al recurso. El parámetro `tags` especifica una matriz de uno o varios objetos. Cada objeto especifica una clave de etiqueta y su valor de etiqueta asociado.

Para añadir una o más etiquetas a un recurso existente, utilice la TagResourceoperación de la API CSPM de Security Hub o, si la utilizaAWS CLI, ejecute el comando tag-resource. En su solicitud, especifique el nombre de recurso de Amazon (ARN) del recurso al que desea añadir una etiqueta. Use el parámetro `tags` para especificar la clave de etiqueta (`key`) y el valor de etiqueta opcional (`value`) de cada etiqueta que quiera añadir. El parámetro `tags` especifica una matriz de objetos, un objeto para cada clave de etiqueta y su valor de etiqueta asociado.

Por ejemplo, el siguiente AWS CLI comando agrega una clave de `Environment` etiqueta con un valor de `Prod` etiqueta a la política de configuración especificada. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

Ejemplo de comando de la CLI:

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags '{"Environment":"Prod"}'
```

Donde:

- `resource-arn` especifica el ARN de la política de configuración a la que se va a agregar una etiqueta.
- *`Environment`* es la clave de etiqueta de la etiqueta que se va a añadir a la regla.
- *`Prod`* es el valor de etiqueta para la clave de etiqueta especificada (*`Environment`*).

En el siguiente ejemplo, el comando agrega varias etiquetas a la política de configuración.

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags '{"Environment":"Prod", "CostCenter":"12345", "Owner":"jane-doe"}'
```

Para cada objeto de una matriz `tags`, se requieren los argumentos `key` y `value`. Sin embargo, el valor del argumento `value` puede ser una cadena vacía. Si no desea asociar un valor de etiqueta a una clave de etiqueta, no especifique un valor para el argumento `value`. Por ejemplo, el comando siguiente añade una clave de etiqueta `Owner` sin un valor de etiqueta asociado:

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags '{"Owner":""}'
```

Si la operación de etiquetado se realiza correctamente, el CSPM de Security Hub devuelve una respuesta HTTP 200 vacía. De lo contrario, el CSPM de Security Hub devuelve una respuesta HTTP 4 xx o 500 que indica el motivo del error de la operación.

Edición de etiquetas de recursos del CSPM de Security Hub

A medida que su entorno o sus requisitos cambien con el tiempo, puede evaluar las etiquetas existentes para los recursos de CSPM de AWS Security Hub y cambiarlas según sea necesario. Puede definir etiquetas y asignarlas a uno o más recursos de AWS, incluidos ciertos tipos de recursos de Macie. Cada etiqueta consta de una clave de etiqueta necesaria y un valor de etiqueta opcional. Una clave de etiqueta es una etiqueta general que actúa como una categoría para un valor de etiqueta más específico. Un valor de etiqueta actúa como descriptor de una clave de etiqueta.

Las etiquetas pueden ayudarle a identificar, clasificar y administrar recursos de distintas formas, como por finalidad, propietario, entorno u otros criterios. Por ejemplo, puede usar etiquetas para aplicar políticas, asignar costos, distinguir entre las versiones de los recursos o identificar los recursos que respaldan determinados requisitos de conformidad o flujos de trabajo.

Puede agregar etiquetas a los siguientes tipos de recursos del CSPM de Security Hub:

- Reglas de automatización
- Políticas de configuración
- Recurso de Hub

Para editar las claves o los valores de las etiquetas de un recurso del CSPM de Security Hub, puede utilizar la API del CSPM de Security Hub. Actualmente, la consola del CSPM de Security Hub no admite la edición de etiquetas.

> **Important**
>
> Modificar las etiquetas de un recurso puede afectar el acceso a él. Antes de editar la etiqueta de un recurso, revise las políticas AWS Identity and Access Management (de IAM) que puedan utilizar etiquetas para controlar el acceso a los recursos.

Security Hub CSPM API

Para editar las etiquetas de un recurso del CSPM de Security Hub (API)

Al editar una etiqueta de un recurso mediante programación, sobrescribe la etiqueta existente con valores nuevos. Por lo tanto, la mejor forma de editar una etiqueta depende de si desea editar

una clave de etiqueta, un valor de etiqueta o ambos. Para editar una clave de etiqueta, elimine la etiqueta actual y añada una nueva.

Para editar o eliminar solo el valor de etiqueta asociado a una clave de etiqueta, sobrescriba el valor existente mediante la TagResourceoperación de la API CSPM de Security Hub. Si utiliza la AWS CLI, ejecute el comando tag-resource. En su solicitud, especifique el nombre de recurso de Amazon (ARN) del recurso cuyo valor de etiqueta desea editar o eliminar.

Para editar el valor de una etiqueta, utilice el parámetro `tags` para especificar la clave de etiqueta cuyo valor de etiqueta desea cambiar. También debe especificar el nuevo valor de etiqueta para la clave. Por ejemplo, el siguiente AWS CLI comando cambia el valor de la etiqueta de `Prod` a `Test` para la clave de `Environment` etiqueta asignada a la regla de automatización especificada. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags '{"Environment":"Test"}'
```

Donde:

- `resource-arn` especifica el ARN de la política de configuración.
- *`Environment`* es la clave de etiqueta asociada al valor de etiqueta que se va a cambiar.
- *`Test`* es el nuevo valor de la etiqueta para la clave especificada (*`Environment`*).

Para eliminar un valor de etiqueta de una clave de etiqueta, no especifique un valor para el argumento `value` de la clave en el parámetro `tags`. Por ejemplo:

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags '{"Owner":""}'
```

Si la operación se realiza correctamente, el CSPM de Security Hub devuelve una respuesta HTTP 200 vacía. De lo contrario, el CSPM de Security Hub devuelve una respuesta HTTP 4 xx o 500 que indica el motivo del error de la operación.

Revisión de etiquetas de recursos del CSPM de Security Hub

Después de añadir o editar etiquetas para los recursos CSPM de AWS Security Hub, puede ver qué claves y valores de etiqueta tiene actualmente un recurso. Puede definir etiquetas y asignarlas a uno o más recursos de AWS, incluidos ciertos tipos de recursos de Macie. Cada etiqueta consta de una clave de etiqueta necesaria y un valor de etiqueta opcional. Una clave de etiqueta es una etiqueta general que actúa como una categoría para un valor de etiqueta más específico. Un valor de etiqueta actúa como descriptor de una clave de etiqueta.

Las etiquetas pueden ayudarle a identificar, clasificar y administrar recursos de distintas formas, como por finalidad, propietario, entorno u otros criterios. Por ejemplo, puede usar etiquetas para aplicar políticas, asignar costos, distinguir entre las versiones de los recursos o identificar los recursos que respaldan determinados requisitos de conformidad o flujos de trabajo.

Puede agregar etiquetas a los siguientes tipos de recursos del CSPM de Security Hub:

- Reglas de automatización
- Políticas de configuración
- Recurso de Hub

Puede revisar las etiquetas de una regla de automatización o una política de configuración del CSPM de Security Hub desde la consola o la API del CSPM de Security Hub. La consola no admite la revisión de las etiquetas del recurso de Hub. Mediante programación, puede revisar las etiquetas de cualquier recurso.

Para revisar las etiquetas de varios recursos del CSPM de Security Hub al mismo tiempo, utilice las operaciones de etiquetado de la API de etiquetado de Grupos de recursos de AWS.

Console

Para revisar las etiquetas de un recurso del CSPM de Security Hub (consola)

1. Con las credenciales del administrador CSPM de Security Hub, abra la consola CSPM AWS de Security Hub en. https://console.aws.amazon.com/securityhub/
2. Elija una de las siguientes opciones, en función del tipo de recurso al que desea añadir una etiqueta:
    - Para revisar las etiquetas de una regla de automatización, seleccione Automatizaciones en el panel de navegación. A continuación, seleccione una regla de automatización.

- Para revisar las etiquetas de una política de configuración, seleccione Configuración en el panel de navegación. A continuación, en la pestaña Políticas, seleccione la opción situada junto a una política de configuración. Se abrirá un panel lateral que mostrará el número de etiquetas asignadas a la política. Puede expandir el encabezado Etiquetas para ver las claves y los valores de las etiquetas.

La sección Etiquetas muestra una lista de todas las etiquetas asignadas actualmente al recurso.

Security Hub CSPM API

Para revisar las etiquetas de un recurso del CSPM de Security Hub (API)

Para recuperar y revisar las etiquetas de un recurso existente, invoque la API. ListTagsForResource En su solicitud, utilice el parámetro `resourceArn` para especificar el nombre de recurso de Amazon (ARN) del recurso.

Si utiliza elAWS CLI, ejecute el comando list-tags-for-resource y utilice el parámetro `resource-arn` para especificar el ARN del recurso. Por ejemplo:

```
$ aws securityhub list-tags-for-resource --resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Si la operación se completa correctamente, el CSPM de Security Hub devuelve una matriz de `tags`. Cada objeto de la matriz especifica una etiqueta (tanto la clave como el valor de la etiqueta) que está asignada actualmente al recurso. Por ejemplo:

```
{
    "tags": [
        {
            "key": "Environment",
            "value": "Prod"
        },
        {
            "key": "CostCenter",
            "value": "12345"
        },
        {
            "key": "Owner",
            "value": ""
        }
```

```
    ]
}
```

Donde `Environment`, `CostCenter` y `Owner` son las claves de etiqueta que se asignan al recurso. `Prod` es el valor de etiqueta asociado a la clave de etiqueta `Environment`. `12345` es el valor de etiqueta asociado a la clave de etiqueta `CostCenter`. La clave de etiqueta `Owner` no tiene un valor de etiqueta asociado.

Para recuperar una lista de todos los recursos CSPM de Security Hub que tienen etiquetas y todas las etiquetas asignadas a cada uno de esos recursos, utilice la GetResourcesoperación de la API de Grupos de recursos de AWS etiquetado. En su solicitud, defina el valor del parámetro `ResourceTypeFilters` como `securityhub`. Para elloAWS CLI, ejecute el comando get-resources y defina el valor del parámetro en. `resource-type-filters` `securityhub` Por ejemplo:

```
$ aws resourcegroupstaggingapi get-resources -\-resource-type-filters "securityhub"
```

Si la operación se lleva a cabo correctamente, Resource Groups devuelve una matriz `ResourceTagMappingList`. La matriz contiene un objeto por cada recurso del CSPM de Security Hub que tenga etiquetas. Cada objeto especifica el ARN de un recurso del CSPM de Security Hub, así como las claves y valores de etiqueta que se asignan al recurso.

Eliminación de etiquetas de recursos del CSPM de Security Hub

Si añade etiquetas a un recurso CSPM de AWS Security Hub, puede eliminar posteriormente una o más de ellas. Una etiqueta es una marca que define y asigna a los recursos de AWS, incluidos ciertos tipos de recursos del CSPM de Security Hub. Puede agregar, editar y eliminar etiquetas de los siguientes tipos de recursos del CSPM de Security Hub: reglas de automatización, políticas de configuración y recursos de Hub.

Para eliminar etiquetas de un recurso CSPM de AWS Security Hub individual, puede utilizar la API CSPM de Security Hub. Actualmente, la consola del CSPM de Security Hub no admite la eliminación de etiquetas.

Para eliminar las etiquetas de varios recursos del CSPM de Security Hub al mismo tiempo, utilice las operaciones de etiquetado de la API de etiquetado de Grupos de recursos de AWS.

> **Important**
>
> La eliminación de etiquetas de un recurso puede afectar al acceso al recurso. Antes de eliminar una etiqueta, revise las políticas AWS Identity and Access Management (de IAM) que puedan utilizarla para controlar el acceso a los recursos.

Security Hub CSPM API

Para eliminar etiquetas de un recurso del CSPM de Security Hub (API)

Para eliminar una o más etiquetas de un recurso mediante programación, utilice la UntagResourceoperación de la API CSPM de Security Hub. En su solicitud, utilice el parámetro `resourceArn` para especificar el nombre de recurso de Amazon (ARN) del recurso del que quiere eliminar una etiqueta. Utilice el parámetro `tagKeys` para especificar la clave de etiqueta de la etiqueta que se va a eliminar. Para eliminar varias etiquetas, añada el parámetro `tagKeys` y el argumento de cada etiqueta que desee eliminar, separados por un signo &, por ejemplo, `tagKeys=`*`key1`*`&tagKeys=`*`key2`*. Para quitar solo un valor de etiqueta específico (no una clave de etiqueta) de un recurso, edite la etiqueta en lugar de eliminarla.

Si utiliza el comando untag-resourceAWS CLI, ejecute el comando untag-resource para eliminar una o más etiquetas de un recurso. Para el parámetro `resource-arn`, especifique el ARN del recurso del que se va a eliminar una etiqueta. Utilice el parámetro `tag-keys` para especificar la clave de etiqueta de la etiqueta que se va a eliminar. Por ejemplo, el siguiente comando elimina la etiqueta `Environment` (tanto la clave como el valor de la etiqueta) de la política de configuración especificada:

```
$ aws securityhub untag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tag-keys Environment
```

Donde `resource-arn` especifica el ARN de la política de configuración de la que se va a eliminar una etiqueta y *`Environment`* es la clave de etiqueta de la etiqueta que se va a eliminar.

Para eliminar varias etiquetas de un recurso, agregue cada clave adicional como argumento para el parámetro `tag-keys`: Por ejemplo:

```
$ aws securityhub untag-resource \
```

```
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tag-keys Environment Owner
```

Si la operación se realiza correctamente, el CSPM de Security Hub devuelve una respuesta HTTP 200 vacía. De lo contrario, el CSPM de Security Hub devuelve una respuesta HTTP 4 xx o 500 que indica el motivo del error de la operación.

Cuotas para Security Hub

Cuenta de AWSTiene determinadas cuotas predeterminadas, anteriormente denominadas límites, para cada una de ellas. Servicio de AWS Estas cuotas establecen el número máximo de recursos u operaciones de servicio que puede haber en su cuenta. En este tema se incluye un enlace a las cuotas que se aplican a los recursos y las operaciones de AWS Security Hub para su cuenta. A menos que se indique lo contrario, cada cuota se aplica a su cuenta en cada Región de AWS.

Algunas cuotas pueden aumentarse, mientras que otras no. Para solicitar el aumento de una cuota, use la consola de Service Quotas. Para saber cómo solicitar el aumento de una cuota, consulte Solicitud de aumento de cuota en la Guía del usuario de Service Quotas. Si no hay una cuota disponible en la consola de Service Quotas, utilice el formulario de aumento del límite de servicio de la AWS Support Center Console para solicitar un aumento de la cuota.

Cuotas máximas

Para obtener una lista de las cuotas que se aplican a los recursos de AWS Security Hub, consulte Puntos de conexión y cuotas de AWS Security Hub en la Referencia general de AWS.

Cuotas de tarifas

Para obtener una lista de las cuotas que se aplican a las operaciones de la API de AWS Security Hub, consulte Referencia de la API de AWS Security Hub.

Si configuró la agregación entre regiones en el CSPM de Security Hub, una llamada a `BatchImportFindings` y `BatchUpdateFindings` afecta a las regiones vinculadas y la región de agregación. La operación `GetFindings` recupera resultados de las regiones vinculadas y la región de agregación. Sin embargo, las `UpdateStandardsControl` operaciones `BatchEnableStandards` y sí lo son Region-specific.

Historial de documentos del AWS Security Hub Guía del usuario de

En la siguiente tabla se describen los cambios importantes en la documentación desde la última versión de AWS Security Hub y Security Hub CSPM. En el caso de las versiones de los nuevos controles CSPM de Security Hub, la fecha especifica cuándo los controles comienzan a estar disponibles como compatibles. Regiones de AWS Los controles pueden tardar entre una y dos semanas en estar disponibles en todas las regiones admitidas. Para obtener más información sobre los cambios relevantes en los controles existentes, consulte Registro de cambios de los controles del CSPM de Security Hub.

Para recibir notificaciones sobre las actualizaciones de la Guía del usuario de AWS Security Hub, se puede suscribir a una fuente RSS.

Cambio	Descripción	Fecha
Se actualizaron los detalles de los hallazgos informativos del escaneo de red	Se agregó información sobre los hallazgos informativos que genera Network Scanning.	3 de septiembre de 2026
Lista actualizada de puertos de escaneo de red	Se agregó la lista de puertos que actualmente admite Network Scanning.	18 de agosto de 2026
Controles de seguridad actualizados	El CSPM de Security Hub eliminó el EFS.6 control del estándar AWS Fundation al Security Best Practices (FSBP). Este control sigue disponible en los estándares NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2 y PCI DSS v4.0.1.	3 de agosto de 2026
Documentación mejorada sobre la habilitación de Security Hub	Se ha mejorado la guía de la página Administración de la configuración de las cuentas	7 de julio de 2026

	de los miembros en una AWS organización.	
Se agregó la documentación sobre la función de escaneo de red	Se agregó documentación para la función de escaneo de red de Security Hub	7 de julio de 2026
Inventario de IA	Se agregó el inventario de IA, que proporciona una vista unificada de los recursos de inteligencia artificial (IA) y aprendizaje automático (ML) gestionados y autohospe dados en todo su AWS entorno. Para obtener más información, consulta el inventario de IA en AWS Security Hub.	7 de julio de 2026
Actualizaciones de una política gestionada — `AWSSecurityHubV2ServiceRolePolicy`	Security Hub actualizó la política AWS gestionada denominada`AWSSecurityHubV2ServiceRolePolicy`. Las actualizaciones agregaron permisos para permitir las integraciones de terceros, incluida la administración de grabadores de configuración de terceros, la creación y administración de conectores y la obtención de tokens de identidad web para la federación.	30 de junio de 2026

Actualizaciones de una política gestionada — `AWSSecurityHubServiceRolePolicy`	Security Hub CSPM actualizó la política AWS administrada denominada. `AWSSecurityHubServiceRolePolicy` Las actualizaciones agregaron permisos para admitir integraciones de terceros. Estos incluyen la administración de grabadores de configuración de terceros y la recuperación de las métricas de estado de los conectores.	30 de junio de 2026
Nuevo estándar de seguridad	Security Hub CSPM publicó el estándar de mejores prácticas de seguridad de IA. Este estándar proporciona un conjunto de controles seleccionados que detectan cuándo los recursos de IA implementados no se alinean con las mejores prácticas de seguridad.	30 de junio de 2026
Nuevos controles de seguridad	Security Hub CSPM lanzó ocho nuevos controles para el estándar de mejores prácticas de seguridad de la IA. Los nuevos controles son: Bedrock.1, BedrockAgentCore.7, SageMaker.20, SageMaker.21, SageMaker.22 SageMaker.23 SageMaker.24, y. SageMaker.25	30 de junio de 2026

Actualizaciones sobre el tipo de rasgo de impacto y la gravedad de los hallazgos de exposición	Se agregó el tipo de rasgo de impacto a los hallazgos de exposición. El impacto describe el radio potencial de explosión si un recurso se ve comprometido, según los permisos efectivos de los AWS Identity and Access Management directores asociados. Se actualizó el cálculo de la gravedad para utilizar una matriz de probabili dad y riesgo de impacto alineada con las directrices del NIST. Se agregó una guía de corrección por recurso para las características de las rutas de acceso afectadas.	23 de junio de 2026
Actualizaciones a los estándares y controles de seguridad	Retiramos los RDS.18 controles ECS.1 y los eliminamos de todos los estándares aplicables. Desde que se retiró la EC2-Classic red de Amazon, las instancia s de Amazon Relational Database Service (Amazon RDS) ya no se pueden implementar fuera de una VPC.	5 de junio de 2026

Actualizaciones de la grabadora vinculada al servicio CSPM	Se agregó información relacionada con el nuevo grabador de configuración vinculado a un servicio que permite al CSPM de Security Hub realizar comprobaciones de control de seguridad en función de la información de configuración de los recursos.	27 de mayo de 2026
Hallazgos de acceso no utilizados	Security Hub agregó una funcionalidad para generar y mostrar los hallazgos de acceso no utilizados de IAM Access Analyzer Comprender los hallazgos de acceso no utilizados en Security Hub	19 de mayo de 2026

Nuevos controles de seguridad	Security Hub CSPM lanzó cinco controles nuevos. Algunos de los controles son compatibles con el estándar AWS Fundational Security Best Practices (FSBP). La mayoría de los controles cumplen con los requisitos del NIST SP 800-53 Rev. 5. • Para el estándar AWS FSBP, los identificadores de los controles aplicables son: y. BedrockAgentCore.5 BedrockAgentCore.6 • Para el NIST SP 800-53 Rev. 5, los ID de los controles aplicables son:, y. BedrockAgentCore.3 BedrockAgentCore.4 SageMaker.18	15 de mayo de 2026
Actualizaciones de una política gestionada — `AWSSecurityHubServiceRolePolicy`	Security Hub CSPM actualizó la política AWS administrada denominada. `AWSSecurityHubServiceRolePolicy` Las actualizaciones agregaron permisos para administrar los grabadores de configuración vinculados al servicio CSPM de Security Hub y crear el rol vinculado al servicio. AWS Config	29 de abril de 2026

Nuevos controles de seguridad	Security Hub CSPM lanzó cuatro nuevos controles para el estándar AWS Fundational Security Best Practices (FSBP). Los nuevos controles son: BedrockAgentCore.1,, y. BedrockAgentCore.2 RDS.51 SageMaker.19	22 de abril de 2026
Nuevos controles de seguridad	Security Hub CSPM lanzó cinco nuevos controles para el estándar AWS Fundational Security Best Practices (FSBP). Los nuevos controles son: APIGateway.11,,, y EC2.183. EKS.9 SageMaker.16 SageMaker.17	7 de abril de 2026
Actualizaciones a los estándares y controles de seguridad	Retiramos los AppSync.6 controles AppSync.1 y los eliminamos del estándar AWS Fundational Security Best Practices (FSBP). AWS AppSync ahora proporciona el cifrado predeterminado en todas las cachés de API actuales y futuras.	9 de marzo de 2026
Actualizaciones a los estándares y controles de seguridad	Retiramos el ECS.1 control y lo eliminamos del estándar AWS Fundational Security Best Practices (FSBP) y del estándar NIST SP 800-53 Rev. 5.	4 de marzo de 2026

Nuevos controles de seguridad	Security Hub CSPM lanzó once nuevos controles para el estándar AWS Fundation al Security Best Practices (FSBP). Los nuevos controles son: APIGateway.10,, ELB.21, ELB.22 y. RDS.50 SageMaker.9 SageMaker.10 SageMaker.11 SageMaker .12 SageMaker.13 SageMaker.14 SageMaker .15	16 de febrero de 2026
Actualizaciones a los estándares y controles de seguridad	Retiramos el MQ.3 control y lo eliminamos de todos los estándares aplicables. Retiramos el control debido a los requisitos de Amazon MQ para las actualizaciones automáticas de versiones secundarias. Anteriormente, este control se aplicaba al estándar AWS Fundational Security Best Practices (FSBP), al estándar NIST SP 800-53 Rev. 5 y al estándar PCI DSS v4.0.1. https://docs.aws.amazon.com/securityhub/latest/userguide/pci-standard.html	12 de enero de 2026

Actualizaciones de la documentación del estimador de costos	Se agregaron detalles a la documentación del estimador de costos de Security Hub sobre cómo conceder el acceso entre cuentas para hacer estimaciones en cuentas distintas de la cuenta de administración.	12 de enero de 2026
Nuevos controles de seguridad	Security Hub CSPM lanzó cinco nuevos controles para el estándar AWS Fundation al Security Best Practices (FSBP). Los nuevos controles son: CloudFormation.4,,, y CloudFront.17. ECS.19 ECS.20 ECS.21	6 de enero de 2026
Actualizaciones a los estándares y controles de seguridad	Debido a los requisitos de Amazon MQ para las actualizaciones automátic as de versiones menores, tenemos previsto retirar el MQ.3 control de todas las normas aplicables el 12 de enero de 2026. Actualmente, el control se aplica al estándar AWS Fundational Security Best Practices (FSBP), al estándar NIST SP 800-53 Rev. 5 y al estándar PCI DSS v4.0.1. https://docs.aws.amazon.com/securityhub/latest/userguide/pci-standard.html	12 de diciembre de 2025

Contenido actualizado para Service-Managed Standard: AWS Control Tower	Contenido actualizado para la versión Service-Managed estándar: AWS Control Tower para proporcionar una guía mejorada para crear, ver y deshabilitar los controles en la versión estándar. AWS Control Tower	8 de diciembre de 2025
Nuevos controles de seguridad	Security Hub CSPM lanzó siete nuevos controles para el estándar AWS Fundation al Security Best Practices (FSBP). Los nuevos controles son: Cognito.4,,, Cognito.5 Cognito.6, EC2.182 y. CloudFormation.3 ECS.18 SES.3	8 de diciembre de 2025
Contenido actualizado para la disponibilidad general de Security Hub	Se agregó contenido para respaldar la versión de disponibilidad general de AWS Security Hub	2 de diciembre de 2025
Se actualizó el contenido de Security Hub	Se agregó contenido para https://docs.aws.amazon.com/securityhub/latest/userguide/dashboard-v2.html#dashboard-v2-widgets.html Tendencias y Agregación Regional. Estos cambios son compatibles con la versión preliminar de Security Hub.	21 de noviembre de 2025

Actualizaciones de una política gestionada — `AWSSecurityHubV2ServiceRolePolicy`	Security Hub actualizó la política AWS gestionada denominada`AWSSecurityHubV2ServiceRolePolicy`. Las actualizaciones agregaron capacidades de medición para Amazon Elastic Container Registry y Amazon AWS Lambda CloudWatch, y AWS Identity and Access Management para respaldar las funciones de Security Hub. Las actualizaciones también agregaron soporte para AWS Config grabadoras globales. Estos cambios son compatibles con la versión preliminar de Security Hub.	17 de noviembre de 2025
Actualizaciones de una política gestionada — `AWSSecurityHubOrganizationsAccess`	Security Hub actualizó la política AWS gestionada denominada`AWSSecurityHubOrganizationsAccess`. Las actualizaciones agregaron permisos para describir las políticas de recursos que admiten las funciones de Security Hub. Estos cambios son compatibles con la versión preliminar de Security Hub.	17 de noviembre de 2025

Actualizaciones de una política gestionada — `AWSSecurityHubFullAccess`	Security Hub actualizó la política AWS gestionada denominada`AWSSecurityHubFullAccess`. Las actualizaciones agregaron funciones relacionadas con la administración GuardDuty, Amazon Inspector y la administración de cuentas para respaldar las funciones de Security Hub. Estos cambios son compatibles con la versión preliminar de Security Hub.	17 de noviembre de 2025
Actualizaciones a los controles de seguridad	Hemos cambiado el nivel de severidad de 10 controles de CSPM de Security Hub: CloudFront.7 CloudTrail.5, ELB.7,, GuardDuty.7, MQ.3, Opensearch.10, RDS.7, ServiceCatalog.1 SNS.4, y. SQS.3 Para ver un desglose de los cambios, consulte el registro de cambios de los controles de CSPM de Security Hub.	13 de noviembre de 2025

Nuevos controles de seguridad	La solución de Administración de la posición de seguridad en la nube (CSPM) de Security Hub lanzó seis controles nuevos para el estándar Prácticas recomendadas de seguridad básica de AWS (FSBP). Los nuevos controles son: Cognito.3 DMS.13, EC2.181, RDS.43, RDS.47, y RDS.48.	28 de octubre de 2025
Nuevo estándar de seguridad	Security Hub CSPM ahora ofrece un estándar de seguridad que se alinea con CIS AWS Foundations Benchmark v5.0.0. Este nuevo estándar incluye 40 controles de seguridad existentes. Los controles realizan comprobaciones automatizadas que evalúan el cumplimiento de ciertos recursos con un subconjunto de los requisitos definidos en el marco.	16 de octubre de 2025
Nueva integración de terceros	Elastic es una nueva integración de terceros con la capacidad de recibir resultados del CSPM de Security Hub.	3 de octubre de 2025

Actualizaciones a los estándares y controles de seguridad	Retiramos los RedshiftS erverless.7 controles Redshift. 9 y los eliminamos de todos los estándares aplicables. Retiramos estos controles debido a las limitaciones inherentes a Amazon Redshift que impedían la correcció n efectiva de los resultados `FAILED` de los controles. Anteriormente, estos controles se aplicaban al estándar Prácticas recomendadas de seguridad básica de AWS (FSBP), así como al estándar NIST SP 800-53 Rev. 5. El Redshift.9 control también se aplicó al estándar de AWS Control Tower gestión de servicios.	24 de septiembre de 2025
Disponibilidad regional	El CSPM de Security Hub ya está disponible en la región de Asia-Pacífico (Nueva Zelanda). Para obtener una lista completa de los Regiones de AWS lugares en los que Security Hub CSPM está disponible actualmente, consulte los puntos finales y las cuotas de AWS Security Hub en. Referencia general de AWS	19 de septiembre de 2025

Nuevos controles de seguridad	Security Hub CSPM lanzó dos nuevos controles para el estándar AWS Fundation al Security Best Practices (FSBP): y. CloudFront.16 RDS.46	3 de septiembre de 2025
Disponibilidad regional	El estándar de etiquetado de recursos de AWS ya se encuentra disponible en las regiones de Asia-Pacífico (Tailandia) y México (centro).	29 de agosto de 2025
Actualizaciones a los estándares y controles de seguridad	Debido a las limitaciones de Amazon Redshift, tenemos previsto retirar los RedshiftS erverless.7 controles Redshift. 9 y de todas las normas aplicables el 15 de septiembr e de 2025. Actualmente, estos controles se aplican al estándar Prácticas recomenda das de seguridad básica de AWS (FSBP), así como al estándar NIST SP 800-53 Rev. 5. El Redshift.9 control también se aplica al estándar de gestión de AWS Control Tower servicios.	15 de agosto de 2025

Nuevo objeto de detalles de recursos en el Formato de resultados de seguridad (ASFF)	El Formato de resultados de seguridad (ASFF) de AWS ahora incluye un objeto de recurso `CodeRepository` . Este objeto proporciona detalles sobre un repositorio de código externo al que conectaste a AWS los recursos y configuraste Amazon Inspector para detectar vulnerabilidades.	1 de agosto de 2025
Disponibilidad regional	El CSPM de Security Hub ya está disponible en la región de Asia-Pacífico (Taipéi). Para obtener una lista de todas las Regiones de AWS en las que el CSPM de Security Hub se encuentra actualmente disponible, consulte Puntos de conexión y cuotas de AWS Security Hub en la Referencia general de AWS.	23 de julio de 2025
Nueva integración de terceros	Dynatrace es una nueva integración de terceros con la capacidad de recibir resultados del CSPM de Security Hub.	18 de julio de 2025

Nuevos controles de seguridad	El CSPM de Security Hub lanzó 13 controles nuevos. La mayoría de los controles admiten el estándar de Prácticas recomendadas de seguridad básica (FSBP) de AWS. Algunos de los controles admiten los requisitos estipulados en NIST SP 800-53 Rev. 5 • Para el estándar AWS FSBP, los ID de los controles aplicables son: CloudFront.15, Cognito.2, EC2.180, ELB.18, MSK.4,, MSK.5, MSK.6, RDS.45, Redshift.18 S3.25 SSM.6, y. SSM.7 • Para el NIST SP 800-53 Rev. 5, los ID de los controles aplicables son: y. Lambda.7 RDS.45	15 de julio de 2025

Actualizaciones a la generación de resultados de control	Para facilitar el seguimiento de los cambios en el cumplimiento, el CSPM de Security Hub ahora actualiza los resultados de control existentes en lugar de generar resultados nuevos, cuando hay un cambio en el estado de cumplimiento de los recursos individuales. Esto significa que puede utilizar los datos de resultados individuales para hacer un seguimiento de cómo cambia el cumplimiento de determinados recursos con respecto a controles específicos.	3 de julio de 2025
Actualizaciones a los estándares y controles de seguridad	Hemos eliminado el IAM.13 control del estándar PCI DSS v4.0.1. También eliminamos el IAM.17 control del estándar NIST SP 800-171, revisión 2. Los estándares no exigen de forma explícita las comprobaciones que realizan estos controles. También actualizamos los detalles de los requisitos relacionados con estas normas para ciertos controles que comprueban las políticas de contraseñas de IAM: IAM.7, y de forma exhaustiva. IAM.10 IAM.17	30 de junio de 2025

Actualizaciones a la retención de resultados	El CSPM de Security Hub ahora almacena los resultados archivados durante 30 días en lugar de 90, lo cual puede reducir el volumen de resultados innecesarios. Para una retención a largo plazo, puedes exportar los resultados a un bucket de S3 mediante una acción personalizada con una regla de Amazon. EventBridge	20 de junio de 2025
Actualizaciones de las políticas administradas existentes	El CSPM de Security Hub agregó un nuevo permiso a la política administrada de AWS denominada `AWSSecurityHubOrganizationsAccess`. El permiso permite a la administración de la organización habilitar y administrar tanto Security Hub como el CSPM de Security Hub dentro de una organización. El CSPM de Security Hub agregó un nuevo permiso a la política administrada de AWS denominada `AWSSecurityHubFullAccess`. El permiso permite que las entidades principales creen un rol vinculado al servicio para Security Hub.	18 de junio de 2025

Versión preliminar pública y una nueva política administrada para Security Hub	Versión preliminar pública de AWS Security Hub y de la guía del usuario AWS de Security Hub. Esta versión incluye una nueva política administrada de AWS, `AWSSecurityHubV2ServiceRolePolicy` . La política permite a Security Hub administrar AWS Config las reglas y los recursos de Security Hub en la organización del cliente y en nombre del cliente. Security Hub se encuentra en versión preliminar y está sujeto a cambios.	17 de junio de 2025
Actualizaciones a los estándares y controles de seguridad	Hemos eliminado el IAM.10 control del estándar PCI DSS v4.0.1. Este control verifica si las políticas de contraseñas de las cuentas de usuario de IAM cumplen los requisitos mínimos, incluida una longitud mínima de 7 caracteres. La versión 4.0.1 de PCI DSS ahora requiere que las contraseñas tengan un mínimo de 8 caracteres. El IAM.10 control sigue aplicándose al estándar PCI DSS v3.2.1, que tiene diferentes requisitos de contraseña.	30 de mayo de 2025

Nuevo estándar de seguridad	El CSPM de Security Hub ahora proporciona un estándar de seguridad alineado con la segunda revisión del marco de ciberseguridad y cumplimiento NIST SP 800-171. Este nuevo estándar incluye más de 60 controles de seguridad existentes. Los controles realizan comprobaciones automatizadas para evaluar el cumplimiento de ciertos recursos Servicios de AWS y determinados recursos con respecto a un subconjunto de los requisitos definidos en el marco.	29 de mayo de 2025
Actualizaciones a los controles de seguridad	Security Hub CSPM anuló por completo la versión del siguiente control Regiones de AWS: [RDS.46] Las instancias de bases de datos de RDS no deben implementarse en subredes públicas con rutas a puertas de enlace a Internet. Anteriormente, este control era compatible con el estándar AWS Fundational Security Best Practices (FSBP).	8 de mayo de 2025

Nuevos controles de seguridad	El CSPM de Security Hub lanzó 9 controles nuevos. La mayoría de los controles admiten el estándar de Prácticas recomendadas de seguridad básica (FSBP) de AWS. Algunos de los controles admiten los requisitos estipulados en NIST SP 800-53 Rev. 5 • Para el estándar AWS FSBP, los ID de los controles aplicables son: DocumentDB.6,,, RDS.44 RedshiftServerless.2 RedshiftServerless.3 RedshiftServerless.5 RedshiftServerless.6, y RedshiftServerless.7 (retirados posteriormente). • En el caso del NIST SP 800-53 Rev. 5, los identificadores de los controles aplicables son: CloudTrail.10 RedshiftServerless.4, y RedshiftServerless.7 (retirados posteriormente).	7 de mayo de 2025

Nuevos controles de seguridad	El CSPM de Security Hub lanzó 24 controles nuevos. La mayoría de los controles admiten el estándar de Prácticas recomendadas de seguridad básica (FSBP) de AWS o el de etiquetado de recursos de AWS. Algunos de los controles admiten los requisitos estipulados en NIST SP 800-53 Rev. 5 • Para el estándar AWS FSBP, los ID de los controles aplicables son: EC2.173,, y. RDS.41 RDS.42 SageMaker.8 • Para el estándar de etiquetado de AWS recursos, los ID de los controles aplicables son: Amplify.1 Amplify.2 , Batch.4, DataSync. 2, EC2.174, EC2.175, EC2.176, EC2.177, EC2.178, EC2.179, Redshift.17 SageMaker .6 SageMaker.7 SSM.5, Transfer.4,, Transfer.5 Transfer.6, y. Transfer.7 • Para el NIST SP 800-53 Rev. 5, los identificadores de los controles aplicables son: y. ECS.17 RDS.42	16 de abril de 2025

Nuevos controles de seguridad	El CSPM de Security Hub lanzó cuatro nuevos controles para el estándar de Prácticas recomendadas de seguridad básica de AWS. Los controles son: • the section called “[FSx.3] FSx para sistemas de archivos OpenZFS debe configurarse para su implementación Multi-AZ” • the section called “[FSx.4] FSx para sistemas de archivos NetApp ONTAP debe configurarse para su implementación Multi-AZ” • the section called “[FSx.5] Los sistemas de archivos FSx for Windows File Server deben configurarse para Multi-AZ su implementación” • the section called “[RedshiftServerless.1] Los grupos de trabajo sin servidor de Amazon Redshift deberían utilizar un enrutamiento de VPC mejorado”	18 de marzo de 2025

Actualizaciones a los estándares y controles de seguridad	Eliminamos el control de RDS.18 seguridad (posteriormente retirado) del estándar AWS Fundational Security Best Practices y realizamos comprobaciones automatizadas para cumplir los requisitos del SP 800-53 Rev. 5 del NIST. Desde que se retiró la EC2-Classic red de Amazon, las instancias de Amazon Relational Database Service (Amazon RDS) ya no se pueden implementar fuera de una VPC.	7 de marzo de 2025
Actualizaciones a los resultados de control	El CSPM de Security Hub ahora genera `WARNING` los resultados de un control habilitado si el registro de recursos no está activado AWS Config para el tipo de recurso que el control comprueba. Esto resulta útil a la hora de identificar y abordar posibles brechas de configuración en las comprobaciones de controles de seguridad.	25 de febrero de 2025

Nuevos controles de seguridad	El CSPM de Security Hub lanzó 11 controles nuevos. Los controles son: • the section called “[Connect .2] Las instancias de Connect Customer deben tener el CloudWatch registro habilitado” • the section called “[ECR.5] Los repositorios de ECR deben estar cifrados y ser gestionados por el cliente AWS KMS keys” • the section called “[ELB.17] Los balanceadores de cargas de aplicaciones y redes con oyentes deben usar las políticas de seguridad recomendadas” • the section called “[Glue.4] AWS GlueLos trabajos de Spark deberían ejecutarse en versiones compatibles deAWS Glue” • the section called “[GuardDuty.11] La monitorización del GuardDuty tiempo de ejecución debe estar habilitada” • the section called “[GuardDuty.12] La monitorización del tiempo de ejecución de GuardDuty ECS debe estar habilitada”	24 de febrero de 2025

- the section called “[GuardDuty.13] La monitorización del tiempo de ejecución de GuardDuty EC2 debe estar habilitada”
- the section called “[Network Firewall.10] Los firewalls de Network Firewall deben tener habilitada la protección contra cambios de subred”
- the section called “[RDS.40] Las instancias de base de datos de RDS para SQL Server deben publicar los registros en Logs CloudWatch”
- the section called “[SQS.3] Las políticas de acceso a las colas de SQS no deberían permitir el acceso público”
- the section called “[Transfer.3] Los conectores Transfer Family deben tener habilitado el registro”

Nuevos controles de seguridad	El CSPM de Security Hub lanzó 37 controles nuevos para el estándar de etiquetado de recursos de AWS. El CSPM de Security Hub también lanzó los siguientes controles nuevos: • the section called “[EMR.3] Las configuraciones de seguridad de Amazon EMR deben cifrarse en reposo” • the section called “[EMR.4] Las configuraciones de seguridad de Amazon EMR deben cifrarse en tránsito” • the section called “SageMaker Los modelos [SageMaker.5] deben tener habilitado el aislamiento de red”	22 de enero de 2025
Nuevo control de seguridad	Security Hub CSPM publicó la configuración EC2.172 EC2 VPC Block Public Access que debería bloquear el tráfico de la puerta de enlace a Internet.	15 de enero de 2025

Nuevos controles de seguridad	Están disponibles los siguientes controles nuevos del CSPM de Security Hub. • the section called “[Cognito.1] Los grupos de usuarios de Cognito deben tener activada la protección contra amenazas y el modo de aplicación con todas las funciones para la autenticación estándar” • the section called “[RDS.38] Las instancias de base de datos de RDS para PostgreSQL deben cifrarse en tránsito” • the section called “[RDS.39] Las instancias de base de datos de RDS para MySQL deben cifrarse en tránsito” • the section called “[Redshift.16] Los grupos de subredes de clústeres de Redshift deben tener subredes de varias zonas de disponibilidad”	17 de diciembre de 2024

El CSPM de Security Hub admite PCI DSS v4.0.1	El CSPM de Security Hub ahora es compatible con la versión 4.0.1 del estándar de seguridad de datos para la industria de tarjetas de pago (PCI DSS). Para obtener más información sobre el estándar y los controles que correspon den a este, consulte PCI DSS en el CSPM de Security Hub.	11 de diciembre de 2024
El CSPM de Security Hub recibe los resultados de la secuencia de ataque GuardDuty	Security Hub CSPM ahora recibe los resultados de la secuencia de ataque de Amazon GuardDuty Extended Threat Detection. Los detalles de la secuencia de ataque están disponibles en el objeto de detección del formato de búsqueda de AWS seguridad (ASFF).	1 de diciembre de 2024
El CSPM de Security Hub es compatible con el nuevo Región de AWS	El CSPM de Security Hub ya está disponible en la región de Asia-Pacífico (Malasia). Algunos controles de seguridad tienen limitacio nes regionales. Para ver la lista de controles que no están disponibles en esta región, consulte Límites regionales de los controles de CSPM de Security Hub.	22 de noviembre de 2024

Cambios en Config.1	El CSPM de Security Hub aumentó la severidad del Config.1 control de `MEDIUM` a `CRITICAL` y agregó nuevos códigos de estado y motivos de estado para detectar errores en los hallazgos . Config.1 Para obtener más información sobre los cambios, consulte la entrada del 20 de noviembre de 2024 en Registro de cambios de los controles de CSPM de Security Hub.	20 de noviembre de 2024

Nuevos controles de seguridad	Están disponibles los siguiente s controles nuevos del CSPM de Security Hub. Estos controles forman parte de AWS Foundational Security Best Practices y del NIST SP 800-53 Rev. 5, y evalúan si una nube privada virtual (VPC) que usted administra tiene un punto final de VPC de interfaz para un recurso o recurso. Servicio de AWS AWS • the section called “[EC2.55] Las VPC deben configura rse con un punto final de interfaz para la API de ECR” • the section called “[EC2.56] Las VPC deben configura rse con un punto final de interfaz para Docker Registry” • the section called “[EC2.57] Las VPC deben configura rse con un punto final de interfaz para Systems Manager” • the section called “[EC2.58] Las VPC deben configura rse con un punto final de interfaz para los contactos de Systems Manager Incident Manager” • the section called “[EC2.60] Las VPC deben configura rse con un punto final de	15 de noviembre de 2024

interfaz para Systems
Manager Incident Manager”

Nuevos controles de seguridad	Están disponibles los siguientes controles nuevos del CSPM de Security Hub. • the section called “[AppSync.1]AWS AppSyncLas cachés de las API deben estar cifradas en reposo” • the section called “[AppSync.6]AWS AppSyncLas cachés de las API deben cifrarse en tránsito” • the section called “[EC2.170] Las plantillas de lanzamiento de EC2 deben utilizar la versión 2 del servicio de metadatos de instancias (IMDSv2)” • the section called “[EC2.171] Las conexiones VPN de EC2 deberían tener el registro habilitado” • the section called “[EFS.8] Los sistemas de archivos EFS deben cifrarse en reposo” • the section called “[KMS.5] Las claves KMS no deben ser de acceso público” • the section called “[SNS.4] Las políticas de acceso a los temas de SNS no deberían permitir el acceso público”	18 de octubre de 2024

Nuevos controles de seguridad	Están disponibles los siguientes controles nuevos del CSPM de Security Hub. • the section called “[ECS.16] Los conjuntos de tareas de ECS no deben asignar automáticamente direcciones IP públicas” • the section called “[GuardDuty.7] La monitorización del tiempo de ejecución de GuardDuty EKS debe estar habilitada” • the section called “[Kinesis.3] Las transmisiones de Kinesis deben tener un período de retención de datos adecuado” • the section called “[MSK.3] Los conectores MSK Connect deben estar cifrados en tránsito” • the section called “[RDS.36] Las instancias de base de datos de RDS para PostgreSQL deben publicar los registros en Logs CloudWatch” • the section called “[RDS.37] Los clústeres de bases de datos de Aurora PostgreSQL deben publicar los registros en Logs CloudWatch”	3 de octubre de 2024

- the section called “[S3.24] Los puntos de Multi-Region acceso S3 deben tener habilitada la configuración de bloqueo del acceso público”

Nuevos controles de seguridad	Están disponibles los siguientes controles nuevos del CSPM de Security Hub. • the section called “[Athena.4] Los grupos de trabajo de Athena deberían tener habilitado el registro” • the section called “[CodeBuild.7] las exportaciones de grupos de CodeBuild informes deben cifrarse en reposo” • the section called “[DataSync.1] DataSync las tareas deberían tener el registro activado” • the section called “[] Los sistemas de archivos EFS deben tener habilitadas las copias de seguridad automáticas EFS.7” • Glue.2 (retirado) • the section called “[Glue.3] AWS GlueLas transformaciones de aprendizaje automático deben cifrarse en reposo” • the section called “[WorkSpaces.1] los volúmenes de WorkSpaces usuarios deben cifrarse en reposo” • the section called “[WorkSpaces.2] los volúmenes	30 de agosto de 2024

	WorkSpaces raíz deben cifrarse en reposo”	
Nuevo panel de resultados	El nuevo panel de resultados en la consola del CSPM de Security Hub facilita actuar rápidamente sobre los resultados, revisar los detalles de los recursos y el historial de resultados, y acceder a otra información relevante sobre cada resultado.	16 de agosto de 2024
Actualizar para Config.1 controlar	El Config.1 control comprueba si AWS Config está habilitado, usa la función vinculada al servicio y registra los recursos de los controles habilitados. El CSPM de Security Hub agregó un parámetro personalizado para el control llamado `includeConfigServiceLinkedRoleCheck` . Si establece este parámetro en `false`, puede optar por no comprobar si AWS Config utiliza el rol vinculado al servicio.	15 de agosto de 2024

Designación de una región de origen sin regiones vinculadas	Ahora puede crear un agregador de búsquedas y establecer una región de origen sin vincular ninguna Regiones de AWS a la región de origen. Esto permite habilitar la configuración centralizada sin especificar las regiones vinculadas.	25 de julio de 2024

Selección de los controles disponibles en más regiones	Los siguientes controles ahora están disponibles de forma adicional Regiones de AWS, incluidos US East (North Virginia) y US East (Ohio). • the section called “[DataFirehose.1] Los flujos de entrega de Firehose deben cifrarse en reposo” • the section called “[DMS.10] Los puntos finales de DMS para las bases de datos de Neptune deben tener habilitada la autorización de IAM” • the section called “[DMS.11] Los puntos finales de DMS para MongoDB deben tener un mecanismo de autenticación habilitado” • the section called “[DMS.12] Los puntos finales de DMS para Redis OSS deben tener el TLS habilitado” • the section called “[DynamoDB.7] Los clústeres de DynamoDB Accelerator deben cifrarse en tránsito” • the section called “[EFS.6] Los destinos de montaje de EFS no deben asociarse a subredes que asignan	15 de julio de 2024

direcciones IP públicas en el momento del lanzamiento”

- the section called “[EKS.3] Los clústeres de EKS deben usar secretos de Kubernetes cifrados”
- the section called “[FSx.2] Los sistemas de archivos FSx for Lustre deben configurarse para copiar etiquetas a las copias de seguridad”
- the section called “[MQ.2] Los corredores de ActiveMQ deben transmitir los registros de auditoría a CloudWatch”
- [MQ.3] Los corredores de Amazon MQ deberían tener habilitada la actualización automática de versiones secundarias
- the section called “[Opensearch.11] OpenSearch los dominios deben tener al menos tres nodos principales dedicados”
- the section called “[Redshift.15] Los grupos de seguridad de Redshift deberían permitir la entrada en el puerto del clúster solo desde orígenes restringidos”
- the section called “[SageMaker.4] Las

variantes de producción de SageMaker terminales deben tener un recuento inicial de instancias superior a 1”

- the section called “[Service Catalog.1] Las carteras de Service Catalog deben compartirse dentro de unAWSsolo una organización”
- the section called “[Transfer.2] Los servidores Transfer Family no deben usar el protocolo FTP para la conexión de puntos finales”

Nuevos controles de seguridad	Los siguientes controles nuevos del CSPM de Security Hub se encuentran disponibles: • the section called “[GuardDuty.5] La monitorización del registro de auditoría de GuardDuty EKS debe estar habilitada” • the section called “[GuardDuty.6] GuardDuty La protección Lambda debe estar habilitada” • the section called “[GuardDuty.8] La protección contra GuardDuty malware para EC2 debe estar habilitada” • the section called “[GuardDuty.9] La protección GuardDuty RDS debe estar habilitada” • the section called “[GuardDuty.10] La protección GuardDuty S3 debe estar habilitada” • the section called “[Inspector.1] El escaneo EC2 de Amazon Inspector debe estar activado” • the section called “[Inspector.2] El escaneo ECR de Amazon Inspector debe estar activado”	11 de julio de 2024

- the section called “[Inspector.3] El escaneo de código Lambda de Amazon Inspector Lambda debe estar activado”
- the section called “[Inspector.4] El escaneo estándar de Amazon Inspector Lambda debe estar activado”

Publicación de CIS AWS Foundations Benchmark v3.0.0	Security Hub CSPM lanzó la versión 3.0.0 de Foundation Benchmark de Center for Internet Security (CIS). AWS La versión incluye los siguientes controles nuevos, así como asignaciones a varios controles existentes. • the section called “[EC2.53] Los grupos de seguridad de EC2 no deberían permitir la entrada desde la versión 0.0.0. 0/0 a los puertos de administración remota del servidor” • the section called “[EC2.54] Los grupos de seguridad de EC2 no deberían permitir la entrada desde: :/0 a los puertos de administración remota del servidor” • the section called “[IAM.26] SSL/TLS Los certificados caducados gestionados en IAM deben eliminarse” • the section called “[IAM.27] Las identidades de IAM no deberían tener la AWSCloudShellFullAccess política adjunta” • the section called “[IAM.28] El analizador de acceso externo de IAM Access Analyzer debe estar habilitado”	13 de mayo de 2024

- the section called “[S3.22] Los cubos de uso general de S3 deben registrar los eventos de escritura a nivel de objeto”
- the section called “[S3.23] Los cubos de uso general de S3 deben registrar los eventos de lectura a nivel de objeto”

Nuevos controles de seguridad	Los siguientes controles nuevos del CSPM de Security Hub se encuentran disponibles: • the section called “[DataFirehose.1] Los flujos de entrega de Firehose deben cifrarse en reposo” • the section called “[DMS.10] Los puntos finales de DMS para las bases de datos de Neptune deben tener habilitada la autorización de IAM” • the section called “[DMS.11] Los puntos finales de DMS para MongoDB deben tener un mecanismo de autenticación habilitado” • the section called “[DMS.12] Los puntos finales de DMS para Redis OSS deben tener el TLS habilitado” • the section called “[DynamoDB.7] Los clústeres de DynamoDB Accelerator deben cifrarse en tránsito” • the section called “[EFS.6] Los destinos de montaje de EFS no deben asociarse a subredes que asignan direcciones IP públicas en el momento del lanzamiento”	3 de mayo de 2024

- the section called “[EKS.3] Los clústeres de EKS deben usar secretos de Kubernetes cifrados”
- the section called “[FSx.2] Los sistemas de archivos FSx for Lustre deben configurarse para copiar etiquetas a las copias de seguridad”
- the section called “[MQ.2] Los corredores de ActiveMQ deben transmitir los registros de auditoría a CloudWatch”
- [MQ.3] Los corredores de Amazon MQ deberían tener habilitada la actualización automática de versiones secundarias
- the section called “[Opensearch.11] OpenSearch los dominios deben tener al menos tres nodos principales dedicados”
- the section called “[Redshift.15] Los grupos de seguridad de Redshift deberían permitir la entrada en el puerto del clúster solo desde orígenes restringidos”
- the section called “[SageMaker.4] Las variantes de producción de SageMaker terminale

	s deben tener un recuento inicial de instancias superior a 1” • the section called “[Service Catalog.1] Las carteras de Service Catalog deben compartirse dentro de unAWSsolo una organización” • the section called “[Transfer.2] Los servidores Transfer Family no deben usar el protocolo FTP para la conexión de puntos finales”	
AWS Estándar de etiquetado de recursos	El Estándar de etiquetado de los recursos de AWS del CSPM de Security Hub ya se encuentra disponible de forma general, junto con los nuevos controles que se aplican al estándar.	30 de abril de 2024
Actualización de la política administrada existente	Security Hub CSPM actualizó la política AWS gestionada denominada `AmazonSecurityHubFullAccess` para obtener información sobre los precios y los productos. Servicios de AWS	24 de abril de 2024

In-context configuración de los parámetros de control	Si utiliza la configuración centralizada, ahora puede configurar los parámetros de control en contexto desde la página de detalles de un control de la consola del CSPM de Security Hub.	29 de marzo de 2024
Actualización de la política administrada existente	El CSPM de Security Hub actualizó la política administrada de AWS denominada `AWSSecurityHubReadOnlyAccess` al agregar un campo `Sid`.	22 de febrero de 2024
Nuevo control de seguridad	Ya está disponible el control [Macie.2] que Macie debería activar automáticamente para detectar datos confidenciales. Para conocer los límites regionales de este control, consulte Availability of controls by Region.	19 de febrero de 2024
El CSPM de Security Hub se encuentra disponible en la región Oeste de Canadá (Calgary)	El CSPM de Security Hub ya está disponible en la región Oeste de Canadá (Calgary). Ya están disponibles en esta región todas las características del CSPM de Security Hub, con la excepción de algunos controles de seguridad. Para obtener más información, consulte Disponibilidad de controles por región.	20 de diciembre de 2023

Nuevos controles de seguridad	Los siguientes controles nuevos del CSPM de Security Hub se encuentran disponibles: • the section called “[Backup.1]AWS Backuplos puntos de recuperación deben estar cifrados en reposo” • the section called “[DynamoDB.6] Las tablas de DynamoDB deben tener habilitada la protección de eliminación” • the section called “[EC2.51] Los puntos finales EC2 Client VPN deben tener habilitado el registro de conexiones de clientes” • the section called “[EKS.8] Los clústeres de EKS deben tener habilitado el registro de auditoría” • the section called “[EMR.2] La configuración de acceso público del bloque Amazon EMR debe estar habilitada” • the section called “[FSx.1] FSx para sistemas de archivos OpenZFS debe configurarse para copiar etiquetas en copias de seguridad y volúmenes”	14 de diciembre de 2023

- the section called “[Macie.1] Amazon Macie debería estar activado”
- the section called “[MSK.2] Los clústeres de MSK deberían tener configurada una supervisión mejorada”
- the section called “[Neptune.9] Los clústeres de base de datos Neptune deben implementarse en varias zonas de disponibilidad”
- the section called “[Network Firewall.1] Los firewalls de Network Firewall deben implementarse en varias zonas de disponibilidad”
- the section called “[Network Firewall.2] El registro de Network Firewall debe estar habilitado”
- the section called “[Opensearch.10] OpenSearch los dominios deben tener instalada la última actualización de software”
- the section called “[PCA.1]AWS Privada CALa autoridad emisora de certificados raíz debe estar deshabilitada”
- the section called “[S3.19] Los puntos de acceso S3 deben tener habilitada la configuración de bloqueo de acceso público”

	• the section called “[S3.20] Los cubos de uso general de S3 deben tener habilitad a la eliminación de MFA”	
Enriquecimiento de resultados	Security Hub CSPM agregó los nuevos campos `AwsAccountName` de búsqueda y `ApplicationName` al formato de búsqueda de AWS seguridad (ASFF). `ApplicationArn`	27 de noviembre de 2023
Mejoras en el panel Resumen	Ahora puede acceder a más widgets del panel en la página Resumen de la consola del CSPM de Security Hub, guardar los conjuntos de filtros del panel para centrarse rápidamente en problemas de seguridad específicos y personalizar el diseño del panel.	27 de noviembre de 2023
Configuración centralizada	La configuración centralizada ya está disponible. Con la configuración centralizada, el administrador delegado del CSPM de Security Hub puede configurar este servicio, estándares y controles en varias cuentas, unidades organizativas (UO) y regiones de la organización.	27 de noviembre de 2023

Actualizaciones a políticas administradas	El CSPM de Security Hub agregó nuevos permisos a la política administrada `AWSSecurityHubServiceRolePolicy`, los cuales permiten leer y actualizar las propiedades de control de seguridad personalizables.	26 de noviembre de 2023
Personalización de los parámetros de control	Ahora puede personalizar los valores de los parámetros para controles específicos del CSPM de Security Hub. Esto puede hacer que los resultados de un control específico sean más relevantes para los requisitos de su empresa y sus expectativas de seguridad.	26 de noviembre de 2023
Actualizaciones de las políticas administradas	Security Hub actualizó las políticas administradas `AWSSecurityHubFullAccess` y `AWSSecurityHubOrganizationsAccess`. Estas permiten utilizar, respectivamente, tanto las características del CSPM de Security Hub como la integración con AWS Organizations.	16 de noviembre de 2023

Los controles de seguridad existentes se agregaron al estándar: Service-Managed AWS Control Tower	Los siguientes controles CSPM de Security Hub existentes se han agregado a Service-Managed Standard:. AWS Control Tower • ACM.2 • AppSync.5 • CloudTrail.6 • DMS.9 • DocumentDB.3 • DynamoDB.3 • EC2.23 • EKS.1 • ElastiCache.3 • ElastiCache.4 • ElastiCache.5 • ElastiCache.6 • EventBridge.3 • KMS.4 • Lambda.3 • MQ.5 • MQ.6 • MSK.1 • RDS.12 • RDS.15 • S3.17	14 de noviembre de 2023

Actualizaciones a la política administrada	El CSPM de Security Hub agregó un nuevo permiso de etiquetado a la política administrada `AWSSecurityHubServiceRolePolicy` , que permite al CSPM de Security Hub leer las etiquetas de recursos relacionadas con los resultados.	7 de noviembre de 2023

Nuevos controles de seguridad	Los siguientes controles nuevos del CSPM de Security Hub se encuentran disponibles: • the section called “[AppSync.5]AWS AppSyncLas API de GraphQL no deben autenticarse con claves de API” • the section called “[DMS.6] Las instancias de replicación de DMS deben tener habilitada la actualización automática de las versiones secundarias” • the section called “[DMS.7] Las tareas de replicación del DMS para la base de datos de destino deben tener el registro habilitado” • the section called “[DMS.8] Las tareas de replicación del DMS para la base de datos de origen deben tener el registro activado” • the section called “[DMS.9] Los puntos finales del DMS deben usar SSL” • the section called “[DocumentDB.3] Las instantáneas de clústeres manuales de Amazon DocumentDB no deben ser públicas”	10 de octubre de 2023

- the section called "[DocumentDB.4] Los clústeres de Amazon DocumentDB deben publicar los registros de auditoría en Logs CloudWatch"
- the section called "[DocumentDB.5] Los clústeres de Amazon DocumentDB deben tener habilitada la protección contra eliminaciones"
- the section called "[ECS.9] Las definiciones de tareas de ECS deben tener una configuración de registro"
- the section called "[EventBridge.3] los autobuses de eventos EventBridge personalizados deben tener adjunta una política basada en los recursos"
- the section called "[EventBridge.4] los puntos finales EventBridge globales deberían tener habilitada la replicación de eventos"
- the section called "[MSK.1] Los clústeres de MSK deben cifrarse en tránsito entre los nodos de intermediación"
- the section called "[MQ.5] Los corredores de ActiveMQ

deberían usar el modo de implementación active/standby”

- the section called “[MQ.6] Los corredores de RabbitMQ deberían usar el modo de despliegue de clústeres”
- the section called “[Network Firewall.9] Los firewalls de Network Firewall deben tener habilitada la protección de eliminación”
- the section called “[RDS.34] Los clústeres de bases de datos Aurora MySQL deben publicar los registros de auditoría en Logs CloudWatch”
- the section called “[RDS.35] Los clústeres de bases de datos de RDS deben tener habilitada la actualización automática de versiones secundarias”
- the section called “[Route53.2] Las zonas alojadas públicas de Route 53 deberían registrar las consultas de DNS”
- the section called “[WAF.12] AWS WAFlas reglas deben tener CloudWatch las métricas habilitadas”

Actualizaciones a la política administrada	El CSPM de Security Hub agregó nuevas acciones de Organizations a la política administrada `AWSSecurityHubServiceRolePolicy` , que permiten al CSPM de Security Hub recuperar información de cuentas y unidades organizativas (UO). Además, agregamos nuevas acciones del CSPM de Security Hub que permiten al CSPM de Security Hub leer y actualizar las configuraciones de los servicios, incluidos los estándares y los controles.	27 de septiembre de 2023

Los controles de seguridad existentes se agregaron a Standard Service-Managed : AWS Control Tower	Los siguientes controles CSPM de Security Hub existentes se han agregado a Service-Managed Standard:. AWS Control Tower • the section called “[Athena.1] Los grupos de trabajo de Athena deben estar cifrados en reposo” • the section called “[DocumentDB.1] Los clústeres de Amazon DocumentDB deben cifrarse en reposo” • the section called “[DocumentDB.2] Los clústeres de Amazon DocumentDB deben tener un período de retención de copias de seguridad adecuado” • the section called “[Neptune.1] Los clústeres de bases de datos de Neptune deben cifrarse en reposo” • the section called “[Neptune.2] Los clústeres de bases de datos de Neptune deberían publicar registros de auditoría en Logs CloudWatch” • the section called “[Neptune.3] Las instantáneas del clúster de base de datos	26 de septiembre de 2023

de Neptune no deben ser públicas”

- the section called “[Neptune.4] Los clústeres de base de datos de Neptune deben tener habilitada la protección contra eliminación”
- the section called “[Neptune.5] Los clústeres de Neptune DB deberían tener habilitadas las copias de seguridad automatizadas”
- the section called “[Neptune.6] Las instantáneas del clúster de base de datos de Neptune deben cifrarse en reposo”
- the section called “[Neptune.7] Los clústeres de base de datos de Neptune deben tener habilitada la autenticación de bases de datos de IAM”
- the section called “[Neptune.8] Los clústeres de bases de datos de Neptune deben configurarse para copiar etiquetas a las instantáneas”
- the section called “[RDS.27] Los clústeres de bases de datos de RDS deben cifrarse en reposo”

La vista de los controles consolidados y los hallazgos de los controles consolidados están disponibles en AWS GovCloud (US)	La vista de los controles consolidados y los resultados de los controles consolidados ya están disponibles en AWS GovCloud (US) Region. La página Controles de la consola del CSPM de Security Hub muestra todos los controles en los estándares. Cada control tiene el mismo ID de control para todos los estándares. Al activar los resultados de control consolidados, recibirá un único resultado por control de seguridad, incluso cuando un control se aplique a varios estándares habilitados.	6 de septiembre de 2023
La vista de los controles consolidados y los resultados de los controles consolidados están disponibles en las regiones de China	La vista de controles consolidados y los resultados de controles consolidados ahora ya están disponibles en las regiones de China. La página Controles de la consola del CSPM de Security Hub muestra todos los controles en los estándares. Cada control tiene el mismo ID de control para todos los estándares. Al activar los resultados de control consolidados, recibirá un único resultado por control de seguridad, incluso cuando un control se aplique a varios estándares habilitados.	28 de agosto de 2023

El CSPM de Security Hub se encuentra disponible en la región de Israel (Tel Aviv)	El CSPM de Security Hub ya está disponible en Israel (Tel Aviv). Ya están disponibl es en esta región todas las características del CSPM de Security Hub, con la excepción de algunos controles de seguridad. Para obtener más información, consulte Disponibilidad de controles por región.	8 de agosto de 2023

Nuevos controles de seguridad	Los siguientes controles nuevos del CSPM de Security Hub se encuentran disponibles: • the section called “[Athena.1] Los grupos de trabajo de Athena deben estar cifrados en reposo” • the section called “[DocumentDB.1] Los clústeres de Amazon DocumentDB deben cifrarse en reposo” • the section called “[DocumentDB.2] Los clústeres de Amazon DocumentDB deben tener un período de retención de copias de seguridad adecuado” • the section called “[Neptune.1] Los clústeres de bases de datos de Neptune deben cifrarse en reposo” • the section called “[Neptune.2] Los clústeres de bases de datos de Neptune deberían publicar registros de auditoría en Logs CloudWatch” • the section called “[Neptune.3] Las instantáneas del clúster de base de datos	28 de julio de 2023

de Neptune no deben ser públicas”

- the section called “[Neptune.4] Los clústeres de base de datos de Neptune deben tener habilitada la protección contra eliminación”
- the section called “[Neptune.5] Los clústeres de Neptune DB deberían tener habilitadas las copias de seguridad automatizadas”
- the section called “[Neptune.6] Las instantáneas del clúster de base de datos de Neptune deben cifrarse en reposo”
- the section called “[Neptune.7] Los clústeres de base de datos de Neptune deben tener habilitada la autenticación de bases de datos de IAM”
- the section called “[Neptune.8] Los clústeres de bases de datos de Neptune deben configurarse para copiar etiquetas a las instantáneas”
- the section called “[RDS.27] Los clústeres de bases de datos de RDS deben cifrarse en reposo”

Nuevos operadores para los criterios de las reglas de automatización	Ahora puede utilizar los operadores de comparación CONTAINS y NOT_CONTAINS para el mapa de reglas de automatización y los criterios de cadena.	25 de julio de 2023
Reglas de automatización	El CSPM de Security Hub ahora ofrece reglas de automatización que actualizan automáticamente los resultados según los criterios que especifique.	13 de junio de 2023
Nueva integración de terceros	Snyk es una nueva integración de terceros que envía los resultados al CSPM de Security Hub.	12 de junio de 2023

Los controles de seguridad existentes se agregaron a Service-Managed Standard: AWS Control Tower	Los siguientes controles CSPM de Security Hub existentes se han agregado a Service-Managed Standard:. AWS Control Tower • the section called “[Account.1] La información de contacto de seguridad debe proporcionarse para unCuenta de AWS” • the section called “[APIGateway.8] Las rutas de API Gateway deben especificar un tipo de autorización” • the section called “[APIGateway.9] El registro de acceso debe configurarse para las etapas V2 de API Gateway” • the section called “[CodeBuild.3] Los registros de CodeBuild S3 deben estar cifrados” • the section called “[EC2.25] Las plantillas de lanzamiento de Amazon EC2 no deben asignar direcciones IP públicas a las interfaces de red” • the section called “[ELB.1] El balanceador de carga de aplicaciones debe configurarse para redirigir todas las solicitudes HTTP a HTTPS”	12 de junio de 2023

- the section called “[Redshift.10] Los clústeres de Redshift deben cifrarse en reposo”
- the section called “[SageMaker.2] las instancias de SageMaker cuadernos deben lanzarse en una VPC personalizada”
- the section called “[SageMaker.3] Los usuarios no deben tener acceso root a las instancias de los SageMaker cuadernos”
- the section called “[WAF.10] AWS WAFLas ACL web deben tener al menos una regla o grupo de reglas”

Nuevos controles de seguridad	Los siguientes controles nuevos del CSPM de Security Hub se encuentran disponibles: • the section called “[ACM.2] Los certificados RSA gestionados por ACM deben utilizar una longitud de clave de al menos 2048 bits” • the section called “[AppSync.2]AWS AppSyncdebe tener habilitado el registro a nivel de campo” • the section called “[CloudFront.13] CloudFront las distribuciones deben usar el control de acceso al origen” • the section called “[Elastic Beanstalk.3] Elastic Beanstalk debería transmitir los registros a CloudWatch” • the section called “[S3.17] Los cubos de uso general de S3 deben cifrarse en reposo con AWS KMS keys” • the section called “[StepFunctions.1] Step Functions indica que las máquinas deben tener el registro activado”	6 de junio de 2023

El CSPM de Security Hub se encuentra disponible en Asia-Pacífico (Melbourne)	El CSPM de Security Hub ya está disponible en la región de Asia-Pacífico (Melbourne). Ya están disponibles en esta región todas las características del CSPM de Security Hub, con la excepción de algunos controles de seguridad. Para obtener más información, consulte Disponibilidad de controles por región.	25 de mayo de 2023
Búsqueda del historial	El CSPM de Security Hub ahora puede rastrear el historial de un resultado durante los últimos 90 días.	4 de mayo de 2023

Nuevos controles de seguridad	Los siguientes controles nuevos del CSPM de Security Hub se encuentran disponibles: • the section called “[EKS.1] Los puntos finales del clúster EKS no deben ser de acceso público” • the section called “[ELB.16] Los balanceadores de carga de aplicaciones deben estar asociados a un AWS WAF ACL web” • the section called “[Redshift.10] Los clústeres de Redshift deben cifrarse en reposo” • the section called “[S3.15] Los cubos de uso general de S3 deben tener activado el bloqueo de objetos”	29 de marzo de 2023
Soporte ampliado para los resultados de control consolidados	La respuesta de seguridad automatizada de la AWS versión 2.0.0 ahora admite los resultados de los controles consolidados.	24 de marzo de 2023
Security Hub (CSPM) está disponible en versiones nuevas Regiones de AWS	El CSPM de Security Hub ya está disponible en las regiones de Asia-Pacífico (Hyderabad), Europa (España) y Europa (Zúrich). Existen límites en cuanto a los controles disponibles en estas regiones.	21 de marzo de 2023

Actualización a la política administrada	El CSPM de Security Hub ha actualizado un permiso existente en la política administrada `AWSSecurityHubServiceRolePolicy` .	17 de marzo de 2023

Nuevos controles de seguridad para el estándar NIST 800-53	El CSPM de Security Hub agregó los siguientes controles de seguridad, que son aplicables al estándar NIST 800-53: • the section called “[Account.2]Cuentas de AWSdebe formar parte de unAWS Organizationsorganización” • the section called “[CloudWatch.15] CloudWatch las alarmas deben tener configuradas acciones específicas” • the section called “[CloudWatch.16] los grupos de CloudWatch registros deben conservarse durante un período de tiempo específico” • the section called “[CloudWatch.17] las acciones CloudWatch de alarma deben estar activadas” • the section called “[DynamoDB.4] Las tablas de DynamoDB deben estar presentes en un plan de respaldo” • the section called “[EC2.28] Los volúmenes de EBS deben estar cubiertos por un plan de respaldo”	3 de marzo de 2023

	• EC2.29 — Las instancias EC2 deben lanzarse en una VPC (retirada) • the section called “[RDS.26] Las instancias de base de datos de RDS deben protegerse mediante un plan de respaldo” • the section called “[S3.14] Los cubos de uso general de S3 deben tener habilitado el control de versiones” • the section called “[WAF.11] AWS WAFEl registro de ACL web debe estar habilitado”	
National Institute of Standards and Technology (NIST, Instituto Nacional de Estándares y Tecnología) 800-53, Rev. 5	El CSPM de Security Hub ahora es compatible con el estándar NIST 800-53 Rev. 5 con más de 200 controles de seguridad aplicables.	28 de febrero de 2023

Vista de controles consolidados y control de resultados	Con el lanzamiento de la vista de controles consolidados, la página Controles de la consola del CSPM de Security Hub muestra todos los controles de los estándares. Cada control tiene el mismo ID de control para todos los estándares. Al activar los resultados de control consolidados, recibirá un único resultado por control de seguridad, incluso cuando un control se aplique a varios estándares habilitados.	23 de febrero de 2023

Nuevos controles de seguridad	Están disponibles los siguientes controles nuevos del CSPM de Security Hub. Algunos controles tienen restricciones regionales. • the section called “[ElastiCache.1] ElastiCache (Redis OSS) los clústeres deben tener habilitadas las copias de seguridad automáticas” • the section called “[ElastiCache.2] ElastiCache los clústeres deberían tener habilitadas las actualizaciones automáticas de las versiones secundarias” • the section called “[ElastiCache.3] los grupos de ElastiCache replicación deberían tener habilitada la conmutación por error automática” • the section called “[ElastiCache.4] los grupos de ElastiCache replicación deben cifrarse en reposo” • the section called “[ElastiCache.5] los grupos de ElastiCache replicación deben cifrarse en tránsito” • the section called “[ElastiCache.6] ElastiCache (Redis OSS) Los grupos de replicación de versiones	16 de febrero de 2023

	anteriores deberían tener habilitada la autenticación de Redis OSS” • the section called “[ElastiCache.7] los ElastiCache clústeres no deben usar el grupo de subredes predeterminado”	
Nuevos campos del ASFF	Security Hub CSPM ha añadido ProductFields.ArchivalReasons:0/Description y ProductFields.ArchivalReasons:0/ReasonCode al formato de búsqueda de AWS seguridad (ASFF).	8 de febrero de 2023
Nuevos campos del ASFF	Security Hub CSPM ha agregado Compliance.AssociatedStandards y Compliance.SecurityControlId al formato de búsqueda de AWS seguridad (ASFF).	31 de enero de 2023
Los detalles de la vulnerabilidad ya están disponibles	Ahora puede ver los detalles de la vulnerabilidad en la consola del CSPM de Security Hub para ver los resultados que Amazon Inspector envía al CSPM de Security Hub.	14 de enero de 2023
El CSPM de Security Hub está disponible en Oriente Medio (EAU)	El CSPM de Security Hub ya está disponible en Oriente Medio (EAU). Algunos controles tienen límites regionales.	12 de enero de 2023

Se agregó la integración de terceros con MetricStream	Security Hub CSPM ahora admite la integración de terceros MetricStream en todas las regiones, excepto en China y. AWS GovCloud (US)	11 de enero de 2023
Se ha incrementado el límite de cuentas organizativas	El CSPM de Security Hub ahora es compatible con hasta 11 000 cuentas de miembro por cada cuenta de administrador de CSPM de Security Hub por región.	27 de diciembre de 2022
ElasticBeanstalk.3 revertido	El CSPM de Security Hub anuló el control [ElasticBeanstalk.3] al que Elastic Beanstalk debía transmitir los registros CloudWatch desde el estándar FSBP en todas las regiones.	21 de diciembre de 2022
El CSPM de Security Hub agrega nuevos controles de seguridad	Los nuevos controles del CSPM de Security Hub están disponibles para los clientes que hayan habilitado el estándar FSBP. Algunos controles tienen restricciones regionales.	15 de diciembre de 2022

Guía sobre las próximas características	El CSPM de Security Hub planea lanzar dos nuevas características: vista consolida da de controles y resultado s de control consolidados. Estas próximas caracterí sticas pueden afectar los flujos de trabajo existente s que dependen del control de campos y valores de búsqueda.	9 de diciembre de 2022
La integración con Amazon Security Lake ya está disponible	Security Lake ahora se integra con el CSPM de Security Hub al recibir los resultados del CSPM de Security Hub.	29 de noviembre de 2022
Service-Managed Soporte para el estándar: AWS Control Tower	Security Hub CSPM admite un nuevo estándar de seguridad llamado Service-Managed Standard:. AWS Control Tower AWS Control Tower administra este estándar.	28 de noviembre de 2022
La versión 1.4.0 de CIS AWS Foundations Benchmark ya está disponible en las regiones de China	Security Hub CSPM ahora es compatible con CIS AWS Foundations Benchmark v1.4.0 en las regiones de China.	18 de noviembre de 2022
Ya está disponible la integración con Jira Service Management Cloud	Jira Service Managemen t Cloud ahora recibe los resultados del CSPM de Security Hub en todas las regiones disponibles, excepto en las regiones de China.	17 de noviembre de 2022

AWS IoT Device Defender la integración ya está disponible	AWS IoT Device Defender ahora envía los hallazgos al CSPM de Security Hub en todas las regiones disponibles.	17 de noviembre de 2022
Soporte para CIS AWS Foundations Benchmark v1.4.0	Security Hub CSPM ahora proporciona controles de seguridad compatibles con CIS AWS Foundatio ns Benchmark v1.4.0. Este estándar está disponible en todas las regiones disponibl es, excepto en las regiones de China.	9 de noviembre de 2022
Compatibilidad con los anuncios de Security Hub CSPM en AWS GovCloud (US)	Ahora puede suscribirse a los anuncios del CSPM de Security Hub con Amazon Simple Notification Service (Amazon SNS) en () y AWS GovCloud AWS GovCloud (US-EastUS-West) para recibir notificaciones sobre el CSPM de Security Hub.	3 de octubre de 2022
AWS Security Hub CSPM añade un nuevo control de seguridad	El nuevo control CSPM de Security Hub AutoScaling.9 está disponible para los clientes que hayan habilitad o el estándar FSBP. Los controles pueden tener restricciones regionales.	1 de septiembre de 2022

Suscríbase a los anuncios del CSPM de Security Hub	Ahora se puede suscribir a los anuncios del CSPM de Security Hub con Amazon Simple Notification Service (Amazon SNS) para recibir notificaciones sobre el CSPM de Security Hub.	29 de agosto de 2022
Expansión regional para la agregación entre regiones	Cross-Region La agregació n ya está disponible para encontrar hallazgos, actualiza ciones e información de todos lados. AWS GovCloud (US)	2 de agosto de 2022
Nuevas integraciones de productos de terceros	Fortinet: FortiCNP es una integración de terceros que recibe los resultados del CSPM de Security Hub y JFrog es una integración de terceros que envía los resultados al CSPM de Security Hub.	26 de julio de 2022
EC2.27 está retirado	El CSPM de Security Hub se ha retirado EC2.27 : las instancias EC2 en ejecución no deben utilizar pares de claves, un control anterior del estándar AWS Found ational Security Best Practices (FSBP).	20 de julio de 2022

Lambda.2 ya no es compatible con python3.6	Security Hub CSPM ya no admite python3.6 como parámetro para Lambda.2 : las funciones de Lambda deberían usar tiempos de ejecución compatibles, un control del estándar Foundatio nal Security Best Practices (FSBP). AWS	19 de julio de 2022
AWS El CSPM de Security Hub agrega nuevos controles de seguridad	Los nuevos controles del CSPM de Security Hub están disponibles para los clientes que hayan habilitad o el estándar FSBP. Algunos controles tienen restricciones regionales.	22 de junio de 2022
AWS El CSPM de Security Hub admite una nueva región	El CSPM de Security Hub ya está disponible en Asia-Pacífico (Yakarta). Algunos controles no están disponibles en esta región.	7 de junio de 2022
Integración mejorada entre AWS Security Hub CSPM y AWS Config	Los usuarios del CSPM de Security Hub pueden ver los resultados de las evaluacio nes de las AWS Config reglas como hallazgos en el CSPM de Security Hub.	6 de junio de 2022

Se agregó la posibilidad de excluirse de los estándares de activación automática	Para los usuarios que lo han integrado AWS Organizations, esta función les permite iniciar sesión en la cuenta de administrador de CSPM de Security Hub y excluir las cuentas de los nuevos miembros de los estándares de activación automática.	25 de abril de 2022
Agregación entre regiones ampliada	Se incluyó la agregación entre regiones para controlar los estados y las puntuaciones de seguridad.	20 de abril de 2022
CompanyName y ahora ProductName son atributos de nivel superior	Se agregaron nuevos atributos de nivel superior para establecer los nombres de las empresas y los productos asociados a las integraciones personalizadas	1 de abril de 2022
Se agregaron nuevos controles al estándar AWS Fundational Security Best Practices	Se agregaron 5 controles nuevos al estándar AWS Fundational Security Best Practices.	31 de marzo de 2022
Se agregaron nuevos objetos de detalles de recursos al ASFF	Se agregó un `AwsRdsDbSecurityGroup` tipo de recurso al ASFF.	25 de marzo de 2022
Se agregaron detalles de recursos adicionales en el ASFF	Se agregaron detalles adicionales a `AwsAutoScalingScalingGroup`, `AwsElbLoadBalancer`, `AwsRedshiftCluster`, y `AwsCodeBuildProject`.	25 de marzo de 2022

Se agregaron nuevos controles al estándar AWS Fundational Security Best Practices	Se agregaron 15 controles nuevos al estándar AWS Fundational Security Best Practices.	16 de marzo de 2022
Se agregaron nuevos controles al estándar de mejores prácticas de seguridad AWS fundamental y al estándar de seguridad de datos del sector de tarjetas de pago (PCI DSS)	Se han añadido nuevos controles para Amazon OpenSearch Service, Amazon RDS, Amazon EC2 y Elastic Load Balancing, así como CloudFront al estándar AWS Foundational Security Best Practices. También se agregaron dos nuevos controles de OpenSearch servicio al PCI DSS.	15 de febrero de 2022
Se agregó un nuevo campo al ASFF	Se agregó un nuevo campo: Muestra.	26 de enero de 2022
Se agregó la integración con AWS Health	AWS Health utiliza la mensajería de eventos de servicio a servicio para enviar los hallazgos al CSPM de Security Hub.	19 de enero de 2022
Se ha añadido la integración con AWS Trusted Advisor	Trusted Advisor envía los resultados de sus comprobac iones a Security Hub CSPM en forma de hallazgos de Security Hub CSPM. El CSPM de Security Hub envía los resultados de sus comprobac iones AWS fundamentales de las mejores prácticas de seguridad a. Trusted Advisor	18 de enero de 2022

Objetos de detalles de recursos actualizados en el ASFF	Se agregaron `MixedInstancesPolicy` y `AvailabilityZones` a `AwsAutoScalingAutoScalingGroup`. Se agregó `MetadataOptions` a `AwsAutoScalingLaunchConfiguration`. Se agregó `BucketVersioningConfiguration` a `AwsS3Bucket`.	20 de diciembre de 2021
Salida actualizada de la documentación del ASFF	Anteriormente, las descripciones de los atributos del ASFF figuraban en un solo tema. Cada objeto de nivel superior y cada objeto de detalles de recursos se encuentran ahora en su propio tema. El tema de sintaxis del ASFF contiene enlaces a esos temas.	20 de diciembre de 2021
Se agregaron nuevos objetos de detalles de recursos a ASFF para AWS Network Firewall	Para AWS Network Firewall, se agregaron los siguientes objetos de detalles de recursos: `AwsNetworkFirewallFirewall` `AwsNetworkFireFirewallPolicy`, y `AwsNetworkFirewallRuleGroup`.	20 de diciembre de 2021

Se agregó soporte para la nueva versión de Amazon Inspector	El CSPM de Security Hub está integrado con la nueva versión de Amazon Inspector y con Amazon Inspector Classic. Amazon Inspector envía resultados al CSPM de Security Hub.	29 de noviembre de 2021
Se modificó la gravedad de EC2.19	La gravedad de EC2.19 (los grupos de seguridad no deben permitir el acceso sin restricciones a los puertos de alto riesgo) pasa de alta a crítica.	17 de noviembre de 2021
Nueva integración con Sonrai Dig	El CSPM de Security Hub ahora ofrece una integración con Sonrai Dig. Sonrai Dig supervisa los entornos de la nube para identificar los riesgos de seguridad. Sonrai Dig envía resultados al CSPM de Security Hub.	12 de noviembre de 2021
Se actualizó la comprobación del CIS 2.1 y los controles CloudTrail.1	Además de comprobar que existe al menos una CloudTrail ruta multirregional, CIS 2.1 y CloudTrail.1 ahora también comprueba que el `ExcludeManagementEventSources` parámetro está vacío en al menos una de las rutas multirregionales CloudTrail .	9 de noviembre de 2021

Se agregó mayor compatibilidad para puntos de conexión de VPC	El CSPM de Security Hub ahora está integrado AWS PrivateLink y es compatible con los puntos finales de la VPC.	3 de noviembre de 2021
Se agregaron controles al estándar AWS Fundational Security Best Practices	Se agregaron nuevos controles para Elastic Load Balancing (ELB.2 and ELB.8) y AWS Systems Manager (SSM.4).	2 de noviembre de 2021
Se agregaron puertos a la comprobación del EC2.19 control	EC2.19 ahora también comprueba que los grupos de seguridad no permiten el acceso sin restricciones a los siguientes puertos: 3000 (marcos de desarrollo web Go y Ruby), 5000 (marcos de desarrollo web de Python), 8088 (puerto HTTP antiguo) y 8888 (puerto HTTP alternativo) Node.js	27 de octubre de 2021
Se agregó la integración con Cloud SIEM Logz.io	Logz.io es un proveedor de Cloud SIEM que proporciona una correlación avanzada de los datos de registro y eventos para ayudar a los equipos de seguridad a detectar, analizar y responder a las amenazas de seguridad en tiempo real. Logz.io recibe los hallazgos del CSPM de Security Hub.	25 de octubre de 2021

Se agregó soporte para la agregación entre regiones de resultados	Cross-Region la agregación le permite ver todos sus hallazgos sin tener que cambiar de región. Las cuentas de administrador eligen una región de agregación y las regiones vinculadas. Los resultados de la cuenta de administrador y sus cuentas de miembros se agregan de las regiones vinculadas a la región de agregación.	20 de octubre de 2021
Objetos de detalles de recursos actualizados en el ASFF	Se agregaron detalles del certificado de visor a `AwsCloudFrontDistribution` . Se agregaron detalles adicionales a `AwsCodeBuildProject` . Se agregaron atributos del equilibrador de carga a `AwsElbV2LoadBalancer` . Se agregó el identificador de la cuenta del propietario del bucket de S3 a `AwsS3Bucket` .	8 de octubre de 2021

Se agregaron nuevos objetos de detalles de recursos al ASFF	Se agregaron los siguientes nuevos objetos de detalles de recursos al ASFF: `AwsEc2VpcEndpointService` , `AwsEcrRepository` , `AwsEksCluster` , `AwsOpenSearchServiceDomain` , `AwsWafRateBasedRule` , `AwsWafRegionalRateBasedRule` , `AwsXrayEncryptionConfig`	8 de octubre de 2021
Se ha eliminado el tiempo de ejecución obsoleto del control Lambda.2	En el estándar AWS Fundation al Security Best Practices , se eliminó el `dotnetcore2.1` tiempo de ejecución de [Lambda.2] Las funciones de Lambda deberían usar los tiempos de ejecución compatibles.	6 de octubre de 2021
Nuevo nombre para la integración de Check Point	La integración con Check Point Dome9 Arc ahora es Check Point Posture Management. CloudGuard El ARN de integración no ha cambiado.	1 de octubre de 2021
Se eliminó la integración con Alcide	Se interrumpe la integración con Alcide KAudit.	30 de septiembre de 2021

Se modificó la gravedad de EC2.19	La gravedad de [EC2.19] Los grupos de seguridad que no deben permitir el acceso sin restricciones a los puertos de alto riesgo cambia de media a alta.	30 de septiembre de 2021
La integración con ahora AWS Organizations es compatible en las regiones de China	La integración del CSPM de Security Hub con Organizat ions ya está disponible en China (Pekín) y China (Ningxia).	20 de septiembre de 2021
Nueva AWS Config regla para los PCI.S3.6 controles S3.1 de tierra	Ambos S3.1 y PCI.S3.6 verifique que la configuración de bloqueo del acceso público de Amazon S3 esté habilitad a. La AWS Config regla para estos controles se cambia de `s3-account-level-public-access-block s` a `s3-account-level-public-access-block s-periodic` .	14 de septiembre de 2021
Se eliminaron los tiempos de ejecución obsoletos del control Lambda.2	En el estándar AWS Fundation al Security Best Practices , se eliminaron los tiempos de `ruby2.5` ejecución de [Lambda.2] Las **`nodejs10.x`** funciones de Lambda deberían utilizar los tiempos de ejecución compatibles.	13 de septiembre de 2021

Se modificó la gravedad del control CIS 2.2	En el estándar CIS AWS Foundations Benchmark, la gravedad de la versión 2.2. — Asegúrese de que la validación del archivo de CloudTrail registro esté habilitada y cambie de Bajo a Medio.	13 de septiembre de 2021
Actualizado ECS.1 y Lambda.2 SSM.1 en el estándar AWS fundamental de mejores prácticas de seguridad	En el estándar AWS Fundational Security Best Practices, ECS.1 ahora tiene un `SkipInactiveTaskDefinitions` parámetro establecido en. `true` Esto garantiza que el control solo compruebe las definiciones de tareas activas. For Lambda.2, agregó Python 3.9 a la lista de tiempos de ejecución. SSM.1 ahora comprueba tanto las instancias detenidas como las que están en ejecución.	7 de septiembre de 2021
PCI.Lambda.2 el control ahora excluye los recursos de Lambda @Edge	En el estándar de seguridad de datos para el sector de las tarjetas de pago (PCI DSS), el PCI.Lambda.2 control ahora excluye los recursos de Lambda @Edge.	7 de septiembre de 2021
Se agregó la integración con HackerOne Vulnerability Intelligence	El CSPM de Security Hub ahora ofrece una integración con HackerOne Vulnerability Intelligence. La integración envía resultados al CSPM de Security Hub.	7 de septiembre de 2021

Objetos de detalles de recursos actualizados en el ASFFF	Para `AwsKmsKey` , se agregó `KeyRotationStatus` . Para `AwsS3Bucket` , se agregaron `AccessControlList` , `BucketLoggingConfiguration` , `BucketNotificationConfiguration` , y `BucketWebsiteConfiguration` .	2 de septiembre de 2021
Se agregaron nuevos objetos de detalles de recursos al ASFF	Se agregaron los siguientes nuevos objetos de detalles de recursos al ASFF: `AwsAutoScalingLaunchConfiguration` , `AwsEc2VpnConnection` , y `AwsEcrContainerImage` .	2 de septiembre de 2021
Se agregaron detalles al objeto `Vulnerabilities` en el ASFF	En `Cvss`, se agregaron `Adjustments` y `Source`. En `VulnerablePackages` , se agregó la ruta del archivo y el administrador de paquetes.	2 de septiembre de 2021
Systems Manager Explorer y su OpsCenter integración ahora son compatibles en las regiones de China	El Security Hub CSPM se integra con SSM Explorer y ahora OpsCenter es compatible en China (Beijing) y China (Ningxia).	31 de agosto de 2021

Retirar el Lambda.4 control	Security Hub CSPM está retirando el control [Lambda.4] Las funciones de Lambda deberían tener configura da una cola de mensajes muertos. Cuando se retira un control, deja de aparecer en la consola y el CSPM de Security Hub deja de efectuar comprobaciones relacionadas con este.	31 de agosto de 2021
Retirar el control PCI.EC2.3	Security Hub CSPM está retirando el control [PCI.EC2.3] Los grupos de seguridad de EC2 no utilizados deben eliminarse. Cuando se retira un control, deja de aparecer en la consola y el CSPM de Security Hub deja de efectuar comprobaciones relacionadas con este.	27 de agosto de 2021
Cambio en la forma en que el CSPM de Security Hub envía los resultados a las acciones personalizadas	Cuando se envían resultados a una acción personalizada, el CSPM de Security Hub ahora envía cada resultado en un evento Security Hub Findings - Custom Action diferente.	20 de agosto de 2021

Se agregó un nuevo código de motivo de estado de cumplimiento para los tiempos de ejecución de Lambda personalizados	Se agregó un nuevo `LAMBDA_CUSTOM_RUNTIME_DETAILS_NOT_AVAILABLE` código de motivo de estado de cumplimiento. Este código de motivo indica que el CSPM de Security Hub no pudo realizar una revisión con un tiempo de ejecución de Lambda personalizado.	20 de agosto de 2021
AWS Firewall Manager la integración ahora es compatible en las regiones de China	La integración del CSPM de Security Hub con Firewall Manager ya es compatible en China (Pekín) y China (Ningxia).	19 de agosto de 2021
Nuevas integraciones con Caveonix Cloud y Forcepoint Cloud Security Gateway	El CSPM de Security Hub ahora ofrece integraciones con Caveonix Cloud y Forcepoint Cloud Security Gateway. Ambas integraciones envían resultados al CSPM de Security Hub.	10 de agosto de 2021

Se agregaron nuevos atributos `CompanyName`, `ProductName` y `Region` al ASFF	Se agregaron los campos `CompanyName`, `ProductName` y `Region` al nivel superior del ASFF. Estos campos se rellenan automáticamente y, a excepción de las integraciones de productos personalizadas, no se pueden actualizar con `BatchImportFindings` o `BatchUpdateFindings`. En la consola, los filtros de búsqueda utilizan estos nuevos campos. En la API, los filtros `CompanyName` y `ProductName` usan los atributos que se encuentran debajo de `ProductFields`.	23 de julio de 2021
Se agregaron y actualizaron los objetos de detalles de los recursos en el ASFF	Se agregaron nuevos `AwsRdsEventSubscription` tipos de recursos y nuevos detalles de recursos. Se agregaron detalles del recurso para el tipo de recurso `AwsEcsService`. Se agregaron atributos al objeto de detalles del recurso `AwsElasticsearchDomain`.	23 de julio de 2021

Se agregaron controles al estándar de mejores prácticas de seguridad AWS fundamentales	Se han añadido nuevos controles para Amazon API Gateway (APIGateway.5), Amazon EC2 (EC2.19), Amazon ECS (ECS.2), Elastic Load Balancing (ELB.7), Amazon OpenSearch Service (ES.5 mediante ES.8), Amazon RDS (RDS.16 mediante RDS.23), Amazon Redshift (Redshift.4) y Amazon SQS (). SQS.1	20 de julio de 2021
Se movió un permiso dentro de la política administrada de roles vinculados a un servicio	Se trasladó el permiso `config:PutEvaluations` a la política `AWSSecurityHubServiceRolePolicy`, gestionada para que se aplique a todos los recursos.	14 de julio de 2021
Se agregaron controles al estándar AWS Fundational Security Best Practices	Se han añadido nuevos controles para Amazon API Gateway (APIGateway.4), Amazon CloudFront (CloudFront.5 y CloudFront.6), Amazon EC2 (EC2.17 y EC2.18), Amazon ECS (ECS.1), Amazon OpenSearch Service (ES.4), AWS Identity and Access Management (IAM.21), Amazon RDS (RDS.15) y Amazon S3 (). S3.8	8 de julio de 2021

Se agregaron nuevos códigos de motivo de estado de cumplimiento para los resultados de control	`INTERNAL_SERVICE_ERROR` indica que se ha producido un error desconocido. `SNS_TOPIC_CROSS_ACCOUNT` indica que el tema de SNS pertenece a una cuenta diferente. `SNS_TOPIC_INVALID` indica que el tema de SNS asociado no es válido.	6 de julio de 2021
Se agregó la integración con Amazon Q Developer en aplicaciones de chat	Se agregó la integración con Amazon Q Developer en aplicaciones de chat El CSPM de Security Hub envía resultados a Amazon Q Developer en aplicaciones de chat.	30 de junio de 2021
Se agregó un nuevo permiso a la política de administración de funciones vinculadas al servicio	Se agregó un nuevo permiso a la política administrada `AWSSecurityHubServiceRolePolicy` para permitir que la función vinculada al servicio entregue los resultados de la evaluación a AWS Config.	29 de junio de 2021

El recurso nuevo y actualizado detalla los objetos en el ASFF	Se agregaron nuevos objetos de detalles de recursos para los clústeres de ECS y las definiciones de tareas de ECS. Se actualizó el objeto de instancia EC2 para enumerar las interfaces de red asociadas. Se agregó el ID de certificado del cliente para las etapas V2 de API Gateway. Se agregó la configuración del ciclo de vida de los buckets S3.	24 de junio de 2021
Se actualizó el cálculo de los estados de control agregados y las puntuaciones de seguridad estándar	El CSPM de Security Hub ahora calcula el estado de control general y la puntuació n de seguridad estándar cada 24 horas. En el caso de las cuentas de administrador, la puntuación ahora refleja si cada control está activado o desactivado para cada cuenta.	23 de junio de 2021
Información actualizada sobre la gestión que realiza el CSPM de Security Hub de las cuentas suspendidas	Se agregó información sobre cómo el CSPM de Security Hub gestiona las cuentas suspendidas en AWS.	23 de junio de 2021

Se agregaron pestañas para mostrar los controles habilitados y deshabilitados de la cuenta de administrador individual	En el caso de la cuenta de administrador, las pestañas principales de la página de detalles estándar contienen información agregada de todas las cuentas. En las nuevas pestañas Habilitada para esta cuenta y Deshabilitada para esta cuenta se muestran las cuentas que están habilitadas o deshabilitadas para la cuenta de administrador individual.	23 de junio de 2021
Se agregó `java8.al2` a los parámetros de `Lambda.2`	En el estándar AWS Fundational Security Best Practices, se agregó `java8.al2` a los tiempos de ejecución compatibles con el control `Lambda.2`	8 de junio de 2021
Nuevas integraciones con Cyber Investigator MicroFocus ArcSight y NETSCOUT	Se agregaron integraciones con Cyber Investigator MicroFocus ArcSight y NETSCOUT. MicroFocus ArcSight recibe los hallazgos del CSPM de Security Hub. NETSCOUT Cyber Investigator envía resultados al CSPM de Security Hub.	7 de junio de 2021

Se agregaron detalles para `AWSSecurityHubServiceRolePolicy`	Se actualizó la sección de políticas administradas para incluir detalles sobre la política administrada existente `AWSSecurityHubServiceRolePolicy`, que utiliza el rol vinculado al servicio de CSPM de Security Hub.	4 de junio de 2021
Nueva integración con Jira Service Management	El conector AWS de administración de servicios de Jira envía las conclusiones a Jira y las usa para crear problemas en Jira. Cuando se actualizan las incidencias de Jira, los resultados correspondientes en el CSPM de Security Hub también se actualizan.	26 de mayo de 2021
Se actualizó la lista de controles compatibles para la región de Asia-Pacífico (Osaka)	Se han actualizado los estándares CIS AWS Foundations y PCI DSS (Payment Card Industry Data Security Standard) para indicar los controles que no son compatibles en Asia Pacífico (Osaka).	21 de mayo de 2021
Nueva integración con Sysdig Secure para la nube	Se agregó una integración con Sysdig Secure para la nube. La integración envía resultados al CSPM de Security Hub.	14 de mayo de 2021

Se agregaron controles al estándar AWS Fundational Security Best Practices	Se agregaron nuevos controles para Amazon API Gateway AWS CloudTrail (APIGateway.2 CloudTrail.4 y APIGateway.3 CloudTrai l.5), Amazon EC2 (EC2.15 y EC2.16), AWS Elastic Beanstalk (ElasticBeanstalk .1 y ElasticBeanstalk.2), AWS Lambda (Lambda.4), Amazon RDS (RDS.12—RDS.14), Amazon Redshift (Redshift.7), AWS Secrets Manager (SecretsManager.3 y SecretsManager.4). AWS WAF WAF.1	10 de mayo de 2021
Actualizaciones y controles de Amazon GuardDuty RDS	Se ha cambiado la gravedad de `GuardDuty.1` y `PCI.GuardDuty.1` de Media a Alta. Se agregó un `databaseEngines` parámetro a `RDS.8`.	4 de mayo de 2021
Se agregaron nuevos detalles de recursos al ASFF	En`Resources.Details` , se agregaron nuevos objetos de detalles de recursos para las ACL de red, las subredes y los entornos de Amazon EC2. AWS Elastic Beanstalk	3 de mayo de 2021

Se agregaron campos de consola para proporcionar valores de filtro para las reglas de Amazon EventBridge	Los nuevos patrones de filtro predefinidos para EventBridge las reglas de CSPM de Security Hub proporcionan campos de consola que puede usar para especificar valores de filtro.	30 de abril de 2021
Se agregó la integración con Explorer y AWS Systems Manager OpsCenter	Security Hub CSPM ahora admite una integración con Systems Manager Explorer y. OpsCenter La integración recibe resultados del CSPM de Security Hub y actualiza esos resultados en el CSPM de Security Hub.	26 de abril de 2021
Nuevo tipo de integraciones de productos	Un nuevo tipo de integración, `UPDATE_FINDINGS_IN_SECURITY_HUB`, indica que la integración de un producto actualiza los resultados que recibe del CSPM de Security Hub.	22 de abril de 2021
Se cambió “cuenta maestra” a “cuenta de administrador”	Se ha cambiado el término "cuenta maestra" por "cuenta de administrador". El término también se cambia en la consola del CSPM de Security Hub y la API.	22 de abril de 2021

Se actualizó APIGateway.1 para reemplazar HTTP por Websocket	Se actualizaron el título, la descripción y la corrección de. APIGateway.1 El control ahora comprueba el registro de ejecución de la API de Websocket en lugar del registro de ejecución de la API HTTP.	9 de abril de 2021
GuardDuty La integración de Amazon ahora es compatible en Beijing y Ningxia	La integración con Security Hub con CSPM ahora GuardDuty es compatible en las regiones de China (Beijing) y China (Ningxia).	5 de abril de 2021
Se agregó `nodejs14.x` a los tiempos de ejecución compatibles para el control Lambda.2	El Lambda.2 control del estándar Foundational Security Best Practices ahora es compatible con el `nodejs14.x` tiempo de ejecución.	30 de marzo de 2021
El CSPM de Security Hub se lanzó en Asia-Pacífico (Osaka)	El CSPM de Security Hub ya está disponible en la región de Asia-Pacífico (Osaka).	29 de marzo de 2021
Se agregaron campos de búsqueda de proveedores a la de resultado de detalles	En el panel de detalles de búsqueda, la nueva sección Búsqueda de campos de proveedores contiene los valores de confianza, criticida d, resultados relacionados, gravedad y tipos de proveedor .	24 de marzo de 2021

Se agregó la opción de recibir resultados confidenciales de Amazon Macie	La integración con Macie ahora se puede configura r para enviar resultados confidenciales al CSPM de Security Hub.	23 de marzo de 2021
Pasando a para la administr ación de AWS Organizations cuentas	Para los clientes que ya tienen una cuenta de administrador con cuentas de miembros, se agregó nueva información sobre cómo pasar de administr ar cuentas mediante invitació n a administrar cuentas mediante Organizations.	22 de marzo de 2021
Nuevos objetos en el ASFF para obtener información sobre la configuración de bloques de acceso público de Amazon S3	En `Resources` , un nuevo tipo de `AwsS3Acco untPublicAccessBlo ck` recurso y un objeto de detalles proporcionan información sobre la configura ción del bloque de acceso público de Amazon S3 para las cuentas. En el objeto de detalles del recurso `AwsS3Bucket` , el objeto `PublicAccessBlockC onfiguration` proporcio na la configuración del bloque de acceso público para el bucket S3.	18 de marzo de 2021

Nuevo objeto en el ASFF que permite buscar proveedores para actualizar campos específicos	El nuevo objeto `FindingProviderFields` del ASFF se utiliza en `BatchImportFindings` para proporcionar valores para `Confidence`, `Criticality`, `RelatedFindings`, `Severity`, y `Types`. Los campos originales solo deben actualizarse utilizando `BatchUpdateFindings`.	18 de marzo de 2021
Nuevo `DataClassification` objeto para los recursos en el ASFF	El nuevo `Resources.DataClassification` objeto del ASFF se utiliza para proporcionar información sobre los datos confidenciales que se detectaron en el recurso.	18 de marzo de 2021
Valor `CONFIG_RETURNS_NOT_APPLICABLE` agregado a los códigos de estado de cumplimiento disponibles	Para el estado de cumplimiento `NOT_AVAILABLE`, se eliminó el código de motivo `RESOURCE_NO_LONGER_EXISTS` y se agregó el código de motivo `CONFIG_RETURNS_NOT_APPLICABLE`.	16 de marzo de 2021

Nueva política gestionada para la integración con AWS Organizations	Una nueva política administrada, `AWSSecurityHubOrganizationsAccess`, proporciona los permisos de Organizations que necesitan la cuenta de administración de la organización y la cuenta delegada de administrador del CSPM de Security Hub.	15 de marzo de 2021
La información sobre las políticas gestionadas y las funciones vinculadas a los servicios se trasladó al capítulo de seguridad	La información sobre las políticas gestionadas se revisa y amplía. Tanto la información sobre las políticas gestionadas como la información sobre las funciones vinculadas a los servicios se han trasladado al capítulo de seguridad.	15 de marzo de 2021
Se revisó la gravedad de los controles CIS 1.1 y CIS 3.1 – CIS 3.14	La gravedad de los controles CIS 1.1 y CIS 3.1 – CIS 3.14 se cambia a Baja.	3 de marzo de 2021
Se eliminó el RDS.11 control	Se ha eliminado el RDS.11 control del estándar Fundational Security Best Practices.	3 de marzo de 2021
Integración actualizada para Turbot	La integración de Turbot se actualizó para enviar y recibir resultados.	26 de febrero de 2021

Se agregaron controles al estándar de prácticas recomendadas de seguridad fundamentales	Se agregaron nuevos controles para Amazon API Gateway (APIGateway.1), Amazon EC2 (EC2.9 and EC2.10), Amazon Elastic File System (EFS.2), Amazon OpenSearch Service (ES.2 and ES.3), Elastic Load Balancing (ELB.6) y AWS Key Management Service (AWS KMS) (KMS.3).	11 de febrero de 2021
Se agregó un filtro `ProductArn` opcional a la `DescribeProducts` API	La operación `DescribeProducts` de API ahora incluye un parámetro `ProductArn` opcional. El parámetro `ProductArn` se utiliza para identificar la integración específica de producto para la que se devolverán los detalles.	3 de febrero de 2021
Nueva integración con Antivirus para Amazon S3 de Cloud Storage Security	La integración con Antivirus para Amazon S3 envía los resultados del análisis de virus al CSPM de Security Hub como resultados.	27 de enero de 2021

Se actualizó el proceso de cálculo de la puntuación de seguridad de las cuentas de administrador	En el caso de una cuenta de administrador, el CSPM de Security Hub utiliza un proceso independiente para calcular la puntuación de seguridad. El nuevo proceso garantiza que la puntuación incluya controles que estén habilitados para las cuentas de miembros, pero deshabili tados para la cuenta de administrador.	21 de enero de 2021
Nuevos campos y objetos en el ASFF	Se agregó un nuevo `Action` objeto para rastrear las acciones que se produjero n contra un recurso. Se agregaron campos al `AwsEc2NetworkInter face` objeto para rastrear los nombres de DNS y las direcciones IP. Se agregó un objeto `AwsSsmPat chCompliance` nuevo a los detalles del recurso.	21 de enero de 2021

Se agregaron controles al estándar de prácticas recomendadas de seguridad fundamentales	Se han añadido nuevos controles para Amazon CloudFront (CloudFront.1 mediante CloudFront.4), Amazon DynamoDB (DynamoDB.1 mediante DynamoDB.3), Elastic Load Balancing (ELB.3 mediante ELB.5), Amazon RDS (RDS.9mediante RDS.11), Amazon Redshift (Redshift.1 mediante Redshift.3 y Redshift.6) y Amazon SNS (). SNS.1	15 de enero de 2021
El estado del flujo de trabajo se restablece en función del estado del registro o del estado de cumplimiento	El CSPM de Security Hub restablece automáticamente el estado del flujo de trabajo de `NOTIFIED` o `RESOLVED` a `NEW` si un resultado archivado se activa, o si el estado de cumplimiento de un resultado cambia de `PASSED` a, ya sea, `FAILED`, `WARNING` o `NOT_AVAILABLE` . Estos cambios indican que es necesaria una investigación adicional.	7 de enero de 2021
Se agregó `ProductFields` información para los resultados basados en el control	Para los hallazgos generados a partir de los controles, se agregó información sobre el contenido del `ProductFields` objeto en el formato de búsqueda de AWS seguridad (ASFF).	29 de diciembre de 2020

Actualizaciones del hallazgo gestionado	Se ha cambiado el título de hallazgo 5. Se agregó un nuevo hallazgo, 32, que comprueba si hay usuarios de IAM con actividades sospechosas.	22 de diciembre de 2020
Actualizaciones IAM.7 y controles Lambda.1	En el estándar AWS Fundation al Security Best Practices, se actualizaron los parámetros para IAM.7. Se actualizaron el título y la descripción de Lambda.1.	22 de diciembre de 2020
Integración ampliada con ServiceNow ITSM	La integración con ServiceNo w ITSM permite a los usuarios crear automáticamente incidentes o problemas cuando reciben un hallazgo de CSPM de Security Hub. Cuando se actualizan estos incidentes o problemas, también se actualizan los resultados en el CSPM de Security Hub.	11 de diciembre de 2020
Nueva integración con Audit Manager AWS	Security Hub CSPM ahora ofrece una integración con AWS Audit Manager. La integración permite a Audit Manager recibir resultados basados en controles de parte del CSPM de Security Hub.	8 de diciembre de 2020

Nueva integración con Aqua Security Kube-bench	Security Hub CSPM agregó una integración con Aqua Security. Kube-bench La integración envía resultados al CSPM de Security Hub.	24 de noviembre de 2020
Cloud Custodian ya está disponible en las regiones de China	La integración con Cloud Custodian ya está disponibl e en las regiones de China (Pekín) y China (Ningxia).	24 de noviembre de 2020
`BatchImportFindings` ahora se puede usar para actualizar campos adicionales	Anteriormente, no se podía utilizar `BatchImportFindings` para actualizar los campos `Confidence`, `Criticality`, `RelatedFindings`, `Severity`, y `Types`. Ahora, si estos campos no se han actualizado con `BatchUpdateFindings`, se pueden actualizar con `BatchImportFindings`. Una vez actualizados por `BatchUpdateFindings`, no se pueden actualizar por `BatchImportFindings`.	24 de noviembre de 2020

Security Hub CSPM ahora está integrado con AWS Organizations	Los clientes ahora pueden administrar las cuentas de los miembros mediante la configuración de sus cuentas de Organizations (Organizaciones). La cuenta de administración de la organización designa la cuenta de administrador del CSPM de Security Hub, quien determina qué cuentas de organización habilitar en el CSPM de Security Hub. El proceso de invitación manual se puede seguir utilizand o para las cuentas que no forman parte de una organizac ión.	23 de noviembre de 2020
Se ha eliminado el formato de lista de resultados independi ente para los controles de gran volumen	La lista de resultados de un control ya no utiliza el formato de página Resultado s cuando hay un gran número de resultados.	19 de noviembre de 2020
Integraciones de terceros nuevas y actualizadas	Security Hub CSPM ahora admite integraciones con cloudtamer.io, 3CoreSec, Prowler y Kubernetes Security. StackRox IBM QRadar ya no envía los resultados. Solo recibe los resultados.	30 de octubre de 2020

Se agregó la opción de descargar la lista de resultados desde la página de detalles del control.	En la página de detalles del control, hay una nueva opción de Descargar que permite descargar la lista de resultados en un archivo.csv. La lista descargada respeta todos los filtros que estén en la lista. Si seleccionó resultados específicos, la lista descargada solo incluye esos resultados.	26 de octubre de 2020
Se agregó la opción de descargar la lista de controles desde la página de detalles estándar.	En la página de detalles estándar, hay una nueva opción de Descargar que permite descargar la lista de controles a un archivo.csv. La lista descargada respeta todos los filtros que estén en la lista. Si ha seleccionado un control específico, la lista descargada solo incluye ese control.	26 de octubre de 2020
Integraciones de socios nuevas y actualizadas	Security Hub CSPM ahora está integrado con ThreatModeler. Se han actualizado las siguientes integraciones de socios para que reflejen los nuevos nombres de sus productos. Twistlock Enterprise Edition ahora es Palo Alto Networks - Prisma Cloud Compute. También de Palo Alto Networks, Demisto ahora es Cortex XSOAR y Redlock ahora es Prisma Cloud Enterprise.	23 de octubre de 2020

Se lanzó el CSPM de Security Hub en China (Pekín) y China (Ningxia)	El CSPM de Security Hub ya está disponible en las regiones de China (Pekín) y China (Ningxia).	21 de octubre de 2020
Formato revisado para los atributos del ASFF y las integraciones de terceros	Las listas de atributos del ASFF y las integraciones de socios ahora utilizan un formato basado en listas en lugar de tablas. La sintaxis, los atributos y la taxonomía de tipos del ASFF se encuentran ahora en temas separados.	15 de octubre de 2020
Página de detalles estándar rediseñada	La página de detalles estándar de un estándar activado ahora muestra una lista de controles en pestañas. Las pestañas filtran la lista de controles en función del estado del control.	7 de octubre de 2020
Se reemplazaron CloudWatch los eventos por EventBridge	Se reemplazaron las referencias a Amazon CloudWatch Events por Amazon EventBridge.	1 de octubre de 2020
Nuevas integraciones con Blue Hexagon para AWS, Alcide, KAudit y Palo Alto Networks. VM-Series	Security Hub CSPM ahora está integrado con Blue Hexagon for AWS, Alcide KAudit y Palo Alto Networks. VM-Series Blue Hexagon for AWS y kAudit envían los resultados a Security Hub CSPM. VM-Series recibe las conclusiones del CSPM de Security Hub.	30 de septiembre de 2020

El recurso nuevo y actualizado detalla los objetos en el ASFF	Se agregaron nuevos `Resources.Details` objetos para `AwsApiGatewayRestApi`, `AwsApiGatewayStage`, `AwsApiGatewayV2Api`, `AwsApiGatewayV2Stage`, `AwsCertificateManagerCertificate`, `AwsElbLoadBalancer`, `AwsIamGroup`, y `AwsRedshiftCluster`. Se agregaron detalles a los objetos `AwsCloudFrontDistribution`, `AwsIamRole` y `AwsIamAccessKey`.	30 de septiembre de 2020
Nuevo `ResourceRole` atributo para los recursos en el ASFF para rastrear si un recurso es un actor o un objetivo.	El `ResourceRole` atributo de los recursos indica si el recurso es el objetivo de la actividad de búsqueda o el autor de la actividad de búsqueda. Los valores válidos son `ACTOR` y `TARGET`.	30 de septiembre de 2020

Se agregó el administrador de AWS Systems Manager parches a las integraciones de servicios disponibles AWS	AWS Systems Manager El administrador de parches ahora está integrado con Security Hub CSPM. El Administrador de parches envía resultados al CSPM de Security Hub cuando las instancias de la flota de un cliente dejan de cumplir su estándar de cumplimiento de parches.	22 de septiembre de 2020
Se agregaron nuevos controles al estándar AWS Fundational Security Best Practices	Se han añadido nuevos controles para los siguiente s servicios: Amazon EC2 (EC2.7 y EC2.8), Amazon EMR (EMR.1), IAM (IAM.8), Amazon RDS (RDS.4 hasta RDS.8), Amazon S3 () y (yS3.6). AWS Secrets Manager SecretsManager.1 SecretsManager.2	15 de septiembre de 2020
Nuevas claves de contexto para la política de IAM para controlar el acceso a los `BatchUpdateFindings` campos	Las políticas de IAM ahora se pueden configurar para restringir el acceso a los campos y a sus valores durante su uso `BatchUpdateFindings` .	10 de septiembre de 2020
Acceso ampliado a `BatchUpdateFindings` las cuentas de los miembros	Por defecto, las cuentas de miembros ahora tienen el mismo acceso a `BatchUpdateFindings` que las cuentas de administrador.	10 de septiembre de 2020

Nuevos controles incluidos en el estándar fundamental AWS KMS de mejores prácticas de seguridad	Se agregaron dos nuevos controles (KMS.1 y KMS.2) al estándar fundamental de mejores prácticas de seguridad. Los nuevos controles comprueban si las políticas de IAM restringen el acceso a las acciones de AWS KMS descifrado.	9 de septiembre de 2020
Se eliminaron los resultados de los controles a nivel de cuenta	El CSPM de Security Hub ya no genera resultados a nivel de cuenta para un control. Solo se generan resultados a nivel de recursos.	1 de septiembre de 2020
Nuevo PatchSummary objeto en el ASFF	Se agregó el `PatchSummary` objeto al ASFF. El `PatchSummary` objeto proporciona información sobre el cumplimiento de los parches de un recurso en relación con un estándar de cumplimiento seleccionado.	1 de septiembre de 2020

Página de detalles de control rediseñada	Se ha rediseñado la página de detalles de los controles . La lista de búsqueda de controles incluye pestañas que permiten filtrar rápidamente la lista en función del estado de cumplimiento. También puede ver rápidamente los resultado s excluidos. Cada entrada proporciona acceso a detalles adicionales sobre el recurso de búsqueda, la AWS Config regla y las notas de búsqueda.	28 de agosto de 2020
Nuevas opciones de filtro para los resultados	Para buscar filtros, puede usar el filtro no es para buscar resultados en los que el valor de un campo no sea igual al valor del filtro. Puede utilizar el campo no empieza por para encontrar resultados en los que un valor de campo no comience por el valor de filtro especificado.	28 de agosto de 2020

El nuevo recurso detalla los objetos en el ASFF	Se agregaron nuevos `Resources.Details` objetos para los siguientes tipos de recursos: `AwsDynamoDbTable` , `AwsEc2Eip` , `AwsIamPolicy` , `AwsIamUser` , `AwsRdsDbCluster` , `AwsRdsDbClusterSnapshot` , `AwsRdsDbSnapshot` , `AwsSecretsManagerSecret`	18 de agosto de 2020
Nueva integración con RSA Archer	El CSPM de Security Hub ahora está integrado con RSA Archer. RSA Archer recibe resultados del CSPM de Security Hub.	18 de agosto de 2020
Nuevo campo de descripción para AwsKmsKey	Se agregó un `Description` campo al `AwsKmsKey` objeto situado abajo de `Resources.Details` .	18 de agosto de 2020
Se agregaron campos a AwsRdsDbInstance	Se agregaron varios atributos al `AwsRdsDbInstance` objeto que se encuentra abajo de `Resources.Details` .	18 de agosto de 2020

Se actualizó la forma en la que el CSPM de Security Hub determina el estado general de un control	En el caso de los controles que no encuentran resultados, el estado es Sin datos en lugar de Desconocido. El estado del control incluye los resultados a nivel de cuenta y a nivel de recursos. El estado de control no utiliza el estado del flujo de trabajo de los resultado s, excepto para ignorar los resultados excluidos.	13 de agosto de 2020
Se actualizó la forma en que el CSPM de Security Hub calcula la puntuación de seguridad de un estándar	Al calcular la puntuación de seguridad de un estándar, el CSPM de Security Hub ahora ignora los controles con el estado Sin datos. La puntuación de seguridad es la proporción entre los controles aprobados y los controles activados, excluyendo los controles sin datos.	13 de agosto de 2020
Nueva opción para habilitar automáticamente nuevos controles en los estándares habilitados	Se agregó una opción a Configuración para habilitar automáticamente los nuevos controles en los estándare s que estén habilitados. También puede utilizar la operación de la API `UpdateSecurityHubConfiguration` para configurar esta opción.	31 de julio de 2020

Nuevos controles para el estándar de Payment Card Industry Data Security Standard (PCI DSS)	Se agregaron nuevos controles al estándar PCI DSS. Los identificadores de los nuevos controles son PCI.DMS.1 PCI.EC2.5 , PCI.EC2.6, PCI.ELBV2.1, PCI.GuardDuty.1, PCI.IAM.7 PCI.IAM.8, PCI.S3.5, PCI.S3.6, PCI.SageMaker.1 PCI.SSM.2, y PCI.SSM.3.	29 de julio de 2020
Controles nuevos y actualizados para el estándar de prácticas recomendadas de seguridad fundamentales	Se agregaron nuevos controles al estándar fundamental de mejores prácticas de seguridad. Los identificadores de los nuevos controles son AutoScaling.1, DMS.1, EC2.4 EC2.6 S3.5, y. SSM.3 Se actualizó el título del `daysToExpiration` parámetro ACM.1 y se cambió su valor a 30.	29 de julio de 2020
Nuevo `Vulnerabilities` objeto en el ASFF	Se agregó el objeto `Vulnerabilities` , que proporciona información sobre las vulnerabilidades asociadas al resultado.	1 de julio de 2020
Nuevos objetos `Resource.Details` en el ASFF para grupos de escalado automático, volúmenes de EC2 y EC2 VPC	Se agregaron los objetos `AwsAutoScalingAutoScalingGroup` , `AWSEc2Volume` , y `AwsEc2Vpc` a `Resource.Details` .	1 de julio de 2020

Nuevo `NetworkPath` objeto en el ASFF	Se agregó el `NetworkPath` objeto, que proporciona información sobre una ruta de red relacionada con el resultado.	1 de julio de 2020
Resuelva automáticamente los resultados cuando `Compliance.Status` es `PASSED`	Para los resultados de los controles, si `Compliance.Status` es `PASSED`, entonces el CSPM de Security Hub establece automáticamente `Workflow.Status` en `RESOLVED`.	24 de junio de 2020
AWS Command Line Interface ejemplos	Se agregaron ejemplos y AWS CLI sintaxis para varias tareas de CSPM de Security Hub. Incluye habilitar el CSPM de Security Hub; administrar los resultados; administrar los estándares y los controles; administrar las integraciones de productos; y desactivar el CSPM de Security Hub.	24 de junio de 2020
Nuevo `Severity.Original` atributo en el ASFF	Se agregó el atributo `Severity.Original`, que es la gravedad original del proveedor de resultados. Esto reemplaza al atributo `Severity.Product` que ha quedado obsoleto.	20 de mayo de 2020

Nuevo `Compliance.StatusReasons` objeto en el ASFF para obtener detalles sobre el estado de un control	Se agregó el objeto `Compliance.StatusReasons`, que proporciona contexto adicional para el estado actual de un control.	20 de mayo de 2020
Nuevo estándar AWS fundamental de mejores prácticas de seguridad	Se agregó el nuevo estándar AWS Fundational Security Best Practices, que consiste en un conjunto de controles que detectan si las cuentas y los recursos desplegados se desvían de las prácticas recomendadas de seguridad.	22 de abril de 2020
Nueva opción de consola para actualizar el estado de flujo de trabajo para un resultado	Se agregó información sobre el uso de la consola o la API de Security Hub para establecer el estado de flujo de trabajo para los hallazgos.	16 de abril de 2020
Nueva `BatchUpdateFindings` API para actualizaciones de cliente según los resultados	Se agregó información sobre el uso de `BatchUpdateFindings` para actualizar información relacionada con el proceso de investigación de un hallazgo. `BatchUpdateFindings` reemplaza a `UpdateFindings`, que está obsoleto.	16 de abril de 2020

Actualizaciones del formato de búsqueda AWS de seguridad (ASFF)	Se agregaron varios tipos de recursos nuevos. Se agregó un nuevo atributo `Label` al objeto `Severity`. `Label` está destinado a reemplaza r el campo `Normalized` . Se agregó un nuevo objeto `Workflow` para realizar un seguimiento del proceso de una investigación sobre un hallazgo. `Workflow` contiene un atributo `Status`, que reemplaza el atributo `Workflowstate` existente.	12 de marzo de 2020
Actualizaciones a la página Integraciones	Actualizado para reflejar los cambios realizados en la página Integrations (Integrac iones). Para cada integraci ón, la página muestra ahora la categoría de integraci ón y si cada integración envía o recibe resultados del CSPM de Security Hub. También proporciona los pasos específicos necesarios para habilitar cada integración.	26 de febrero de 2020
Nuevas integraciones de productos de terceros	Se agregaron las siguientes integraciones de productos nuevas: Cloud Custodian , FireEye Helix, Forcepoin t CASB, Forcepoint DLP, Forcepoint NGFW, Rackspace Cloud Native Security y Cognito Detect. Vectra.ai	21 de febrero de 2020

Nuevo estándar de seguridad para el Payment Card Industry Data Security Standard (PCI DSS)	Se agregó el estándar de seguridad del CSPM de Security Hub correspondiente al estándar de seguridad de datos para la industria de tarjetas de pago (PCI DSS). Cuando este estándar está habilitado, el CSPM de Security Hub realiza comprobaciones automatiz adas de los controles relacionados con los requisitos de PCI DSS.	13 de febrero de 2020
AWS Actualizaciones del formato de búsqueda de seguridad (ASFF)	Se agregó un campo para los requisitos relacionados para los controles de estándares. Se agregaron nuevos tipos de recursos y nuevos detalles de recursos. El ASFF ahora también le permite proporcio nar hasta 32 recursos.	5 de febrero de 2020
Nueva opción para desactiva r los controles estándar de seguridad individuales	Se agregó información acerca de cómo controlar si cada control del estándar de seguridad individual está habilitado.	15 de enero de 2020
Actualizaciones a los conceptos del CSPM de Security Hub	Se actualizaron algunas descripciones y se agregaron nuevos términos a Conceptos del CSPM de Security Hub.	21 de septiembre de 2019

AWS Versión de disponibilidad general de Security Hub CSPM	Actualizaciones de contenido para reflejar las mejoras realizadas al CSPM de Security Hub durante el período de versión beta.	25 de junio de 2019
Se agregaron pasos de corrección para las comprobaciones de CIS Foundations AWS	Se agregaron pasos correctivos a los estándares de seguridad compatibles con AWS Security Hub CSPM.	15 de abril de 2019
versión beta de Security Hub AWS CSPM	Se publicó la versión preliminar de la Guía del usuario del CSPM de AWS Security Hub.	18 de noviembre de 2018

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.