Entwicklerhandbuch

AWS Global Accelerator

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

AWS Global Accelerator: Entwicklerhandbuch

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

Die Marken und Handelsmarken von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, die geeignet ist, Kunden irrezuführen oder Amazon in irgendeiner Weise herabzusetzen oder zu diskreditieren. Alle anderen Marken, die nicht Eigentum von Amazon sind, sind Eigentum ihrer jeweiligen Inhaber, die mit Amazon verbunden oder nicht verbunden oder von Amazon gesponsert oder nicht gesponsert sein können.

Table of Contents

Was ist AWS Global Accelerator? ... 1
Komponenten ... 2
Funktionsweise ... 5
Leerlauf-Timeout ... 7
Statische IP-Adressen ... 7
Verkehrszifferblätter und Endpunktgewichte ... 8
Zustandsprüfungen ... 10
-Accelerator-Arten ... 11
Standort- und IP-Adressbereiche von -Edge-Servern ... 12
Anwendungsfälle ... 12
Speed Comparison Tool ... 14
Erste Schritte ... 14
Markieren ... 16
Tagging-Unterstützung in Global Accelerator ... 17
Hinzufügen, Bearbeiten und Löschen von Tags in Global Accelerator ... 17
Preise ... 18
Erste Schritte ... 19
Erste Schritte mit einem Standard-Accelerator ... 19
Bevor Sie beginnen ... 20
Schritt 1: Erstellen eines Accelerators ... 21
Schritt 2: Hinzufügen von Listener ... 21
Schritt 3: Hinzufügen von Endpunktgruppen ... 22
Schritt 4: Hinzufügen von Endpunkten ... 23
Schritt 5: Testen Sie Ihren Accelerator ... 24
Schritt 6 (optional): Löschen des Accelerators ... 24
Erste Schritte mit einem benutzerdefinierten Routing-Accelerator ... 25
Bevor Sie beginnen ... 26
Schritt 1: Erstellen eines benutzerdefinierten Routing-Accelerators ... 26
Schritt 2: Hinzufügen von Listener ... 27
Schritt 3: Hinzufügen von Endpunktgruppen ... 28
Schritt 4: Hinzufügen von VPC -Subnetzendpunkten ... 29
Schritt 5 (optional): Löschen des Accelerators ... 30
Aktionen ... 32
Arbeiten mit Standard-Beschleunigern ... 35

Standard-Acceleratoren ... 36
Erstellen oder Aktualisieren eines Standard-Beschleunigers ... 37
Löscht eines Accelerators ... 38
Anzeigen Ihrer Beschleuniger ... 39
Hinzufügen eines Accelerators ... 39
Verwenden von globalen statischen IP-Adressen anstelle von regionalen statischen IP-Adressen ... 41
Listener für Standard-Beschleuniger ... 42
Hinzufügen, Bearbeiten oder Entfernen eines Standardlisteners ... 42
Client-Affinität ... 44
Endpunktgruppen für Standardbeschleuniger ... 44
Hinzufügen, Bearbeiten oder Entfernen einer Standard-Endpunktgruppe ... 45
Verwenden von Verkehrsziffern ... 47
Port-Überschreibungen ... 48
Zustandsprüfungsoptionen ... 50
Endpunkte für Standardbeschleuniger ... 52
Hinzufügen, Bearbeiten oder Entfernen eines Standard-Endpunkts ... 53
Endpoint Gewichtungen ... 56
Hinzufügen von Endpunkten mit Client-IP-Adresserhaltung ... 58
Übergänge von Endpunkten zur Verwendung der Client-IP-Adresserhaltung ... 59
Arbeiten mit benutzerdefinierten Routing-Beschleunigern ... 63
Funktionsweise von benutzerdefinierten Routing-Beschleunigern ... 64
Beispiel für die Funktionsweise von benutzerdefiniertem Routing in Global Accelerator ... 66
Richtlinien und Einschränkungen für benutzerdefinierte Routing-Beschleuniger ... 69
Benutzerdefinierte Routing-Acceleratoren ... 71
Erstellen oder Aktualisieren eines benutzerdefinierten Routing-Accelerators ... 73
Anzeigen Ihrer benutzerdefinierten Routing-Beschleuniger ... 74
Löschen eines benutzerdefinierten Routing-Beschleunigers ... 74
Listener für benutzerdefinierte Routing-Beschleuniger ... 75
Hinzufügen, Bearbeiten oder Entfernen eines benutzerdefinierten Routinglisteners ... 76
Endpunktgruppen für benutzerdefinierte Routing-Beschleuniger ... 77
Hinzufügen, Bearbeiten oder Entfernen einer Endpunktgruppe ... 78
VPC -Subnetzendpunkte für benutzerdefinierte Routing-Beschleuniger ... 80
Hinzufügen, Bearbeiten oder Entfernen eines VPC -Subnetzendpunkts ... 81
DNS-Adressierung und benutzerdefinierte Domänen ... 84
Support für DNS-Adressierung in Global Accelerator ... 84

Weiterleiten von benutzerdefinierten Domain-Traffic an Ihren Accelerator 85
Bring Your Own IP Addresses 85
Requirements 87
Autorisierung des IP-Adressbereichs 87
Bereitstellen des Adressbereichs für die Verwendung mit AWS Global Accelerator 91
Veröffentlichen des Adressbereichs über AWS 92
Aufheben der Bereitstellung des Adressbereichs 94
Erstellen eines Accelerators 94
Die Client-IP-Adressen beibehalten 96
So aktivieren Sie die Erhaltung der Client-IP-Adresse 97
Die Vorteile der Client-IP-Adresse 98
Wie die Client-IP-Adresse erhalten bleibt 99
Bewährte Methoden für die Erhaltung von Client-IP-Adressen 100
Unterstützte AWS Regionen für die Erhaltung der Client-IP-Adresse 102
Protokollierung und Überwachung 104
Flow-Protokolle 104
Veröffentlichung auf Amazon S3 105
Zeitplan der Dateizustellung von Protokolldateien 110
Syntax des Flow-Protokolldat 111
Überwachung von CloudWatch Überwachung 114
Metriken für Global Accelerator — 115
Metrikdimensionen für Acceleratoren 116
Statistiken für Global Accelerator Metriken 118
Anzeigen von CloudWatch Metriken für Ihre Accelerators 119
CloudTrail Protokollierung 121
Informationen zu Global Accelerator 122
Grundlagen der Global Accelerator-Protokolldateieinträge 123
Sicherheit 132
Identitäts- und Zugriffsverwaltung 133
Konzepte und Begriffe 133
Erforderliche Berechtigungen für den Konsolenzugriff, die Authentifizierungsverwaltung und die Zugriffssteuerung 136
Funktionsweise von Global Accelerator mit IAM 140
Fehlerbehebung bei der Authentifizierung und Zugriffskontrolle 142
Tagbasierte Richtlinien 143
Serviceverknüpfte Rolle für Global Accelerator 145

Übersicht über den Zugriff und die Authentifizierung 150
Sichere VPC Verbindungen 175
Protokollierung und Überwachung 176
Compliance-Validierung 177
Ausfallsicherheit 178
Sicherheit der Infrastruktur 179
Kontingente 180
Allgemeine Kontingente 180
Kontingente für Endpunkte pro Endpunktgruppe 181
Zugehörige Kontingente 182
Ähnliche Informationen 183
AWS Global Accelerator Dokumentation 183
Supportanfragen 183
Tipps aus dem Amazon Web Services-Blog 184
Dokumentverlauf 185
AWS-Glossar 190
..... cxci

Was ist AWS Global Accelerator?

AWS Global Accelerator ist ein Service, in dem Sie-Acceleratorszur Verbesserung der Leistung Ihrer Anwendungen für lokale und globale Benutzer Je nach Art des -Accelerators können Sie zusätzliche Vorteile erzielen.

- Durch den Einsatz eines Standard-Accelerators können Sie die Verfügbarkeit Ihrer Internetanwendungen verbessern, die von einer globalen Zielgruppe verwendet werden. Mit einem Standardbeschleuniger leitet Global Accelerator Datenverkehr über das globale AWS Netzwerk an Endpunkte in der nächstgelegenen Region zum Client weiter.
- Mithilfe eines benutzerdefinierten Routingbeschleunigers können Sie einen oder mehrere Benutzer einem bestimmten Ziel unter vielen Zielen zuordnen.

Global Accelerator ist ein globaler Service, der Endpunkte in mehreren AWS Regionen unterstützt, die imAWS Regionentabelle.

Standardmäßig stellt Ihnen Global Accelerator zwei statische IP-Adressen zur Verfügung, die Sie Ihrem Accelerator zuordnen. Anstatt die von Global Accelerator bereitgestellten IP-Adressen zu verwenden, können Sie diese Einstiegspunkte als IPv4-Adressen aus Ihren eigenen IP-Adressbereichen konfigurieren, die Sie zu Global Accelerator bringen. Die statischen IP-Adressen stammen aus dem AWS Edge-Netzwerk.

> **Important**
>
> Die statischen IP-Adressen bleiben Ihrem Accelerator so lange zugewiesen, wie er existiert, auch wenn Sie den Accelerator deaktivieren und keinen Datenverkehr mehr annehmen oder weiterleiten. Allerdings, wenn Siedeleteeinen Beschleuniger verwenden, verlieren Sie die ihm zugewiesenen statischen IP-Adressen, sodass Sie den Datenverkehr nicht mehr mithilfe dieser Adressen weiterleiten können. Sie können IAM-Richtlinien wie tag-basierte Berechtigungen mit Global Accelerator verwenden, um die Benutzer einzuschränken, die über Berechtigungen zum Löschen eines Accelerators verfügen. Weitere Informationen finden Sie unter Tagbasierte Richtlinien.

Für Standardbeschleuniger verwendet Global Accelerator das globale AWS Netzwerk, um Datenverkehr an den optimalen regionalen Endpunkt zu leiten, basierend auf der Integrität, dem Clientstandort und den von Ihnen konfigurierten Richtlinien, wodurch die Verfügbarkeit Ihrer

Anwendungen erhöht wird. Endpunkte für Standardbeschleuniger können Network Load Balancers, Application Load Balancers, Amazon EC2 Instances oder Elastic IP-Adressen sein, die sich in einer AWS Region oder mehreren Regionen befinden. Der Dienst reagiert sofort auf Änderungen des Zustands oder der Konfiguration, um sicherzustellen, dass der Internetverkehr von Clients immer an gesunde Endpunkte weitergeleitet wird.

Benutzerdefinierte Routingbeschleuniger unterstützen nur VPC -Subnetz-Endpunkttypen (Virtual Private Cloud) und leiten den Datenverkehr an private IP-Adressen in diesem Subnetz weiter.

Eine Liste der AWS Regionen, in denen Global Accelerator und andere Services derzeit unterstützt werden, finden Sie unter derAWS Regionentabelle.

Themen

- AWS Global Accelerator Komponenten
- Funktionsweise von AWS Global Accelerator
- -Accelerator-Arten
- Standort- und IP-Adressbereiche von Global Accelerator-Edge-Servern
- AWS Global Accelerator
- AWS Global Accelerator
- Erste Schritte mit AWS Global Accelerator
- Taggen in AWS Global Accelerator
- AWS Global Accelerator

AWS Global Accelerator Komponenten

AWS Global Accelerator umfasst die folgenden Komponenten:

Statische IP-Adressen

Global Accelerator stellt Ihnen einen Satz von zwei statischen IP-Adressen zur Verfügung, die aus dem AWS Edge-Netzwerk stammen. Wenn Sie AWS (BYOIP) einen eigenen IP-Adressbereich für den Global Accelerator verwenden, können Sie stattdessen IP-Adressen aus Ihrem eigenen Pool zuweisen, um sie mit Ihrem Accelerator zu verwenden. Weitere Informationen finden Sie unter Bring Your Own IP Addresses (BYOIP) in AWS Global Accelerator.

Die IP-Adressen dienen als einzelne feste Einstiegspunkte für Ihre Clients. Wenn Sie bereits Elastic Load Balancing Load Balancers, Amazon EC2 Instances oder Elastic IP-Adressressourcen

für Ihre Anwendungen eingerichtet haben, können Sie diese einfach zu einem Standard-Accelerator in Global Accelerator hinzufügen. Dadurch kann Global Accelerator statische IP-Adressen für den Zugriff auf die Ressourcen verwenden.

Die statischen IP-Adressen bleiben Ihrem Accelerator so lange zugewiesen, wie er existiert, auch wenn Sie den Accelerator deaktivieren und keinen Datenverkehr mehr annehmen oder weiterleiten. Allerdings, wenn Siedeleteeinen Beschleuniger verwenden, verlieren Sie die ihm zugewiesenen statischen IP-Adressen, sodass Sie den Datenverkehr nicht mehr mithilfe dieser Adressen weiterleiten können. Sie können IAM-Richtlinien wie tag-basierte Berechtigungen mit Global Accelerator verwenden, um die Benutzer einzuschränken, die über Berechtigungen zum Löschen eines Accelerators verfügen. Weitere Informationen finden Sie unter Tagbasierte Richtlinien.

-Accelerator

Ein Beschleuniger leitet den Datenverkehr über das globale AWS Netzwerk an Endpunkte weiter, um die Leistung Ihrer Internetanwendungen zu verbessern. Jeder Beschleuniger enthält einen oder mehrere Zuhörer.

Es gibt zwei Arten von Beschleunigern:

- AStandard--Beschleuniger leitet Datenverkehr auf der Grundlage verschiedener Faktoren an den optimalen AWS Endpunkt, einschließlich des Standorts des Benutzers, der Integrität des Endpunkts und der von Ihnen konfigurierten Endpunktgewichte. Dadurch wird die Verfügbarkeit und Leistung Ihrer Anwendungen verbessert. Endpunkte können Network Load Balancers, Application Load Balancers, Amazon EC2 Instances oder Elastic IP-Adressen sein.
- ABenutzerdefinierte Weiterleitungermöglicht es Ihnen, mehrere Benutzer deterministisch an ein bestimmtes EC2-Ziel hinter Ihrem Accelerator weiterzuleiten, wie dies für einige Anwendungsfälle erforderlich ist. Dazu leiten Sie Benutzer zu einer eindeutigen IP-Adresse und einem Port auf Ihrem Accelerator, den Global Accelerator dem Ziel zugeordnet hat.

Weitere Informationen finden Sie unter -Accelerator-Arten.

DNS-Name

Jeder Global Accelerator weist einen standardmäßigen DNS-Namen (Domain Name System) ähnlich wie`a1234567890abcdef.awsglobalaccelerator.com`, die auf die statischen IP-Adressen verweist, die Ihnen Global Accelerator zuweist oder die Sie aus Ihrem eigenen IP-Adressbereich auswählen. Je nach Anwendungsfall können Sie die statischen IP-Adressen oder den DNS-Namen Ihres Beschleunigers verwenden, um Datenverkehr an Ihren Beschleuniger

weiterzuleiten, oder DNS-Einträge einrichten, um Datenverkehr mithilfe Ihres eigenen benutzerdefinierten Domänennamens weiterzuleiten.

Netzwerk-Zone

Eine Netzwerkzone bedient die statischen IP-Adressen für den Accelerator aus einem eindeutigen IP-Subnetz. Ähnlich wie bei einer AWS Availability Zone ist eine Netzwerkzone eine isolierte Einheit mit eigener physischer Infrastruktur. Wenn Sie einen Accelerator konfigurieren, weist Global Accelerator standardmäßig zwei IPv4-Adressen zu. Wenn eine IP-Adresse aus einer Netzwerkzone aufgrund der Blockierung von IP-Adressen durch bestimmte Client-Netzwerke oder Netzwerkunterbrechungen nicht verfügbar ist, können Clientanwendungen die fehlerfreie statische IP-Adresse aus der anderen isolierten Netzwerkzone erneut versuchen.

Listener

Ein Listener verarbeitet eingehende Verbindungen von Clients zu Global Accelerator, basierend auf dem Port (oder Portbereich) und Protokoll (oder Protokollen), die Sie konfigurieren. Ein Listener kann für TCP, UDP oder sowohl TCP als auch UDP Protokolle konfiguriert werden. Jedem Listener ist eine oder mehrere Endpunktgruppen zugeordnet, und der Datenverkehr wird an Endpunkte in einer der Gruppen weitergeleitet. Sie ordnen Endpunktgruppen Listener zu, indem Sie die Regionen angeben, an die Sie den Datenverkehr verteilen möchten. Bei einem Standardbeschleuniger wird der Datenverkehr an optimale Endpunkte innerhalb der Endpunktgruppen verteilt, die einem Listener zugeordnet sind.

Endpunktgruppe

Jede Endpunktgruppe ist einer bestimmten AWS Region zugeordnet. Endpunktgruppen enthalten einen oder mehrere Endpunkte in der Region. Mit einem Standardbeschleuniger können Sie den Prozentsatz des Datenverkehrs erhöhen oder reduzieren, der andernfalls an eine Endpunktgruppe weitergeleitet wird, indem Sie eine Einstellung anpassen, dieVerkehrsmittel-Wahl. Mit der Verkehrswahl können Sie auf einfache Weise Leistungstests oder blau/grüne Bereitstellungstests durchführen, z. B. für neue Versionen in verschiedenen AWS Regionen.

Endpunkt

Ein Endpunkt ist die Ressource, an die Global Accelerator Datenverkehr weiterleitet.

Endpunkte für Standardbeschleuniger können Network Load Balancers, Application Load Balancers, EC2-Instances oder Elastic IP-Adressen sein. Ein Application Load Balancer kann ein internetorientierter oder internetorientierter Endpunkt sein. Der Datenverkehr für Standardbeschleuniger wird basierend auf der Integrität des Endpunkts zusammen mit den von Ihnen ausgewählten Konfigurationsoptionen wie Endpunktgewichtungen an Endpunkte

weitergeleitet. Für jeden Endpunkt können Sie Gewichtungen konfigurieren. Dabei handelt es sich um Zahlen, mit denen Sie den Anteil des Datenverkehrs angeben können, der an den einzelnen Endpunkt weitergeleitet werden soll. Dies kann beispielsweise nützlich sein, um Leistungstests innerhalb einer Region durchzuführen.

Endpunkte für benutzerdefinierte Routing-Beschleuniger sind virtuelle Private Cloud-Subnetze (VPC -Subnetze) mit einer oder mehreren Amazon EC2 Instances, die die Ziele für den Datenverkehr sind.

Funktionsweise von AWS Global Accelerator

Die von AWS Global Accelerator bereitgestellten statischen IP-Adressen dienen als einzelne feste Einstiegspunkte für Ihre Kunden. Wenn Sie Ihren Accelerator mit Global Accelerator einrichten, ordnen Sie die statischen IP-Adressen regionalen Endpunkten in einer oder mehreren AWS Regionen zu. Bei Standard-Beschleunigern sind die Endpunkte Network Load Balancers, Application Load Balancers, Amazon EC2 Instances oder Elastic IP-Adressen. Bei benutzerdefinierten Routing-Beschleunigern sind Endpunkte virtuelle private Cloud-Subnetze (VPC) mit einer oder mehreren EC2-Instanzen. Die statischen IP-Adressen akzeptieren eingehenden Datenverkehr in das globale AWS Netzwerk von der Edge-Position, die Ihren Benutzern am nächsten liegt.

> **Note**
>
> Wenn Sie AWS (BYOIP) einen eigenen IP-Adressbereich verwenden, um sie mit Global Accelerator zu verwenden, können Sie stattdessen statische IP-Adressen aus Ihrem eigenen Pool zuweisen, um sie mit Ihrem Accelerator zu verwenden. Weitere Informationen finden Sie unter Bring Your Own IP Addresses (BYOIP) in AWS Global Accelerator.

Vom Edge-Standort aus wird der Datenverkehr für Ihre Anwendung basierend auf dem Typ des von Ihnen konfigurierten Beschleunigers weitergeleitet.

- Bei Standardbeschleunigern wird der Datenverkehr auf der Grundlage verschiedener Faktoren an den optimalen AWS Endpunkt weitergeleitet, einschließlich des Standorts des Benutzers, der Integrität des Endpunkts und der von Ihnen konfigurierten Endpunktgewichtungen.
- Bei benutzerdefinierten Routing-Beschleunigern wird jeder Client basierend auf der externen statischen IP-Adresse und dem von Ihnen bereitgestellten Listener-Port an eine bestimmte Amazon EC2 Instance und einen bestimmten Port in einem VPC -Subnetz weitergeleitet.

Der Datenverkehr verläuft über das gut überwachte, überlastungsfreie, redundante AWS Netzwerk bis zum Endpunkt. Durch die Maximierung der Datenverkehrszeit im AWS Netzwerk stellt Global Accelerator sicher, dass der Datenverkehr immer über den optimalen Netzwerkpfad geleitet wird.

Bei einigen Endpunkttypen (in einigen AWS Regionen), haben Sie die Möglichkeit, die Client-IP-Adresse beizubehalten und darauf zuzugreifen. Zwei Arten von Endpunkten können die Quell-IP-Adresse des Clients in eingehenden Paketen beibehalten: Application Load Balancers und Amazon EC2 Instances. Global Accelerator unterstützt keine Client-IP-Adresserhaltung für Network Load Balancer und Elastic IP-Adressenendpunkte. Endpunkte auf benutzerdefinierten Routingbeschleunigern haben immer die Client-IP-Adresse beibehalten.

Global Accelerator beendet TCP-Verbindungen von Clients an AWS Edge-Standorten und stellt fast gleichzeitig eine neue TCP-Verbindung mit Ihren Endpunkten her. Dies ermöglicht Clients schnellere Reaktionszeiten (geringere Latenz) und einen höheren Durchsatz.

In Standardbeschleunigern überwacht Global Accelerator kontinuierlich die Integrität aller Endpunkte und leitet den Datenverkehr sofort an einen anderen verfügbaren Endpunkt weiter, wenn festgestellt wird, dass ein aktiver Endpunkt fehlerhaft ist. Auf diese Weise können Sie eine Architektur mit hoher Verfügbarkeit für Ihre Anwendungen in AWS erstellen. Zustandsprüfungen werden nicht mit benutzerdefinierten Routingbeschleunigern verwendet, und es gibt kein Failover, da Sie das Ziel angeben, an das der Datenverkehr weitergeleitet werden soll.

Wenn Sie einen Accelerator hinzufügen, funktionieren Sicherheitsgruppen und AWS WAF Regeln, die Sie bereits konfiguriert haben, weiterhin wie vor dem Hinzufügen des Accelerators.

Wenn Sie eine präzise Kontrolle über Ihren globalen Datenverkehr wünschen, können Sie Gewichtungen für Ihre Endpunkte in einem Standardbeschleuniger konfigurieren. Sie können den Prozentsatz des Datenverkehrs zu einer bestimmten Endpunktgruppe auch erhöhen (nach oben wählen) oder verringern (nach unten fahren), z. B. für Leistungstests oder Stack-Upgrades.

Beachten Sie bei der Verwendung von Global Accelerator:

- AWS Direct Connect kündigt keine IP-Adresspräfixe für AWS Global Accelerator über eine öffentliche virtuelle Schnittstelle an. Es wird empfohlen, keine IP-Adressen anzukündigen, die Sie für die Kommunikation mit Global Accelerator über Ihre öffentliche virtuelle AWS Direct Connect Schnittstelle verwenden. Wenn Sie IP-Adressen ankündigen, die Sie für die Kommunikation mit Global Accelerator über Ihre öffentliche virtuelle AWS Direct Connect Schnittstelle verwenden, führt dies zu einem asymmetrischen Datenverkehr: Ihr Datenverkehr in Richtung Global Accelerator geht über das Internet zu Global Accelerator, aber der Datenverkehr wird zu Ihrem lokalen -Netzwerk über Ihre öffentliche virtuelle AWS Direct Connect Schnittstelle.

- Global Accelerator unterstützt das Hinzufügen einer Ressource, die zu einem anderen AWS Konto gehört, nicht als Endpunkt.

Themen

- Leerlauf-Timeout in AWS Global Accelerator
- Statische IP-Adressen in AWS Global Accelerator
- Verkehrsflussmanagement mit Verkehrszifferblättern und Endpunktgewichten
- Health sprüfungen für AWS Global Accelerator

Leerlauf-Timeout in AWS Global Accelerator

Bei AWS Global Accelerator wird ein Leerlauf-Timeout festgelegt, der für seine Verbindungen gilt. Wenn bis zum Ablauf des Leerlaufzeitlimits keine Daten versandt oder empfangen wurden, schließt Global Accelerator die Verbindung. Um sicherzustellen, dass die Verbindung am Leben bleibt, muss der Client oder der Endpunkt mindestens 1 Byte Daten senden, bevor der Zeitüberschreitungszeitraum im Leerlauf verstrichen ist.

Die Zeitüberschreitung im Leerlauf von Global Accelerator für eine Netzwerkverbindung hängt vom Verbindungstyp ab:

- Das Timeout beträgt 340 Sekunden für TCP-Verbindungen.
- Das Timeout beträgt 30 Sekunden für UDP-Verbindungen.

Global Accelerator leitet den Datenverkehr weiterhin an einen Endpunkt weiter, bis die Zeitüberschreitung im Leerlauf erreicht ist, selbst wenn der Endpunkt als fehlerhaft gekennzeichnet ist. Global Accelerator wählt bei Bedarf einen neuen Endpunkt nur dann aus, wenn eine neue Verbindung gestartet wird oder nach einer Leerlaufzeitüberschreitung.

Statische IP-Adressen in AWS Global Accelerator

Sie verwenden die statischen IP-Adressen, die Global Accelerator Ihrem Accelerator zuweist — oder die Sie aus Ihrem eigenen IP-Adresspool für Standardbeschleuniger angeben —, um Internetverkehr an das globale AWS Netzwerk weiterzuleiten, in der Nähe Ihrer Benutzer, unabhängig von ihrem Standort. Bei Standardbeschleunigern verknüpfen Sie die Adressen mit Network Load Balancern, Application Load Balancern, Amazon EC2 Instances oder Elastic IP-Adressen, die in

einer einzelnen AWS Region oder mehreren Regionen ausgeführt werden. Für benutzerdefinierte Routingbeschleuniger leiten Sie Datenverkehr an EC2-Ziele in VPC -Subnetzen in einer oder mehreren Regionen weiter. Das Routing von Datenverkehr über das globale AWS Netzwerk verbessert die Verfügbarkeit und Leistung, da der Datenverkehr nicht mehrere Hops über das öffentliche Internet ausführen muss. Mit statischen IP-Adressen können Sie auch eingehenden Anwendungsdatenverkehr auf mehrere Endpunktressourcen in mehreren AWS Regionen verteilen.

Darüber hinaus erleichtert die Verwendung statischer IP-Adressen das Hinzufügen Ihrer Anwendung zu mehreren Regionen oder das Migrieren von Anwendungen zwischen Regionen. Die Verwendung fester IP-Adressen bedeutet, dass Benutzer eine konsistente Möglichkeit haben, eine Verbindung mit Ihrer Anwendung herzustellen, während Sie Änderungen vornehmen.

Wenn Sie möchten, können Sie Ihren eigenen benutzerdefinierten Domänennamen mit den statischen IP-Adressen für Ihren Accelerator verknüpfen. Weitere Informationen finden Sie unter Weiterleiten von benutzerdefinierten Domain-Traffic an Ihren Accelerator.

Global Accelerator stellt Ihnen die statischen IP-Adressen aus dem Amazon-Pool von IP-Adressen zur Verfügung, es sei denn, Sie bringen Ihren eigenen IP-Adressbereich in AWS und geben dann die statischen IP-Adressen aus diesem Pool an. (Weitere Informationen finden Sie unter Bring Your Own IP Addresses (BYOIP) in AWS Global Accelerator.) Um einen Accelerator auf der Konsole zu erstellen, müssen Sie Global Accelerator zunächst auffordern, die statischen IP-Adressen bereitzustellen, indem Sie einen Namen für den Accelerator eingeben oder eigene statische IP-Adressen auswählen. Informationen zu den Schritten zum Erstellen eines Beschleunigers finden Sie unterErste Schritte mit AWS Global Accelerator.

Die statischen IP-Adressen bleiben Ihrem Accelerator so lange zugewiesen, wie er existiert, auch wenn Sie den Accelerator deaktivieren und keinen Datenverkehr mehr annehmen oder weiterleiten. Allerdings, wenn Siedeleteeinen Beschleuniger verwenden, verlieren Sie die ihm zugewiesenen statischen IP-Adressen, sodass Sie den Datenverkehr nicht mehr mithilfe dieser Adressen weiterleiten können. Sie können IAM-Richtlinien wie tag-basierte Berechtigungen mit Global Accelerator verwenden, um die Benutzer einzuschränken, die über Berechtigungen zum Löschen eines Accelerators verfügen. Weitere Informationen finden Sie unter Tagbasierte Richtlinien.

Verkehrsflussmanagement mit Verkehrszifferblättern und Endpunktgewichten

Es gibt zwei Möglichkeiten, wie AWS Global Accelerator mit einem Standardbeschleuniger Datenverkehr an Ihre Endpunkte sendet:

- Ändern der Verkehrswahl, um den Datenverkehr für eine oder mehrere Endpunktgruppen zu begrenzen
- Angeben von Gewichtungen, um den Anteil des Datenverkehrs zu den Endpunkten in einer Gruppe zu ändern

Funktionsweise von Verkehrszifferblättern

Für jede Endpunktgruppe in einem Standardbeschleuniger können Sie eine Verkehrswahl festlegen, um den Prozentsatz des Datenverkehrs zu steuern, der an die Endpunktgruppe gesendet wird. Der Prozentsatz wird nur auf Datenverkehr angewendet, der bereits an die Endpunktgruppe geleitet ist, nicht auf den gesamten Listener-Datenverkehr.

Die Verkehrswahl begrenzt den Anteil des Datenverkehrs, den eine Endpunktgruppe akzeptiert, ausgedrückt als Prozentsatz des Datenverkehrs, der an diese Endpunktgruppe geleitet wird. Wenn Sie beispielsweise die Verkehrswahl für eine Endpunktgruppe in`us-east-1`auf 50 (d. h. 50%) und der Accelerator 100 Benutzeranforderungen an diese Endpunktgruppe weiterleitet, werden nur 50 Anforderungen von der Gruppe akzeptiert. Der Accelerator leitet die verbleibenden 50 Anforderungen an Endpunktgruppen in anderen Regionen.

Weitere Informationen finden Sie unter Anpassen des Verkehrsflusses mit Verkehrszifferblättern.

Funktionsweise von Gewichten

Für jeden Endpunkt in einem Standardbeschleuniger können Sie Gewichtungen angeben, d. h. Zahlen, die den Anteil des Datenverkehrs ändern, den der Beschleuniger zu jedem Endpunkt leitet. Dies kann beispielsweise nützlich sein, um Leistungstests innerhalb einer Region durchzuführen.

Eine Gewichtung ist ein Wert, der den Anteil des Datenverkehrs bestimmt, den der Beschleuniger an einen Endpunkt leitet. Standardmäßig beträgt die Gewichtung eines Endpunkts 128, d. h. die Hälfte des Maximalwerts für eine Gewichtung, 255.

Der Accelerator berechnet die Summe der Gewichtungen für die Endpunkte in einer Endpunktgruppe und leitet dann den Datenverkehr auf der Grundlage des Verhältnisses der Gewichtung jedes Endpunkts zur Summe an die Endpunkte weiter. Ein Beispiel für die Funktionsweise von Gewichtungen finden Sie unterEndpoint Gewichtungen.

Verkehrszifferblätter und -gewichte beeinflussen, wie der Standardbeschleuniger den Verkehr auf unterschiedliche Weise bedient:

- Sie konfigurieren Verkehrswahlen fürEndpunktgruppen. Mit der Verkehrswahl können Sie einen Prozentsatz des Traffics (oder des gesamten Traffics) an die Gruppe abschneiden, indem Sie den Datenverkehr, den der Beschleuniger bereits auf der Grundlage anderer Faktoren, wie etwa der Nähe, an die Gruppe weitergeleitet hat, „herunterwählen“.
- Auf der anderen Seite verwenden Sie Gewichte, um Werte fürIndividuelle Endpunkteinnerhalb einer Endpunktgruppe. Gewichtungen bieten eine Möglichkeit, den Datenverkehr innerhalb der Endpunktgruppe aufzuteilen. Beispielsweise können Sie Gewichtungen verwenden, um Leistungstests für bestimmte Endpunkte in einer Region durchzuführen.

> **Note**
>
> Weitere Informationen zur Auswirkung von Verkehrswahlen und -gewichten finden Sie unterFailover für fehlerhafte Endpunkte.

Health sprüfungen für AWS Global Accelerator

Bei Standardbeschleunigern überprüft AWS Global Accelerator automatisch die Integrität der Endpunkte, die Ihren statischen IP-Adressen zugeordnet sind, und leitet dann den Benutzerverkehr nur an fehlerfreie Endpunkte weiter.

Global Accelerator enthält Standardintegritätsprüfungen, die automatisch ausgeführt werden. Sie können jedoch das Timing für die Prüfungen und andere Optionen konfigurieren. Wenn Sie benutzerdefinierte Einstellungen für die Integritätsprüfung konfiguriert haben, verwendet Global Accelerator diese Einstellungen je nach Konfiguration auf bestimmte Weise. Sie konfigurieren diese Einstellungen in Global Accelerator für Amazon EC2 Instances oder Elastic IP-Adressenendpoints oder indem Sie Einstellungen in der Elastic Load Balancing Konsole für Network Load Balancers oder Application Load Balancers konfigurieren. Weitere Informationen finden Sie unter Zustandsprüfungsoptionen.

Wenn Sie einem Standardbeschleuniger einen Endpunkt hinzufügen, muss er eine Integritätsprüfung bestehen, um als fehlerfrei zu gelten, bevor der Datenverkehr an ihn weitergeleitet wird. Wenn Global Accelerator über keine fehlerfreien Endpunkte verfügt, an die der Datenverkehr in einem Standardbeschleuniger weitergeleitet werden kann, leitet er Anforderungen an alle Endpunkte weiter.

-Accelerator-Arten

Es gibt zwei Arten von Beschleunigern, die Sie mit AWS Global Accelerator verwenden können:- AcceleratorsundBenutzerdefinierte Routing-Beschleuniger. Beide Arten von Beschleunigern leiten Datenverkehr über das globale AWS Netzwerk, um die Leistung und Stabilität zu verbessern. Sie sind jedoch für unterschiedliche Anwendungsanforderungen konzipiert.

-Accelerator-Standard

Durch die Verwendung eines Standard-Beschleunigers können Sie die Verfügbarkeit und Leistung Ihrer Anwendungen verbessern, die auf Application Load Balancern, Network Load Balancern oder Amazon EC2 Instances ausgeführt werden. Mit einem Standardbeschleuniger leitet Global Accelerator Clientdatenverkehr basierend auf geografischer Nähe und Endpunktzustand über regionale Endpunkte weiter. Darüber hinaus können Kunden den Client-Datenverkehr auf Endpunkte basierend auf Steuerelementen wie Verkehrswahlen und Endpunktgewichten verschieben. Dies funktioniert für eine Vielzahl von Anwendungsfällen, einschließlich blau/grüner Bereitstellung, A/B-Tests und Bereitstellung in mehreren Regionen. Weitere Anwendungsfälle finden Sie unterAWS Global Accelerator.

Weitere Informationen hierzu finden Sie unter Arbeiten mit Standard-Beschleunigern in AWS Global Accelerator.

Benutzerdefinierte Routing-Beschleuniger

Benutzerdefinierte Routingbeschleuniger eignen sich gut für Szenarien, in denen Sie benutzerdefinierte Anwendungslogik verwenden möchten, um einen oder mehrere Benutzer an ein bestimmtes Ziel und einen bestimmten Port unter vielen zu lenken, während sie dennoch die Leistungsvorteile von Global Accelerator nutzen. Ein Beispiel dafür sind VoIP Anwendungen, die einem bestimmten Medienserver mehrere Anrufer zuweisen, um Sprach-, Video- und Messaging-Sitzungen zu starten. Ein weiteres Beispiel sind Online-Echtzeit-Gaming-Anwendungen, bei denen Sie mehrere Spieler einer einzelnen Sitzung auf einem Spielserver basierend auf Faktoren wie geografischer Lage, Spielerfähigkeiten und Spielmodus zuweisen möchten.

Weitere Informationen hierzu finden Sie unter Arbeiten mit benutzerdefinierten Routing-Beschleunigern in AWS Global Accelerator.

Basierend auf Ihren spezifischen Anforderungen erstellen Sie eine dieser Arten von Beschleunigern, um Ihren Kundenverkehr zu beschleunigen.

Standort- und IP-Adressbereiche von Global Accelerator-Edge-Servern

Eine Liste der Edge-Serverstandorte von Global Accelerator finden Sie im AbschnittWo wird AWS Global Accelerator heute bereitgestellt?-Abschnitt imHäufig gestellte Fragen zu AWS Global Acceleratorangezeigten.

AWS veröffentlicht seine aktuellen IP-Adressbereiche im JSON-Format. Um die aktuellen Bereiche anzuzeigen, laden Sieip-ranges.json. Weitere Informationen finden Sie unter AWS IP-Adressbereiche im Amazon Web Services General Reference.

Um die IP-Adressbereiche zu finden, die den AWS Global Accelerator -Edge-Servern zugeordnet sind, suchen Sie nach`ip-ranges.json`für die folgende Zeichenfolge:

```
"service": "GLOBALACCELERATOR"
```

Global Accelerator-Einträge, die`"region": "GLOBAL"`beziehen sich auf die statischen IP-Adressen, die den Beschleunigern zugewiesen sind. Wenn Sie den Datenverkehr über den Beschleuniger filtern möchten, der von POPs (Points of Presence) in einem Gebiet stammt, filtern Sie nach Einträgen, die ein bestimmtes geografisches Gebiet enthalten, z. B.`us-*`oder `.eu-*`. Wenn Sie beispielsweise nach`us-*`, sehen Sie nur Traffic, der über POPs in den USA (USA) kommt.

AWS Global Accelerator

Die Verwendung von AWS Global Accelerator kann Ihnen dabei helfen, eine Vielzahl von Zielen zu erreichen. In diesem Abschnitt werden einige von ihnen aufgeführt, um Ihnen eine Vorstellung davon zu geben, wie Sie Global Accelerator verwenden können, um Ihre Anforderungen zu erfüllen.

Skalierung für erhöhte Anwendungsauslastung

Wenn die Anwendungsnutzung zunimmt, erhöht sich auch die Anzahl der IP-Adressen und Endpunkte, die Sie verwalten müssen. Mit Global Accelerator können Sie Ihr Netzwerk nach oben oder unten skalieren. Damit können Sie regionale Ressourcen, wie Load Balancer und Amazon EC2 Instances, zwei statischen IP-Adressen zuordnen. Sie fügen diese Adressen in Zulassungslisten nur einmal in Ihre Clientanwendungen, Firewalls und DNS-Einträge ein. Mit Global Accelerator können Sie Endpunkte in AWS Regionen hinzufügen oder entfernen, blau/grüne Bereitstellung ausführen und A/B-Tests durchführen, ohne die IP-Adressen in Ihren Clientanwendungen aktualisieren zu müssen. Dies ist besonders nützlich für IoT, Einzelhandel,

Medien, Automobilindustrie und Gesundheitswesen, in denen Sie Client-Anwendungen nicht einfach häufig aktualisieren können.

Beschleunigung für latenzempfindliche Anwendungen

Viele Anwendungen, insbesondere in Bereichen wie Gaming, Medien, mobile Apps und Finanzen, erfordern eine sehr geringe Latenz für eine hervorragende Benutzererfahrung. Um die Benutzererfahrung zu verbessern, leitet Global Accelerator den Benutzerverkehr an den Anwendungsendpunkt weiter, der dem Client am nächsten liegt. Dadurch wird die Internetlatenz und der Jitter reduziert. Global Accelerator leitet den Datenverkehr mithilfe von Anycast an den nächstgelegenen Edge-Standort weiter und leitet ihn dann über das globale AWS Netzwerk an den nächstgelegenen regionalen Endpunkt weiter. Global Accelerator reagiert schnell auf Änderungen der Netzwerkleistung, um die Anwendungsleistung Ihrer Benutzer zu verbessern.

Disaster Recovery und Ausfallsicherheit in mehreren Regionen

Sie müssen sich darauf verlassen können, dass Ihr Netzwerk verfügbar ist. Möglicherweise führen Sie Ihre Anwendung in mehreren AWS Regionen aus, um Disaster Recovery, höhere Verfügbarkeit, geringere Latenz oder Compliance zu unterstützen. Wenn Global Accelerator feststellt, dass Ihr Anwendungsendpunkt in der primären AWS Region ausfällt, löst er sofort das Umleiten des Datenverkehrs zu Ihrem Anwendungsendpunkt in der nächsten verfügbaren, nächstgelegenen AWS-Region aus.

Schützen Sie Ihre Anwendungen

Wenn Sie Ihre AWS Ursprünge, z. B. Application Load Balancers oder Amazon EC2 Instances, dem öffentlichen Internetverkehr zugänglich machen, entsteht eine Chance für böswillige Angriffe. Global Accelerator verringert das Angriffsrisiko, indem du deinen Ursprung hinter zwei statischen Eintrittspunkten maskierst. Diese Einstiegspunkte sind standardmäßig vor Distributed Denial of Service (DDoS) -Angriffen mit AWS Shield geschützt. Global Accelerator erstellt mithilfe privater IP-Adressen eine Peering-Verbindung mit Ihrer Amazon Virtual Private Cloud und hält Verbindungen zu Ihren internen Application Load Balancern oder privaten EC2-Instances außerhalb des öffentlichen Internets.

Verbessern Sie die Leistung für VoIP - oder Online-Gaming-Anwendungen

Mit einem benutzerdefinierten Routing Accelerator können Sie die Leistungsvorteile von Global Accelerator für Ihre VoIP - oder Gaming-Anwendungen nutzen. Beispielsweise können Sie Global Accelerator für Online-Gaming-Anwendungen verwenden, die mehreren Spielern einer einzelnen Spielsitzung zuweisen. Verwenden Sie Global Accelerator, um Latenz und Jitter global für Anwendungen zu reduzieren, die benutzerdefinierte Logik benötigen, um Benutzer bestimmten

Endpunkten zuzuordnen, z. B. Multiplayer-Spiele oder VoIP Anrufe. Sie können einen einzigen Beschleuniger verwenden, um Clients mit Tausenden von Amazon EC2 Instances zu verbinden, die in einer oder mehreren AWS Regionen ausgeführt werden. Dabei behalten Sie die volle Kontrolle darüber, welcher Client an welche EC2-Instanz und welchen Port weitergeleitet wird.

AWS Global Accelerator

Sie können das AWS Global Accelerator Speed Comparison Tool verwenden, um die Downloadgeschwindigkeiten von Global Accelerator im Vergleich zu direkten Internet-Downloads in allen AWS-Regionen anzuzeigen. Mit diesem Tool können Sie Ihren Browser verwenden, um den Leistungsunterschied beim Übertragen von Daten mit Global Accelerator anzuzeigen. Sie wählen eine Dateigröße, die heruntergeladen werden soll, und das Tool lädt Dateien über HTTPS/TCP von Application Load Balancers in verschiedenen Regionen in Ihren Browser herunter. Für jede Region wird ein direkter Vergleich der Download-Geschwindigkeiten angezeigt.

Um auf das Geschwindigkeitsvergleichs-Tool zuzugreifen, kopieren Sie die folgende URL in Ihren Browser:

```
https://speedtest.globalaccelerator.aws
```

> **Important**
>
> Die Ergebnisse können abweichen, wenn Sie den Test mehrmals ausführen. Die Downloadzeiten können je nach Faktoren variieren, die außerhalb von Global Accelerator liegen, wie Qualität, Kapazität und Entfernung der Verbindung im Netzwerk der letzten Meile, das Sie verwenden.

Erste Schritte mit AWS Global Accelerator

Sie können mit der Einrichtung von AWS Global Accelerator beginnen, indem Sie die API oder die AWS Global Accelerator-Konsole verwenden. Da Global Accelerator ein globaler Service ist, ist er nicht an eine bestimmte AWS Region gebunden. Beachten Sie, dass Global Accelerator ein globaler Service ist, der Endpunkte in mehreren AWS Regionen unterstützt. Sie müssen jedoch die Region USA West (Oregon) angeben, um Beschleuniger zu erstellen oder zu aktualisieren.

Gehen Sie folgendermaßen vor, um mit dem Global Accelerator zu beginnen:

1. Wählen Sie den -Accelerator-Typ aus, der erstellt werden soll: Ein Standard-Accelerator oder ein benutzerdefiniertes Routing-Accelerator
2. Konfigurieren Sie die erste Einrichtung für Global Accelerator: Geben Sie einen Namen für Ihr Accelerator ein. Konfigurieren Sie dann einen oder mehrere Listener, um eingehende Verbindungen von Clients zu verarbeiten, basierend auf dem von Ihnen angegebenen Protokoll und Port (oder Portbereich).
3. Konfigurieren Sie regionale Endpunktgruppen für Ihren Beschleuniger: Sie können eine oder mehrere regionale Endpunktgruppen auswählen, die Ihrem Listener hinzugefügt werden sollen. Der Listener leitet Anforderungen an die Endpunkte weiter, die Sie einer Endpunktgruppe hinzugefügt haben.

   Bei einem Standardbeschleuniger überwacht Global Accelerator die Integrität von Endpunkten innerhalb der Gruppe mithilfe der Integritätsprüfungseinstellungen, die für jeden Endpunkt definiert sind. Für jede Endpunktgruppe in einem Standardbeschleuniger können Sie eineVerkehrsmittel-WahlProzentsatz, um den Prozentsatz des Datenverkehrs zu steuern, den eine Endpunktgruppe akzeptiert. Der Prozentsatz wird nur auf Datenverkehr angewendet, der bereits an die Endpunktgruppe geleitet ist, nicht auf den gesamten Listener-Datenverkehr. Standardmäßig ist die Verkehrswahl für alle regionalen Endpunktgruppen auf 100% festgelegt.

   Bei benutzerdefinierten Routingbeschleunigern wird der Datenverkehr auf der Grundlage des Listener-Ports, an den der Datenverkehr empfangen wird, deterministisch an ein bestimmtes Ziel in einem VPC -Subnetz weitergeleitet.
4. Endpunkte zu Endpunktgruppen hinzufügen: Die hinzugefügten Endpunkte hängen vom -Accelerator-Typ ab.
   - Bei einem Standardbeschleuniger können Sie jeder Endpunktgruppe eine oder mehrere regionale Ressourcen wie Load Balancer oder EC2-Instances hinzufügen. Als Nächstes können Sie entscheiden, wie viel Datenverkehr Sie an jeden Endpunkt weiterleiten möchten, indem Sie die Gewichtung der Endpunkte festlegen.
   - Für einen benutzerdefinierten Routing Accelerator fügen Sie ein oder mehrere virtuelle Private Cloud (VPC) -Subnetze mit bis zu Tausenden von Amazon EC2 Instance-Zielen hinzu.

Ausführliche Schritte zum Erstellen eines Standard-Beschleunigers oder eines benutzerdefinierten Routing-Beschleunigers mit der AWS Global Accelerator Konsole finden Sie unterErste Schritte mit AWS Global Accelerator. Weitere Informationen zur Arbeit mit API-Operationen finden Sie unterHäufige Aktionen, die Sie mit AWS Global Accelerator verwenden könnenund dieAWS Global Accelerator.

Taggen in AWS Global Accelerator

Tags sind Wörter oder Phrasen (Metadaten), die Sie verwenden, um Ihre AWS Ressourcen zu identifizieren und zu verwalten. Sie können jeder Ressource mehrere Tags hinzufügen, und jedes Tag enthält einen Schlüssel und einen Wert, den Sie festlegen. Der Schlüssel könnte zum Beispiel sein`environment`und der Wert könnte`production`. Sie können die Ressourcen auf Grundlage der hinzugefügten Tags durchsuchen und filtern. In AWS Global Accelerator können Sie Beschleuniger taggen.

Im Folgenden finden Sie zwei Beispiele dafür, wie nützlich es sein kann, in Global Accelerator zu arbeiten:

- Verwenden Sie Tags, um Fakturierungsinformationen in verschiedenen Kategorien nachzuverfolgen. Wenden Sie dazu Tags auf Beschleuniger oder andere AWS Ressourcen an (z. B. Network Load Balancers, Application Load Balancers oder Amazon EC2 Instances) und aktivieren Sie die Tags. AWS generiert einen Kostenzuordnungsbericht als durch Kommas getrennten Werten (CSV-Datei) mit Informationen über Ihre Nutzung und Ihre Kosten gemäß Ihren aktiven Tags. Sie können Tags anwenden, die geschäftliche Kategorien (wie Kostenstellen, Anwendungsnamen oder Eigentümer) darstellen, um die Kosten für mehrere Services zu organisieren. Weitere Informationen finden Sie unter Verwendung von Kostenzuordnungs-Tags im AWS-Fakturierung und Kostenmanagement-Benutzerhandbuch.
- Verwenden Sie Tags, um Tag-basierte Berechtigungen für Accelerators zu erzwingen. Erstellen Sie hierzu IAM-Richtlinien, die Tags und Tag-Werte angeben, um Aktionen zuzulassen oder zu unterbinden. Weitere Informationen finden Sie unter Tagbasierte Richtlinien.

Verwendungskonventionen und Links zu anderen Ressourcen zum Tagging finden Sie unterTaggen von AWS Ressourcenim Allgemeine AWS-Referenz. Tipps zur Verwendung von Tags finden Sie unterBewährte Methoden für Taggen: AWS Strategie zur Ressourcenkennzeichnungim AWS-Whitepaper-Blog.

Informationen zur maximalen Anzahl von Tags, die Sie einer Ressource in Global Accelerator hinzufügen können, finden Sie unterKontingente für AWS Global Accelerator.

Sie können Tags über die AWS-Konsole, die AWS-CLI oder die Global Accelerator-Accelerator-API hinzufügen und aktualisieren. Dieses Kapitel enthält Schritte zum Arbeiten mit Tagging in der Konsole. Weitere Informationen zum Arbeiten mit Tags mithilfe der AWS CLI und der Global Accelerator-API, einschließlich CLI-Beispiele, finden Sie in den folgenden Vorgängen im AWS Global Accelerator:

- CreateAccelerator
- TagResource
- UntagResource
- ListTagsForResource

Tagging-Unterstützung in Global Accelerator

AWS Global Accelerator unterstützt Tagging für Beschleuniger.

Global Accelerator unterstützt die tagbasierte Zugriffssteuerungsfunktion von AWS Identity and Access Management (IAM). Weitere Informationen finden Sie unter Tagbasierte Richtlinien.

Hinzufügen, Bearbeiten und Löschen von Tags in Global Accelerator

Im folgenden Verfahren wird erläutert, wie Sie Tags für Accelerators in der Global Accelerator-Konsole hinzufügen, bearbeiten und löschen.

> **Note**
>
> Sie können Tags über die -Konsole, die AWS CLI oder die Global Accelerator-API hinzufügen oder entfernen. Weitere Informationen, einschließlich CLI-Beispielen, finden Sie unterTagResourceimAWS Global Accelerator.

So fügen Sie Tags hinzu, bearbeiten oder löschen sie

1. Öffnen Sie die Global Accelerator-Konsole unterhttps://console.aws.amazon.com/globalaccelerator/home.
2. Wählen Sie die Accelerator, für die Sie Tags hinzufügen oder aktualisieren möchten.
3. In derTagsGehen Sie folgendermaßen vor:

   Hinzufügen eines Tags

   Klicken Sie aufTag hinzufügenGeben Sie einen Schlüssel und optional einen Wert für das Tag ein.

Bearbeiten eines Tags

Aktualisieren Sie den Text für einen Schlüssel, einen Wert oder beides. Sie können auch den Wert für ein Tag löschen, aber der Schlüssel ist erforderlich.

Löschen eines Tags

Klicken Sie aufRemoveauf der rechten Seite des Wertfelds klicken.

4. Wählen Sie Save Changes.

AWS Global Accelerator

Mit AWS Global Accelerator bezahlen Sie nur für das, was Sie wirklich nutzen. Ihnen werden ein Stundensatz und Datenübertragungskosten für jeden Beschleuniger in Ihrem Konto in Rechnung gestellt. Weitere Informationen finden Sie unterAWS Global Accelerator.

Erste Schritte mit AWS Global Accelerator

Diese Tutorials enthalten die Schritte für die ersten Schritte mit AWS Global Accelerator über die Konsole. Sie können auch AWS Global Accelerator API-Vorgänge verwenden, um Ihre Beschleuniger zu erstellen und anzupassen. Bei jedem Schritt in diesem Lernprogramm gibt es einen Link zum entsprechenden API-Vorgang, um die Aufgabe programmgesteuert abzuschließen. (Wenn Sie einen benutzerdefinierten Routingbeschleuniger einrichten, müssen Sie die API für bestimmte Konfigurationsschritte verwenden.) Weitere Informationen zum Arbeiten mit AWS Global Accelerator - API-Operationen finden Sie imAWS Global Accelerator -API.

> **Tip**
>
> Um zu erfahren, wie Sie Global Accelerator verwenden können, um die Leistung und Verfügbarkeit von Webanwendungen zu verbessern, lesen Sie den folgenden Workshop zum Selbststudium: AWS Global Accelerator Workshop.

Global Accelerator ist ein globaler Service, der Endpunkte in mehreren AWS Regionen unterstützt, die imAWS Regionentabelle.

Dieses Kapitel enthält zwei Tutorials: eine zum Erstellen eines Standard-Beschleunigers und eine zum Erstellen eines benutzerdefinierten Routing-Beschleunigers. Weitere Informationen zu den beiden Accelerator-Typen finden Sie unterArbeiten mit Standard-Beschleunigern in AWS Global AcceleratorundArbeiten mit benutzerdefinierten Routing-Beschleunigern in AWS Global Accelerator.

Themen

- Erste Schritte mit einem Standard-Accelerator
- Erste Schritte mit einem benutzerdefinierten Routing-Accelerator

Erste Schritte mit einem Standard-Accelerator

Dieser Abschnitt enthält die Schritte zum Erstellen eines Standard-Accelerators, der den Datenverkehr an einen optimalen Endpunkt weiterleitet.

Aufgaben

- Bevor Sie beginnen

- Schritt 1: Erstellen eines Accelerators
- Schritt 2: Hinzufügen von Listener
- Schritt 3: Hinzufügen von Endpunktgruppen
- Schritt 4: Hinzufügen von Endpunkten
- Schritt 5: Testen Sie Ihren Accelerator
- Schritt 6 (optional): Löschen des Accelerators

Bevor Sie beginnen

Erstellen Sie vor dem Erstellen eines Beschleunigers mindestens eine Ressource, die Sie als Endpunkt hinzufügen können, an den Datenverkehr weitergeleitet werden soll. Erstellen Sie beispielsweise einen der folgenden:

- Starten Sie mindestens eine Amazon EC2 Instance, die als Endpunkt hinzugefügt werden soll. Weitere Informationen finden Sie unterErstellen Sie Ihre EC2-Ressourcen und starten Sie Ihre EC2-InstanceimAmazon EC2-Benutzerhandbuch für Linux-Instances.
- Erstellen Sie optional einen oder mehrere Network Load Balancer oder Application Load Balancer, die EC2-Instanzen enthalten. Weitere Informationen finden Sie unterErstellen eines Network Load Balancer Application Load BalancerimBenutzerhandbuch für Network Load Balancer.

Achten Sie beim Erstellen einer Ressource zum Global Accelerator auf Folgendes:

- Wenn Sie einen internen Application Load Balancer oder einen EC2-Instance-Endpunkt in Global Accelerator hinzufügen, können Sie den Internetverkehr direkt zum und vom Endpunkt in virtuellen privaten Clouds (VPCs) übertragen, indem Sie ihn in einem privaten Subnetz ansprechen. Die VPC, die den Load Balancer oder die EC2-Instance enthält, muss über einenInternet-Gatewayangehängt, um anzuzeigen, dass die VPC Internetverkehr akzeptiert. Weitere Informationen finden Sie unter Sichere VPC Verbindungen in AWS Global Accelerator.
- Global Accelerator erfordert, dass Ihre Router- und Firewallregeln eingehenden Datenverkehr von den IP-Adressen, die mit Route 53-Integritätsprüfungen verknüpft sind, zulassen, um Integritätsprüfungen für EC2-Instances oder Elastic IP-Adressenendpunkte abzuschließen. Informationen zu den IP-Adressbereichen, die mit Amazon Route 53 Health Checkers verknüpft sind, finden Sie unterZustandsprüfungen für Ihre ZielgruppenimAmazon Route 53 Entwicklerhandbuch.

Schritt 1: Erstellen eines Accelerators

Um den Accelerator zu erstellen, geben Sie einen Namen ein.

> **Note**
>
> Um diese Aufgabe mit einer -API-Operation anstelle mit der -Konsole mit der -API-Operation abzuschließen, informierenCreateAcceleratorimAWS Global Accelerator -API.

So erstellen Sie einen Accelerator

1. Öffnen Sie die Global Accelerator-Konsole unterhttps://console.aws.amazon.com/globalaccelerator/home.
2. Klicken Sie aufErstellen eines Accelerators.
3. Geben Sie einen Namen für Ihren Accelerator an.
4. Optional können Sie ein oder mehrere Tags hinzufügen, um Ihre Global Accelerator-Ressourcen zu identifizieren.
5. Wählen Sie Next.

Schritt 2: Hinzufügen von Listener

Erstellen Sie einen Listener, um eingehende Verbindungen von Ihren Benutzern zu Global Accelerator zu verarbeiten

> **Note**
>
> Um diese Aufgabe mit einer -API-Operation anstelle mit der -Konsole mit der -API-Operation abzuschließen, informierenCreateListenerimAWS Global Accelerator -API.

So erstellen Sie einen Listener

1. Klicken Sie auf derHinzufügen eines Listenersdie Ports oder Portbereiche ein, die Sie dem Listener zuordnen möchten. Listener unterstützen Ports 1-65535.
2. Wählen Sie das Protokoll oder die Protokolle für die eingegebenen Ports aus.

3. Optional können Sie die Clientaffinität aktivieren. Clientaffinität für einen Listener bedeutet, dass Global Accelerator sicherstellt, dass Verbindungen von einer bestimmten Quell-IP-Adresse (Client) immer an denselben Endpunkt weitergeleitet werden. Um dieses Verhalten zu aktivieren, wählen Sie in der Dropdown-ListeQuell-IP.

   Der Standardwert istKeine, was bedeutet, dass die Clientaffinität nicht aktiviert ist und Global Accelerator den Datenverkehr gleichmäßig zwischen den Endpunkten in den Endpunktgruppen für den Listener verteilt.

   Weitere Informationen finden Sie unter Client-Affinität.
4. Wählen Sie alternativ die OptionHinzufügen eines Listeners, um einen zusätzlichen Listener hinzuzufügen.
5. Wählen Sie nach dem Hinzufügen von Listenern ausWeiter.

Schritt 3: Hinzufügen von Endpunktgruppen

Fügen Sie eine oder mehrere Endpunktgruppen hinzu, die jeweils einer bestimmten AWS Region zugeordnet sind.

> **Note**
>
> Um diese Aufgabe mit einer -API-Operation anstelle mit der -Konsole mit der -API-Operation abzuschließen, informierenCreateEndpointGroupimAWS Global Accelerator -API.

Hinzufügen einer Endpunktgruppe

1. Klicken Sie auf derHinzufügen von Endpunktgruppenim Abschnitt für einen Listener eineRegionWählen Sie aus der Dropdown-Liste aus.
2. Optional fürVerkehrs-Wahleine Zahl zwischen 0 und 100 ein, um einen Prozentsatz des Datenverkehrs für diese Endpunktgruppe festzulegen. Der Prozentsatz wird nur auf den Datenverkehr angewendet, der bereits an diese Endpunktgruppe gerichtet ist, nicht auf den gesamten Listener-Datenverkehr. Standardmäßig ist die Verkehrswahl für eine Endpunktgruppe auf 100 (d. h. 100%) festgelegt.
3. Wählen Sie optional für benutzerdefinierte IntegritätsprüfungswerteKonfigurieren von Zustandsprüfungen. Wenn Sie Einstellungen für die Integritätsprüfung konfigurieren, verwendet Global Accelerator die Einstellungen für Integritätsprüfungen für EC2-Instanzen und

Elastic IP-Adressenendpunkte. Für Network Load Balancer und Application Load Balancer Endpunkte verwendet Global Accelerator die Integritätsprüfungseinstellungen, die Sie bereits für die Load Balancer selbst konfiguriert haben. Weitere Informationen finden Sie unter Zustandsprüfungsoptionen.

4. Wählen Sie alternativ die OptionFügt einen Endpunkt hinzu., um zusätzliche Endpunktgruppen für diesen Listener oder andere Listener hinzuzufügen.
5. Wählen Sie Next.

Schritt 4: Hinzufügen von Endpunkten

Fügen Sie einen oder mehrere Endpunkte hinzu, die bestimmten Endpunktgruppen zugeordnet sind. Dieser Schritt ist nicht erforderlich, aber kein Datenverkehr wird an Endpunkte in einer Region weitergeleitet, es sei denn, die Endpunkte sind in einer Endpunktgruppe enthalten.

> **Note**
>
> Wenn Sie den Beschleuniger programmgesteuert erstellen, fügen Sie Endpunkte als Teil des Hinzufügens von Endpunktgruppen hinzu. Weitere Informationen finden Sie unterCreateEndpointGroupimAWS Global Accelerator -API.

Hinzufügen von Endpunkten

1. Klicken Sie auf derErstellen von Endpunktenim Abschnitt für einen Endpunkt eine-Endpunkt.
2. Optional fürGewichteine Zahl zwischen 0 und 255 ein, um eine Gewichtung für das Routing von Datenverkehr an diesen Endpunkt festzulegen. Wenn Sie Endpunkten Gewichtungen hinzufügen, konfigurieren Sie Global Accelerator so, dass der Datenverkehr basierend auf den von Ihnen angegebenen Proportionen weitergeleitet wird. Standardmäßig haben alle Endpunkte eine Gewichtung von 128. Weitere Informationen finden Sie unter Endpoint Gewichtungen.
3. Optional können Sie für einen Application Load Balancer er-Endpunkt unterBeibehalten der Client-IP-AdresseWählen Sie bei denBeibehalten von Adresse. Weitere Informationen finden Sie unter Beibehalten von Client-IP-Adressen in AWS Global Accelerator.
4. Wählen Sie alternativ die OptionHinzufügen eines Endpunkts, um weitere Endpunkte hinzuzufügen.
5. Wählen Sie Next.

Nachdem SieWeiterauf dem Global Accelerator-Dashboard wird eine Meldung angezeigt, dass Ihr Accelerator in Bearbeitung ist. Wenn der Vorgang abgeschlossen ist, lautet der Accelerator-Status im DashboardAktiv.

Schritt 5: Testen Sie Ihren Accelerator

Führen Sie Schritte aus, um den Beschleuniger zu testen, um sicherzustellen, dass der Datenverkehr an Ihre Endpunkte weitergeleitet wird. Führen Sie beispielsweise einen curl-Befehl wie den folgenden aus, indem Sie eine der statischen IP-Adressen Ihres Accelerators ersetzen, um die AWS Regionen anzuzeigen, in denen Anforderungen verarbeitet werden. Dies ist besonders hilfreich, wenn Sie unterschiedliche Gewichtungen für Endpunkte festlegen oder die Verkehrswahl für Endpunktgruppen anpassen.

Führen Sie einen curl-Befehl wie folgt aus, indem Sie eine der statischen IP-Adressen Ihres Accelerators ersetzen, um die IP-Adresse 100 Mal aufzurufen und dann eine Anzahl von Stellen auszugeben, an denen jede Anforderung verarbeitet wurde.

```
for ((i=0;i<100;i++)); do  curl http://198.51.100.0/ >> output.txt; done; cat
 output.txt | sort | uniq -c ; rm output.txt;
```

Wenn Sie die Verkehrswahl für Endpunktgruppen angepasst haben, können Sie mit diesem Befehl bestätigen, dass der Accelerator die richtigen Prozentsätze des Datenverkehrs an verschiedene Gruppen weiterleitet. Weitere Informationen finden Sie in den ausführlichen Beispielen im folgenden BlogbeitragVerkehrsmanagement mit AWS Global Accelerator.

Schritt 6 (optional): Löschen des Accelerators

Wenn Sie einen Accelerator als Test erstellt haben oder wenn Sie keinen Accelerator mehr verwenden, können Sie ihn löschen. Deaktivieren Sie auf der Konsole den Beschleuniger, und Sie können ihn dann löschen. Sie müssen keine Listener und Endpunktgruppen aus dem Accelerator entfernen.

Um einen Accelerator mithilfe eines API-Vorgangs anstelle der Konsole zu löschen, müssen Sie zuerst alle Listener und Endpunktgruppen entfernen, die dem Accelerator zugeordnet sind, sowie deaktivieren. Weitere Informationen finden Sie im .DeleteAcceleratorOperation (Operation) imAWS Global Accelerator -API.

Beachten Sie Folgendes, wenn Sie Endpunkte oder Endpunktgruppen entfernen oder einen Beschleuniger löschen:

- Wenn Sie einen Accelerator erstellen, stellt Ihnen Global Accelerator einen Satz von zwei statischen IP-Adressen zur Verfügung. Die IP-Adressen werden Ihrem Accelerator so lange zugewiesen, wie er existiert, auch wenn Sie den Accelerator deaktivieren und der Datenverkehr nicht mehr akzeptiert oder weiterleitet. Allerdings, wenn Siedeleteeinen Beschleuniger verwenden, verlieren Sie die statischen IP-Adressen, die dem Beschleuniger zugewiesen sind, sodass Sie den Datenverkehr nicht mehr mithilfe dieser Adressen weiterleiten können. Stellen Sie als bewährte Methode sicher, dass Sie über Berechtigungen verfügen, um ein versehentliches Löschen von Beschleunigern zu vermeiden. Sie können IAM-Richtlinien mit Global Accelerator verwenden, z. B. tagbasierte Berechtigungen, um die Benutzer einzuschränken, die über Berechtigungen zum Löschen eines Accelerators verfügen. Weitere Informationen finden Sie unter Tagbasierte Richtlinien.
- Wenn Sie eine EC2-Instance beenden, bevor Sie sie aus einer Endpunktgruppe in Global Accelerator entfernen und dann eine weitere Instance mit derselben privaten IP-Adresse erstellen und Integritätsprüfungen bestehen, leitet Global Accelerator Datenverkehr an den neuen Endpunkt weiter. Wenn dies nicht geschehen soll, entfernen Sie die EC2-Instanz aus der Endpunktgruppe, bevor Sie die Instanz beenden.

Löschen eines Accelerators

1. Öffnen Sie die Global Accelerator-Konsole unterhttps://console.aws.amazon.com/globalaccelerator/home.
2. Wählen Sie den Accelerator aus, den Sie löschen möchten.
3. Wählen Sie Edit (Bearbeiten) aus.
4. Klicken Sie aufDeaktivieren des AcceleratorsKlicken Sie auf und danach auf.Save.
5. Wählen Sie den Accelerator aus, den Sie löschen möchten.
6. Klicken Sie aufLöschen Accelerator.
7. Wählen Sie im Bestätigungsdialogfeld die Option Delete (Löschen).

Erste Schritte mit einem benutzerdefinierten Routing-Accelerator

Dieser Abschnitt enthält die Schritte, wie Sie einen benutzerdefinierten Routing-Accelerator erstellen, der den Datenverkehr deterministisch an Amazon EC2 Instance-Ziele in VPC -Subnetzendpunkten weiterleitet.

Aufgaben

- Bevor Sie beginnen
- Schritt 1: Erstellen eines benutzerdefinierten Routing-Accelerators
- Schritt 2: Hinzufügen von Listener
- Schritt 3: Hinzufügen von Endpunktgruppen
- Schritt 4: Hinzufügen von Endpunkten
- Schritt 5 (optional): Löschen des Accelerators

Bevor Sie beginnen

Bevor Sie einen benutzerdefinierten Routingbeschleuniger erstellen, erstellen Sie eine Ressource, die Sie als Endpunkt hinzufügen können, an den Datenverkehr weitergeleitet werden soll. Ein benutzerdefinierter Routing-Accelerator-Endpunkt muss ein VPC -Subnetz sein, das mehrere Amazon EC2 Instances enthalten kann. Weitere Informationen zum Erstellen der Ressourcen finden Sie hier:

- Erstellt ein VPC -Subnetz. Weitere Informationen finden Sie unterErstellen und Konfigurieren Ihrer VPCimAWS Directory Service Administrationshandbuch.
- Optional können Sie eine oder mehrere Amazon EC2 Instances in Ihrer VPC starten. Weitere Informationen finden Sie unterErstellen Sie Ihre EC2-Ressourcen und starten Sie Ihre EC2-InstanceimAmazon EC2-Benutzerhandbuch für Linux-Instances.

Achten Sie beim Erstellen einer Ressource zum Global Accelerator auf Folgendes:

- Wenn Sie einen EC2-Instance-Endpunkt in Global Accelerator hinzufügen, können Sie Internetdatenverkehr direkt zum und vom Endpunkt in VPCs übertragen, indem Sie ihn in einem privaten Subnetz ansprechen. Die VPC, die die EC2-Instance enthält, muss über einenInternet-Gatewayangehängt, um anzuzeigen, dass die VPC Internetverkehr akzeptiert. Weitere Informationen finden Sie unter Sichere VPC Verbindungen in AWS Global Accelerator.

Schritt 1: Erstellen eines benutzerdefinierten Routing-Accelerators

> **Note**
>
> Um diese Aufgabe mit einer -API-Operation anstelle mit der -Konsole mit der -API-Operation abzuschließen, informierenCreateCustomRoutingAcceleratorimAWS Global Accelerator -API.

So erstellen Sie einen Accelerator

1. Öffnen Sie die Global Accelerator-Konsole unterhttps://console.aws.amazon.com/globalaccelerator/home.
2. Geben Sie einen Namen für Ihren Accelerator an.
3. Für-Accelerator-TypWählen Sie bei denBenutzerdefinierte Routing.
4. Optional können Sie ein oder mehrere Tags hinzufügen, um Ihre Accelerator-Accelerator-Ressourcen zu identifizieren.
5. Klicken Sie aufWeiter, um Listener, Endpunktgruppen und VPC -Subnetzendpunkte hinzuzufügen.

Schritt 2: Hinzufügen von Listener

Erstellen Sie einen Listener, um eingehende Verbindungen von Ihren Benutzern zu Global Accelerator zu verarbeiten

Der Bereich, den Sie beim Erstellen eines Listener angeben, legt fest, wie viele Listener-Port- und Ziel-IP-Adresskombinationen Sie mit Ihrem benutzerdefinierten Routingbeschleuniger verwenden können. Um maximale Flexibilität zu gewährleisten, empfehlen wir, dass Sie einen großen Portbereich angeben. Jeder Listener-Portbereich, den Sie angeben, muss mindestens 16 Ports enthalten.

> **Note**
>
> Um diese Aufgabe mit einer -API-Operation anstelle mit der -Konsole mit der -API-Operation abzuschließen, informierenCreateCustomRoutingListenerimAWS Global Accelerator -API.

So erstellen Sie einen Listener

1. Klicken Sie auf derHinzufügen eines Listenersdie Ports oder Portbereiche ein, die Sie dem Listener zuordnen möchten. Listener unterstützen die Ports 1-65535.
2. Wählen Sie das Protokoll oder die Protokolle für die eingegebenen Ports aus.
3. Wählen Sie alternativ die OptionHinzufügen eines Listeners, um einen zusätzlichen Listener hinzuzufügen.
4. Wählen Sie nach dem Hinzufügen von Listenern ausWeiter.

Schritt 3: Hinzufügen von Endpunktgruppen

Fügen Sie eine oder mehrere Endpunktgruppen hinzu, die jeweils einer bestimmten AWS Region zugeordnet sind. Geben Sie für jede Endpunktgruppe einen oder mehrere Gruppen von Portbereichen und Protokollen an. Global Accelerator verwendet diese, um Datenverkehr an Amazon EC2 Instances in Subnetzen in der Region zu leiten.

Für jeden von Ihnen bereitgestellten Portbereich geben Sie auch das zu verwendende Protokoll an: UDP, TCP oder sowohl UDP als auch TCP.

> **Note**
>
> Um diese Aufgabe mit einer -API-Operation anstelle mit der -Konsole mit der -API-Operation abzuschließen, informierenCreateCustomRoutingendPointGroupimAWS Global Accelerator -API.

Hinzufügen einer Endpunktgruppe

1. Klicken Sie auf derHinzufügen von Endpunktgruppenim Abschnitt für einen Listener eineRegion.
2. FürPorts und ProtokollePortbereiche und Protokolle für Ihre Amazon EC2 Instances ein.
   - Geben Sie einenVom Hafenund einPortKlicken Sie auf, um einen Bereich von Ports anzugeben.
   - Geben Sie für jeden Portbereich das Protokoll bzw. die Protokolle für diesen Bereich an.

   Der Portbereich muss keine Teilmenge des Listener-Portbereichs sein, aber es muss genügend Gesamtanschlüsse im Listener-Portbereich vorhanden sein, um die Gesamtanzahl der von Ihnen angegebenen Ports zu unterstützen.
3. Wählen Sie Save (Speichern) aus.
4. Wählen Sie alternativ die OptionFügt einen Endpunkt hinzu., um zusätzliche Endpunktgruppen für diesen Listener oder andere Listener hinzuzufügen.
5. Wählen Sie Next.

Schritt 4: Hinzufügen von VPC -Subnetzendpunkten

Fügen Sie einen oder mehrere VPC -Subnetzendpunkte für diese regionale Endpunktgruppe ein oder mehrere VPC-Subnetzendpunkte hinzu. Endpunkte für benutzerdefinierte Routingbeschleuniger definieren die VPC -Subnetze, die Datenverkehr über einen benutzerdefinierten Routingbeschleuniger empfangen können. Jedes Subnetz kann ein oder mehrere Amazon EC2 Instance-Ziele enthalten.

Wenn Sie einen VPC -Subnetzendpunkt hinzufügen, generiert Global Accelerator neue Portzuordnungen, mit denen Sie Datenverkehr an die IP-Adressen der EC2-Zielinstanz im Subnetz weiterleiten können. Anschließend können Sie die Global Accelerator-API verwenden, um eine statische Liste aller Portzuordnungen für das Subnetz abzurufen und die Zuordnung verwenden, um den Datenverkehr deterministisch auf bestimmte EC2-Instanzen zu leiten.

> **Note**
>
> Die hier beschriebenen Schritte zeigen, wie Sie Endpunkte in der Konsole hinzufügen. Wenn Sie den Beschleuniger programmgesteuert erstellen, fügen Sie Endpunkte mit Endpunktgruppen hinzu. Weitere Informationen finden Sie unterCreateCustomRoutingendPointGroupimAWS Global Accelerator -API.

Hinzufügen von Endpunkten

1. Klicken Sie auf derHinzufügen von Endpunktenim Abschnitt für die Endpunktgruppe, der Sie den Endpunkt hinzufügen möchten, eine Subnetz-ID für-Endpunkt.
2. Führen Sie optional einen der folgenden Schritte aus, um Datenverkehr zu EC2-Instance-Zielen im Subnetz zu aktivieren:
   - Damit der Datenverkehr an alle EC2-Endpunkte und Ports im Subnetz weitergeleitet werden kann, wählen SieAllen Datenverkehr zulassen
   - Um Datenverkehr zu bestimmten EC2-Endpunkten und Ports im Subnetz zuzulassen, wählen SieDatenverkehr zu bestimmten Ziel-Socket-Adressen zulassen. Geben Sie dann die IP-Adressen und Ports oder Portbereiche an, die zugelassen werden sollen. Wählen Sie abschließend die OptionDiese Ziele zulassen.

Standardmäßig ist kein Datenverkehr für Subnetz-Endpunkte zulässig. Wenn Sie keine Option zum Zulassen von Datenverkehr auswählen, wird der Datenverkehr zu allen Zielen im Subnetz verweigert.

> **Note**
>
> Wenn Sie Datenverkehr zu bestimmten EC2-Instanzen und Ports im Subnetz aktivieren möchten, können Sie dies programmgesteuert tun. Weitere Informationen finden Sie unterAllowCustomRoutingTrafficimAWS Global Accelerator -API.

3. Wählen Sie Next.

Nachdem SieWeiterauf dem Global Accelerator Dashboard wird eine Meldung angezeigt, dass Ihr Accelerator in Bearbeitung ist. Wenn der Vorgang abgeschlossen ist, lautet der Accelerator-Status im DashboardAktiv.

Schritt 5 (optional): Löschen des Accelerators

Wenn Sie einen Accelerator als Test erstellt haben oder wenn Sie keinen Accelerator mehr verwenden, können Sie ihn löschen. Deaktivieren Sie auf der Konsole den Beschleuniger, und Sie können ihn dann löschen. Sie müssen keine Listener und Endpunktgruppen aus dem Accelerator entfernen.

Um einen Accelerator mithilfe eines API-Vorgangs anstelle der Konsole zu löschen, müssen Sie zuerst alle Listener und Endpunktgruppen entfernen, die dem Accelerator zugeordnet sind, sowie deaktivieren. Weitere Informationen finden Sie im .DeleteCustomRoutingAcceleratorOperation (Operation) imAWS Global Accelerator -API.

Beachten Sie beim Löschen eines Accelerators Folgendes:

- Wenn Sie einen Accelerator erstellen, stellt Ihnen Global Accelerator einen Satz von zwei statischen IP-Adressen zur Verfügung. Die IP-Adressen werden Ihrem Accelerator so lange zugewiesen, wie er existiert, auch wenn Sie den Accelerator deaktivieren und der Datenverkehr nicht mehr akzeptiert oder weiterleitet. Allerdings, wenn Siedeleteeinen Beschleuniger verwenden, verlieren Sie die statischen IP-Adressen, die dem Beschleuniger zugewiesen sind, sodass Sie den Datenverkehr nicht mehr mithilfe dieser Adressen weiterleiten können. Stellen Sie als bewährte Methode sicher, dass Sie über Berechtigungen verfügen, um ein versehentliches Löschen von

Beschleunigern zu vermeiden. Sie können IAM-Richtlinien wie tag-basierte Berechtigungen mit Global Accelerator verwenden, um die Benutzer einzuschränken, die über Berechtigungen zum Löschen eines Accelerators verfügen. Weitere Informationen finden Sie unter Tagbasierte Richtlinien.

Löschen eines Accelerators

1. Öffnen Sie die Global Accelerator-Konsole unterhttps://console.aws.amazon.com/globalaccelerator/home.
2. Wählen Sie den Accelerator aus, den Sie löschen möchten.
3. Wählen Sie Edit (Bearbeiten) aus.
4. Klicken Sie aufDeaktivieren des AcceleratorsKlicken Sie auf und danach auf.Save.
5. Wählen Sie den Accelerator aus, den Sie löschen möchten.
6. Klicken Sie aufLöschen Accelerator.
7. Wählen Sie im Bestätigungsdialogfeld die Option Delete (Löschen).

Häufige Aktionen, die Sie mit AWS Global Accelerator verwenden können

In diesem Abschnitt werden allgemeine AWS Global Accelerator Aktionen aufgeführt, die Sie mit Global Accelerator-Ressourcen verwenden können, sowie Links zu relevanten Dokumentationen.

Aktionen, die mit Standardressourcen verwendet werden sollen

In der folgenden Tabelle sind allgemeine Global Accelerator-Aktionen aufgeführt, die Sie mit Global Accelerator-Standardbeschleunigern verwenden können, sowie Links zu relevanten Dokumentationen.

Action	Verwenden der Global Accelerator Console	Verwenden der Global Accelerator-API-
Erstellen eines Standard-Beschleunigers	Siehe Erste Schritte mit einem Standard-Accelerator	Siehe `CreateAccelerator`
Einen Listener für einen Standard-Accelerator erstellen	Siehe Listener für Standardbeschleuniger in AWS Global Accelerator	Siehe `CreateListener`
Erstellen einer Endpunktgruppe für einen Standardbeschleuniger	Siehe Endpunktgruppen für Standardbeschleuniger in AWS Global Accelerator	Siehe `CreateEndpointGroup`
Aktualisieren eines Standard-Beschleunigers	Siehe AWS Global Accelerator	Siehe `UpdateAccelerator`
Listen Sie Ihre Beschleuniger auf	Siehe Anzeigen Ihrer Beschleuniger	Siehe `ListAccelerator`
Alle Informationen zu einem -Accelerator abrufen	Siehe Anzeigen Ihrer Beschleuniger	Siehe `DescribeAccelerator`
Löschen eines -Accelerators	Siehe Erstellen oder Aktualisieren eines Standard-Beschleunigers	Siehe `DeleteAccelerator`

Aktionen, die mit benutzerdefinierten Routingressourcen verwendet werden sollen

In der folgenden Tabelle sind allgemeine Global Accelerator-Aktionen aufgeführt, die Sie mit benutzerdefinierten Routing-Beschleunigern verwenden können, sowie Links zu relevanten Dokumentationen.

Action	Verwenden der Global Accelerator Console	Verwenden der Global Accelerator-API-
Erstellen eines benutzerdefinierten Routing-Accelerators	Siehe Erste Schritte mit einem benutzerdefinierten Routing-Accelerator	Siehe `CreateCustomRoutingAccelerator`
Erstellen eines Listeners für einen benutzerdefinierten Routing-Accelerator	Siehe Listener für benutzerdefinierte Routing-Beschleuniger in AWS Global Accelerator	Siehe `CreateCustomRoutingListener`
Erstellen einer Endpunktgruppe für einen benutzerdefinierten Routing-Accelerator	Siehe Endpunktgruppen für benutzerdefinierte Routing-Beschleuniger in AWS Global Accelerator	Siehe `CreateCustomRoutingEndpointGroup`
Aktualisieren eines benutzerdefinierten Routing-Beschleunigers	Siehe Benutzerdefinierte Routing-Beschleuniger in AWS Global Accelerator	Siehe `UpdateCustomRoutingAccelerator`
Listen Sie Ihre benutzerdefinierten Routing-Beschleuniger auf	Siehe Anzeigen Ihrer benutzerdefinierten Routing-Beschleuniger	Siehe `ListCustomRoutingAccelerator`
Alle Informationen zu einem benutzerdefinierten Routing-Accelerator	Siehe Anzeigen Ihrer benutzerdefinierten Routing-Beschleuniger	Siehe `DescribeCustomRoutingAccelerator`
Löschen eines benutzerdefinierten Routing-Beschleunigers	Siehe Erstellen oder Aktualisieren eines benutzerdefinierten Routing-Accelerators	Siehe `DeleteCustomRoutingAccelerator`

Action	Verwenden der Global Accelerator Console	Verwenden der Global Accelerator-API-
Abrufen der statischen Portzuordnung für einen benutzerdefinierten Routing-Accelerator	–	Siehe `ListCustomRoutingPortMappings`
Allen Zieldatenverkehr für ein Subnetz in einem benutzerdefinierten Routingbeschleuniger zulassen	Siehe Hinzufügen, Bearbeiten oder Entfernen eines VPC - Subnetzendpunkts	Siehe `AllowCustomRoutingTraffic`
Verweigern des gesamten Zielverkehrs für ein Subnetz in einem benutzerdefinierten Routingbeschleuniger	Siehe Hinzufügen, Bearbeiten oder Entfernen eines VPC - Subnetzendpunkts	Siehe `DenyCustomRoutingTraffic`
Zuweisen von Datenverkehr zu bestimmten Zielen in einem benutzerdefinierten Routingbeschleuniger	Siehe Hinzufügen, Bearbeiten oder Entfernen eines VPC - Subnetzendpunkts	Siehe `AllowCustomRoutingTraffic`
Datenverkehr zu bestimmten Zielen in einem benutzerdefinierten Routingbeschleuniger verweigern	Siehe Hinzufügen, Bearbeiten oder Entfernen eines VPC - Subnetzendpunkts	Siehe `DenyCustomRoutingTraffic`

Arbeiten mit Standard-Beschleunigern in AWS Global Accelerator

Dieses Kapitel enthält Verfahren und Empfehlungen zum Erstellen von Standardbeschleunigern in AWS Global Accelerator. Mit einem Standardbeschleuniger wählt Global Accelerator den nächstgelegenen fehlerfreien Endpunkt für Ihren Datenverkehr aus.

Wenn Sie stattdessen eine benutzerdefinierte Anwendungslogik verwenden möchten, um einen oder mehrere Benutzer an einen bestimmten Endpunkt unter vielen Endpunkten zu verweisen, erstellen Sie einen benutzerdefinierten Routingbeschleuniger. Weitere Informationen finden Sie unter Arbeiten mit benutzerdefinierten Routing-Beschleunigern in AWS Global Accelerator.

Um einen Standardbeschleuniger einzurichten, gehen Sie wie folgt vor:

1. Erstellen Sie einen Beschleuniger, und wählen Sie die Standardbeschleuniger-Option.
2. Fügen Sie einen Listener mit einem bestimmten Satz von Ports oder Portbereich hinzu, und wählen Sie das Protokoll aus, das akzeptiert werden soll: TCP, UDP oder beides.
3. Fügen Sie eine oder mehrere Endpunktgruppen hinzu, eine für jede AWS Region, in der Sie über Endpunktressourcen verfügen.
4. Fügen Sie Endpunktgruppen einen oder mehrere Endpunkte hinzu. Dies ist nicht erforderlich, aber der Datenverkehr wird nicht weitergeleitet, wenn Sie keine Endpunkte haben. Endpunkte können Network Load Balancers, Application Load Balancers, Amazon EC2 Instances oder Elastic IP-Adressen sein.

In den folgenden Abschnitten wird die Arbeit mit Standardbeschleunigern, Listener, Endpunktgruppen und Endpunkten erläutert.

Themen

- AWS Global Accelerator
- Listener für Standardbeschleuniger in AWS Global Accelerator
- Endpunktgruppen für Standardbeschleuniger in AWS Global Accelerator
- Endpunkte für Standardbeschleuniger in AWS Global Accelerator

AWS Global Accelerator

AStandard-AcceleratorIn AWS Global Accelerator Jeder Beschleuniger enthält einen oder mehrere Zuhörer. Ein Listener verarbeitet eingehende Verbindungen von Clients zu Global Accelerator, basierend auf dem von Ihnen konfigurierten Protokoll (oder den Protokollen) und Port (oder Portbereich).

Wenn Sie einen Accelerator erstellen, stellt Ihnen Global Accelerator standardmäßig zwei statische IP-Adressen zur Verfügung. Wenn Sie AWS (BYOIP) einen eigenen IP-Adressbereich hinzufügen, können Sie stattdessen statische IP-Adressen aus Ihrem eigenen Pool zuweisen, um sie mit Ihrem Accelerator zu verwenden. Weitere Informationen finden Sie unter Bring Your Own IP Addresses (BYOIP) in AWS Global Accelerator.

> **Important**
>
> Die IP-Adressen werden Ihrem Accelerator so lange zugewiesen, wie er existiert, auch wenn Sie den Accelerator deaktivieren und der Datenverkehr nicht mehr akzeptiert oder weiterleitet. Allerdings, wenn Siedeleteeinen Beschleuniger verwenden, verlieren Sie die statischen IP-Adressen von Global Accelerator, die dem Beschleuniger zugewiesen sind, sodass Sie den Datenverkehr nicht mehr mithilfe dieser Adressen weiterleiten können. Stellen Sie als bewährte Methode sicher, dass Sie über Berechtigungen verfügen, um ein versehentliches Löschen von Beschleunigern zu vermeiden. Sie können IAM-Richtlinien mit Global Accelerator verwenden, z. B. tagbasierte Berechtigungen, um die Benutzer einzuschränken, die über Berechtigungen zum Löschen eines Accelerators verfügen. Weitere Informationen finden Sie unter Tagbasierte Richtlinien.

In diesem Abschnitt wird erläutert, wie Sie einen Standardbeschleuniger in der Global Accelerator-Konsole erstellen, bearbeiten oder löschen. Wenn Sie API-Operationen mit Global Accelerator verwenden möchten, finden Sie weitere Informationen unterAWS Global Accelerator.

Themen

- Erstellen oder Aktualisieren eines Standard-Beschleunigers
- Löscht eines Accelerators
- Anzeigen Ihrer Beschleuniger
- Hinzufügen eines Accelerators
- Verwenden von globalen statischen IP-Adressen anstelle von regionalen statischen IP-Adressen

Erstellen oder Aktualisieren eines Standard-Beschleunigers

Dieser Abschnitt erläutert, wie Sie Standard-Acceleratoren auf der Konsole erstellen oder aktualisieren. Informationen zum programmgesteuerten Arbeiten mit Global Accelerator finden Sie imAWS Global Accelerator.

So erstellen Sie einen Standard-Accelerator

1. Öffnen Sie die Global Accelerator-Konsole unterhttps://console.aws.amazon.com/globalaccelerator/home.
2. Klicken Sie aufErstellt Accelerator.
3. Geben Sie einen Namen für Ihren Accelerator an.
4. Für-AcceleratorWählen SieStandard-.
5. Wenn Sie Ihre eigenen IP-Adressbereiche in AWS (BYOIP) übertragen haben, können Sie optional eine statische IP-Adresse für Ihren Accelerator angeben, eine aus jedem Adresspool. Treffen Sie diese Wahl für jede der beiden statischen IP-Adressen für Ihren Beschleuniger.
   - Wählen Sie für jede statische IP-Adresse den IP-Adresspool aus, der verwendet werden soll.

     > **Note**
     >
     > Sie müssen für jede statische IP-Adresse einen anderen IP-Adresspool auswählen. Diese Einschränkung liegt daran, dass Global Accelerator für hohe Verfügbarkeit jeden Adressbereich einer anderen Netzwerkzone zuweist.

   - Wenn Sie Ihren eigenen IP-Adresspool ausgewählt haben, wählen Sie auch eine bestimmte IP-Adresse aus dem Pool. Wenn Sie den Standard-IP-Adresspool von Amazon auswählen, weist Global Accelerator Ihrem Beschleuniger eine bestimmte IP-Adresse zu.
6. Optional können Sie ein oder mehrere Tags hinzufügen, um Ihnen bei der Identifizierung Ihrer Accelerator-Ressourcen zu helfen.
7. Klicken Sie aufWeiter, um Listener, Endpunktgruppen und Endpunkte hinzuzufügen.

So bearbeiten Sie einen Standardbeschleuniger

1. Öffnen Sie die Global Accelerator-Konsole unterhttps://console.aws.amazon.com/globalaccelerator/home.
2. Wählen Sie in der Liste der Acceleratoren einBearbeiten.

3. Klicken Sie auf derBearbeiten des AcceleratorsNehmen Sie alle gewünschten Änderungen vor. Beispielsweise können Sie den Beschleuniger deaktivieren, damit er den Datenverkehr nicht mehr akzeptiert oder weiterleitet oder Sie ihn löschen können. Wenn der Beschleuniger deaktiviert ist, können Sie ihn auch aktivieren.
4. Wählen Sie Save Changes.

Löscht eines Accelerators

Wenn Sie einen Accelerator als Test erstellt haben oder wenn Sie keinen Accelerator mehr verwenden, können Sie ihn löschen. Deaktivieren Sie auf der Konsole den Beschleuniger, und Sie können ihn dann löschen. Sie müssen keine Listener und Endpunktgruppen aus dem Accelerator entfernen.

Wenn Sie einen Accelerator mithilfe eines API-Vorgangs anstelle der Konsole löschen möchten, müssen Sie zuerst alle Listener und Endpunktgruppen entfernen, die dem Accelerator zugeordnet sind, und dann deaktivieren. Weitere Informationen finden Sie im .DeleteAccelerator-Operation imAWS Global Accelerator.

So deaktivieren Sie einen Accelerator

1. Öffnen Sie die Global Accelerator-Konsole unterhttps://console.aws.amazon.com/globalaccelerator/home.
2. Wählen Sie in der Liste ein Accelerator aus, das Sie deaktivieren möchten.
3. Wählen Sie Edit (Bearbeiten) aus.
4. Klicken Sie aufDeaktivieren des AcceleratorsKlicken Sie auf und danach aufSave.

So löschen Sie einen Accelerator

1. Öffnen Sie die Global Accelerator-Konsole unterhttps://console.aws.amazon.com/globalaccelerator/home.
2. Wählen Sie in der Liste ein Accelerator aus, das Sie löschen möchten.
3. Wählen Sie Delete.

> **Note**
>
> Wenn Sie den Accelerator nicht deaktiviert haben,Löschenist nicht verfügbar.

4. Wählen Sie im Bestätigungsdialogfeld die Option Delete (Löschen).

> **Important**
>
> Wenn Sie einen Accelerator löschen, verlieren Sie die statischen IP-Adressen, die dem Beschleuniger zugewiesen sind, sodass Sie den Datenverkehr nicht mehr mithilfe dieser Adressen weiterleiten können.

Anzeigen Ihrer Beschleuniger

Sie können auf der Konsole Informationen zu Ihren Acceleratoren anzeigen. Informationen zu Beschreibungen Ihrer Beschleuniger programmgesteuert finden Sie unterListAcceleratorsundDescribeAcceleratorimAWS Global Accelerator.

So zeigen Sie Informationen über Ihren Accelerator

1. Öffnen Sie die Global Accelerator-Konsole unterhttps://console.aws.amazon.com/globalaccelerator/home.
2. Um Details zu einem Beschleuniger anzuzeigen, wählen Sie in der Liste einen Beschleuniger aus, und wählen Sie dannAnzeigen.

Hinzufügen eines Accelerators

Wenn Sie einen Application Load Balancer in der AWS Management Console erstellen, können Sie optionalGleichzeitig einen Accelerator. Elastic Load Balancing und Global Accelerator arbeiten zusammen, um den Beschleuniger transparent für Sie hinzuzufügen. Der Accelerator wird in Ihrem Konto erstellt, wobei der Load Balancer als Endpunkt dient. Mit einem Accelerator werden statische IP-Adressen bereitgestellt und die Verfügbarkeit und Leistung Ihrer Anwendungen verbessert.

> **Important**
>
> Zum Erstellen eines Accelerators benötigen Sie die richtigen Berechtigungen. Weitere Informationen finden Sie unter Erforderliche Berechtigungen für den Konsolenzugriff, die Authentifizierungsverwaltung und die Zugriffssteuerung.

Konfigurieren und Anzeigen des Beschleunigers

Sie müssen Ihre DNS-Konfiguration aktualisieren, um den Datenverkehr auf die statischen IP-Adressen oder den DNS-Namen für den Beschleuniger zu leiten. Der Datenverkehr wird erst durch den Beschleuniger zu Ihrem Load Balancer geleitet, wenn die Konfigurationsänderungen abgeschlossen sind.

Nachdem Sie Ihren Load Balancer erstellt haben, indem Sie das Global Accelerator-Add-on auf der Amazon EC2 Konsole auswählen, rufen Sie dieIntegrierte Services, um die statischen IP-Adressen und den DNS-Namen (Domain Name System) für Ihren Accelerator anzuzeigen. Sie verwenden diese Informationen, um den Benutzerverkehr über das globale AWS Netzwerk an den Lastausgleichsdienst weiterzuleiten. Weitere Informationen zum DNS-Namen, der Ihrem Accelerator zugewiesen ist, finden Sie unterDNS-Adressierung und benutzerdefinierte Domänen in AWS Global Accelerator.

Sie können Ihren Accelerator anzeigen und konfigurieren, indem SieNavigieren zum Global AcceleratorIn der AWS Management Console. Sie können beispielsweise die Accelerators sehen, die Ihrem Konto zugeordnet sind, oder zusätzliche Load Balancer zu Ihrem Accelerator hinzufügen. Weitere Informationen finden Sie unter Anzeigen Ihrer Beschleuniger und Erstellen oder Aktualisieren eines Standard-Beschleunigers.

Preise

Mit AWS Global Accelerator Ihnen werden ein Stundensatz und Datenübertragungskosten für jeden Accelerator in Ihrem Konto in Rechnung gestellt. Weitere Informationen finden Sie unterAWS Global Accelerator.

Verwenden des Accelerators

Wenn Sie das Routing von Datenverkehr über Global Accelerator an Ihren Load Balancer beenden möchten, gehen Sie wie folgt vor:

1. Aktualisieren Sie Ihre DNS-Konfiguration, um Ihren Datenverkehr direkt auf den Load Balancer zu verweisen.
2. Löschen Sie den Load Balancer aus dem Accelerator. Weitere Informationen finden Sie unterSo entfernen Sie einen Endpunkt:inHinzufügen, Bearbeiten oder Entfernen eines Standard-Endpunkts.
3. Löscht den Accelerator. Weitere Informationen finden Sie unter Löscht eines Accelerators.

Verwenden von globalen statischen IP-Adressen anstelle von regionalen statischen IP-Adressen

Wenn Sie eine statische IP-Adresse vor einer AWS Ressource, z. B. einer Amazon EC2 Instance, verwenden möchten, haben Sie mehrere Optionen. Sie können beispielsweise eine Elastic IP-Adresse zuweisen, bei der es sich um eine statische IPv4-Adresse handelt, die Sie einer Amazon EC2 Instance oder einer Netzwerkschnittstelle in einer einzelnen AWS Region zuordnen können.

Wenn Sie eine globale Zielgruppe haben, können Sie mit Global Accelerator einen Accelerator erstellen, um zwei globale statische IP-Adressen zu erhalten, die von AWS Edge-Standorten auf der ganzen Welt angekündigt werden. Wenn Sie bereits AWS Ressourcen für Ihre Anwendungen in einer oder mehreren Regionen eingerichtet haben, einschließlich Amazon EC2 Instances, Network Load Balancers und Application Load Balancers, können Sie diese einfach zu Global Accelerator hinzufügen, um sie mit globalen statischen IP-Adressen zu versorgen.

Wenn Sie globale statische IP-Adressen verwenden, die von Global Accelerator bereitgestellt werden, können Sie auch die Verfügbarkeit und Leistung Ihrer Anwendungen verbessern. Mit Global Accelerator akzeptieren statische IP-Adressen eingehenden Datenverkehr in das globale AWS Netzwerk von der Edge-Position, die Ihren Benutzern am nächsten liegt. Die Maximierung der Zeit für den Datenverkehr im AWS Netzwerk kann eine schnellere und bessere Kundenerfahrung bieten. Weitere Informationen finden Sie unter Funktionsweise von AWS Global Accelerator.

Sie können einen Beschleuniger über die AWS Management Console oder mithilfe von API-Vorgängen mit der AWS CLI oder SDKs hinzufügen. Weitere Informationen finden Sie unter Erstellen oder Aktualisieren eines Standard-Beschleunigers.

Beachten Sie beim Hinzufügen eines Accelerators Folgendes:

- Die globalen statischen IP-Adressen, die von Global Accelerator bereitgestellt werden, bleiben Ihnen so lange zugewiesen, wie Ihr Accelerator vorhanden ist, auch wenn Sie den Accelerator deaktivieren und der Datenverkehr nicht mehr akzeptiert oder weiterleitet. Wenn Sie jedoch einen Beschleuniger löschen, verlieren Sie die ihm zugewiesenen statischen IP-Adressen. Weitere Informationen finden Sie unter Löscht eines Accelerators.
- Mit Global Accelerator Ihnen werden ein Stundensatz und Datenübertragungskosten für jeden Accelerator in Ihrem Konto in Rechnung gestellt. Weitere Informationen finden Sie unterAWS Global Accelerator.

Listener für Standardbeschleuniger in AWS Global Accelerator

Mit AWS Global Accelerator fügen Sie Listener hinzu, die eingehende Verbindungen von Clients basierend auf den von Ihnen angegebenen Ports und Protokollen verarbeiten. Listener unterstützen TCP, UDP oder beide TCP- und UDP-Protokolle.

Sie definieren einen Standard-Listener, wenn Sie Ihren Standard-Accelerator erstellen, und Sie können jederzeit weitere Listener hinzufügen. Sie verknüpfen jeden Listener einer oder mehreren Endpunktgruppen und ordnen jede Endpunktgruppe einer AWS Region zu.

Themen

- Hinzufügen, Bearbeiten oder Entfernen eines Standardlisteners
- Client-Affinität

Hinzufügen, Bearbeiten oder Entfernen eines Standardlisteners

In diesem Abschnitt wird erläutert, wie Sie mit Listener auf der AWS Global Accelerator Konsole arbeiten. Informationen zum Ausführen dieser Aufgaben mithilfe eines API-Vorgangs anstelle der Konsole finden Sie unter`CreateListener`,`UpdateListener`, und`DeleteListener`imAWS Global Accelerator -API-Referenz.

So fügen Sie einen Listener hinzu

1. Öffnen Sie die Global Accelerator-Konsole unterhttps://console.aws.amazon.com/globalaccelerator/home.
2. Klicken Sie auf der-AcceleratorsWählen Sie einen Accelerator aus.
3. Wählen Sie Add listener (Listener hinzufügen) aus.
4. Klicken Sie auf derListener hinzufügendie Ports oder Portbereiche ein, die Sie dem Listener zuordnen möchten. Listener unterstützen die Ports 1-65535.
5. Wählen Sie das Protokoll für die eingegebenen Ports.
6. Optional können Sie die Clientaffinität aktivieren. Clientaffinität für einen Listener bedeutet, dass Global Accelerator sicherstellt, dass Verbindungen von einer bestimmten Quell-IP-Adresse (Client) immer an denselben Endpunkt weitergeleitet werden. Um dieses Verhalten zu aktivieren, wählen Sie in der Dropdown-ListeQuell-IP.

Der Standardwert istKeine, was bedeutet, dass die Clientaffinität nicht aktiviert ist und Global Accelerator den Datenverkehr gleichmäßig zwischen den Endpunkten in den Endpunktgruppen für den Listener verteilt.

Weitere Informationen finden Sie unter Client-Affinität.

7. Wählen Sie Add listener (Listener hinzufügen) aus.

So bearbeiten Sie einen Standardlistener

1. Öffnen Sie die Global Accelerator-Konsole unterhttps://console.aws.amazon.com/globalaccelerator/home.
2. Klicken Sie auf der-AcceleratorsWählen Sie einen Accelerator aus.
3. Wählen Sie einen Listener aus und wählen Sie dannListener bearbeiten.
4. Klicken Sie auf derListener bearbeitendie Ports, Portbereiche oder Protokolle, die Sie dem Listener zuordnen möchten.
5. Optional können Sie die Clientaffinität aktivieren. Clientaffinität für einen Listener bedeutet, dass Global Accelerator sicherstellt, dass Verbindungen von einer bestimmten Quell-IP-Adresse (Client) immer an denselben Endpunkt weitergeleitet werden. Um dieses Verhalten zu aktivieren, wählen Sie in der Dropdown-ListeQuell-IP.

   Der Standardwert istKeine, was bedeutet, dass die Clientaffinität nicht aktiviert ist und Global Accelerator den Datenverkehr gleichmäßig zwischen den Endpunkten in den Endpunktgruppen für den Listener verteilt.

   Weitere Informationen finden Sie unter Client-Affinität.
6. Wählen Sie Save (Speichern) aus.

So entfernen Sie einen Listener

1. Öffnen Sie die Global Accelerator-Konsole unterhttps://console.aws.amazon.com/globalaccelerator/home.
2. Klicken Sie auf der-AcceleratorsWählen Sie einen Accelerator aus.
3. Wählen Sie einen Listener aus und wählen Sie dannRemove.
4. Wählen Sie im -BestätigungsdialogfeldRemove.

Client-Affinität

Wenn Sie über statusbehaftete Anwendungen verfügen, die Sie mit einem Standardbeschleuniger verwenden, können Sie festlegen, dass Global Accelerator alle Anforderungen eines Benutzers an eine bestimmte Quell-IP-Adresse (Client) an dieselbe Endpunktressource weiterleitet, um die Clientaffinität aufrechtzuerhalten.

Standardmäßig ist die Clientaffinität für einen Standardlistener aufKeineund Global Accelerator verteilt den Datenverkehr gleichmäßig zwischen den Endpunkten in den Endpunktgruppen für den Listener.

Global Accelerator verwendet einen Hash-Algorithmus mit konsistenten Ablläufen, um den optimalen Endpunkt für die Verbindung eines Benutzers auszuwählen. Wenn Sie die Clientaffinität für Ihre Global Accelerator-Ressource so konfigurieren, dassKeineWenn Sie den Hash-Wert anhand der Eigenschaften von fünf Tupeln — Quell-IP, Quell-Port, Ziel-IP-Adresse, Ziel-Port und Protokoll — auswählen. Als Nächstes wählt er den Endpunkt aus, der die beste Leistung bietet. Wenn ein Client andere Ports für die Verbindung zu Global Accelerator nutzt und Sie diese Einstellung festgelegt haben, kann Global Accelerator nicht sicherstellen, dass Verbindungen vom Client immer an denselben Endpunkt weitergeleitet werden.

Wenn Sie die Clientaffinität beibehalten möchten, indem Sie bei jeder Verbindung einen bestimmten Benutzer (identifiziert durch seine Quell-IP-Adresse) an denselben Endpunkt weiterleiten, setzen Sie die Clientaffinität aufQuell-IP. Wenn Sie diese Option angeben, wählt Global Accelerator den Hash-Wert anhand der Eigenschaften von zwei Tupeln — Quell-IP und Ziel-IP — aus und leitet den Benutzer an denselben Endpunkt weiter, wenn er eine Verbindung hat. Global Accelerator berücksichtigt die Clientaffinität nach der ausgewählten Endpunktgruppe.

Endpunktgruppen für Standardbeschleuniger in AWS Global Accelerator

Eine Endpunktgruppe leitet Anforderungen an einen oder mehrere registrierte Endpunkte in AWS Global Accelerator weiter. Wenn Sie einen Listener in einem Standardbeschleuniger hinzufügen, geben Sie die Endpunktgruppen für Global Accelerator an, an die der Datenverkehr weitergeleitet werden soll. Eine Endpunktgruppe und alle darin enthaltenen Endpunkte müssen sich in einer AWS Region befinden. Sie können verschiedene Endpunktgruppen für verschiedene Zwecke hinzufügen, z. B. für blau/grüne Bereitstellungstests.

Global Accelerator leitet Datenverkehr an Endpunktgruppen in Standardbeschleunigern basierend auf dem Standort des Clients und der Integrität der Endpunktgruppe weiter. Wenn Sie möchten, können Sie auch den Prozentsatz des Datenverkehrs festlegen, der an eine Endpunktgruppe gesendet werden soll. Verwenden Sie dies, indem Sie den Datenverkehr verwenden, um den Datenverkehr an die Gruppe zu erhöhen (nach oben zu skalieren) oder zu verringern (nach unten zu skalieren). Der Prozentsatz wird nur auf den Datenverkehr angewendet, den Global Accelerator bereits an die Endpunktgruppe weiterleitet, nicht auf den gesamten Datenverkehr, der zu einem Listener kommt.

Sie können Integritätsprüfungseinstellungen für Global Accelerator für jede Endpunktgruppe definieren. Durch die Aktualisierung der Integritätsprüfungseinstellungen können Sie Ihre Anforderungen für die Abfrage und Überprüfung der Integrität von Amazon EC2 Instances und Elastic IP-Adressenendpunkten ändern. Konfigurieren Sie für Network Load Balancer und Application Load Balancer -Endpunkte die Einstellungen für die Integritätsprüfung in der Elastic Load Balancing Konsole.

Global Accelerator überwacht kontinuierlich die Integrität aller Endpunkte, die in einer Standard-Endpunktgruppe enthalten sind, und leitet Anforderungen nur an die aktiven Endpunkte weiter, die fehlerfrei sind. Wenn keine fehlerfreien Endpunkte zum Weiterleiten des Datenverkehrs vorhanden sind, leitet Global Accelerator Anforderungen an alle Endpunkte weiter.

In diesem Abschnitt wird erläutert, wie Sie mit Endpunktgruppen für Standardbeschleuniger in der AWS Global Accelerator Konsole arbeiten. Wenn Sie API-Vorgänge mit AWS Global Accelerator verwenden möchten, finden Sie weitere Informationen unterAWS Global Accelerator -API.

Themen

- Hinzufügen, Bearbeiten oder Entfernen einer Standard-Endpunktgruppe
- Anpassen des Verkehrsflusses mit Verkehrszifferblättern
- Port-Überschreibungen
- Zustandsprüfungsoptionen

Hinzufügen, Bearbeiten oder Entfernen einer Standard-Endpunktgruppe

Sie arbeiten mit Endpunktgruppen in der AWS Global Accelerator Konsole oder verwenden einen API-Vorgang. Sie können jederzeit Endpunktgruppen hinzufügen oder aus dieser entfernen.

In diesem Abschnitt wird erläutert, wie Sie mit Standard-Endpunktgruppen auf der AWS Global Accelerator Konsole arbeiten. Wenn Sie API-Vorgänge mit Global Accelerator verwenden möchten, finden Sie weitere Informationen unterAWS Global Accelerator -API.

So fügen Sie eine Standard-Endpunktgruppe hinzu

1. Öffnen Sie die Global Accelerator-Konsole unterhttps://console.aws.amazon.com/globalaccelerator/home.
2. Klicken Sie auf der-AcceleratorsWählen Sie einen Accelerator aus.
3. In derListenerAbschnitts erstellt, fürListener-IDWählen Sie die ID des Listeners, dem Sie eine Endpunktgruppe hinzufügen möchten.
4. Klicken Sie aufHinzufügen von Endpunktgruppen.
5. Geben Sie im Abschnitt für einen Listener eine Region für die Endpunktgruppe an, indem Sie eine Region aus der Dropdown-Liste auswählen.
6. Optional fürTraffic-Zifferblatteine Zahl zwischen 0 und 100 ein, um einen Prozentsatz des Datenverkehrs für diese Endpunktgruppe festzulegen. Der Prozentsatz wird nur auf den Datenverkehr angewendet, der bereits an diese Endpunktgruppe geleitet ist, nicht auf den gesamten Listener-Datenverkehr. Standardmäßig ist die Verkehrswahl auf 100 festgelegt.
7. Optional können Sie den Listener-Port überschreiben, der für das Routing von Datenverkehr an Endpunkte verwendet wird, und den Datenverkehr an bestimmte Ports auf Ihren Endpunkten umleiten, indem SieKonfigurieren von Portüberschreibungen. Weitere Informationen finden Sie unter Port-Überschreibungen.
8. Optional können Sie benutzerdefinierte Integritätsprüfungswerte angeben, die auf EC2-Instanzen und Elastic IP-Adressenendpunkte angewendet werden sollen, wählen SieKonfigurieren von Zustandsprüfungen. Weitere Informationen finden Sie unter Zustandsprüfungsoptionen.
9. Wählen Sie optional die OptionHinzufügen von EndpunktgruppenSo fügen Sie zusätzliche Endpunktgruppen für diesen Listener oder andere Listeners hinzu.
10. Klicken Sie aufHinzufügen von Endpunktgruppen.

So bearbeiten Sie eine Endpunktgruppe

1. Öffnen Sie die Global Accelerator-Konsole unterhttps://console.aws.amazon.com/globalaccelerator/home.
2. Klicken Sie auf der-AcceleratorsWählen Sie einen Accelerator aus.
3. In derListenerAbschnitts erstellt, fürListener-IDWählen Sie die ID des Listeners, dem die Endpunktgruppe zugeordnet ist.
4. Klicken Sie aufBearbeiten von Endpunktgruppen.

5. Klicken Sie auf derBearbeiten von Endpunktgruppendie Region, passen Sie den Prozentsatz der Verkehrswahl an, oder wählen SieKonfigurieren von Zustandsprüfungen, um die Zustandsprüfungseinstellungen zu ändern.
6. Wählen Sie Save (Speichern) aus.

So entfernen Sie eine Standard-Endpunktgruppe

1. Öffnen Sie die Global Accelerator-Konsole unterhttps://console.aws.amazon.com/globalaccelerator/home.
2. Klicken Sie auf der-AcceleratorsWählen Sie einen Accelerator aus.
3. In derListenerWählen Sie einen Listener aus und wählen Sie dannRemove.
4. In derEndpunktgruppenWählen Sie eine Endpunktgruppe und dannRemove.
5. Wählen Sie im -BestätigungsdialogfeldRemove.

Anpassen des Verkehrsflusses mit Verkehrszifferblättern

Für jede Standard-Endpunktgruppe können Sie eine Verkehrswahl festlegen, um den Prozentsatz des Datenverkehrs zu steuern, der an die Gruppe geleitet wird. Der Prozentsatz wird nur auf Datenverkehr angewendet, der bereits an die Endpunktgruppe geleitet ist, nicht auf den gesamten Listener-Datenverkehr.

Standardmäßig ist die Verkehrswahl für alle regionalen Endpunktgruppen in einem Accelerator auf 100 (d. h. 100%) festgelegt. Mit der Verkehrswahl können Sie beispielsweise Performance-Tests oder blau/grüne Bereitstellungstests für neue Versionen in verschiedenen AWS Regionen durchführen.

Im Folgenden finden Sie einige Beispiele, die veranschaulichen, wie Sie Verkehrszifferblätter verwenden können, um den Verkehrsfluss in Endpunktgruppen zu ändern.

Aktualisieren Sie Ihre Anwendung nach Region

> Wenn Sie eine Anwendung in einer Region aktualisieren oder Wartungsarbeiten durchführen möchten, legen Sie zunächst die Verkehrswahl auf 0 fest, um den Datenverkehr für die Region zu unterbinden. Wenn Sie die Arbeit abgeschlossen haben und bereit sind, die Region wieder in Betrieb zu nehmen, stellen Sie die Verkehrswahl auf 100 ein, um den Datenverkehr wieder aufzunehmen.

Mix des Datenverkehrs zwischen zwei Regionen

Dieses Beispiel zeigt, wie der Verkehrsfluss funktioniert, wenn Sie die Verkehrswahlen für zwei regionale Endpunktgruppen gleichzeitig ändern. Angenommen, Sie haben zwei Endpunktgruppen für Ihren Beschleuniger — eine für die`us-west-2`Region und eine für die`us-east-1`Region — und Sie haben die Verkehrswahlen für jede Endpunktgruppe auf 50% festgelegt.

Nehmen wir an, Sie haben 100 Anfragen an Ihren Beschleuniger, mit 50 von der Ostküste der Vereinigten Staaten und 50 von der Westküste. Der Accelerator leitet den Datenverkehr wie folgt:

- Die ersten 25 Anfragen an jeder Küste (insgesamt 50 Anfragen) werden von der nahe gelegenen Endpunktgruppe bedient. Das heißt, 25 Anfragen werden an die Endpunktgruppe in`us-west-2`und 25 werden an die Endpunktgruppe in`us-east-1`.
- Die nächsten 50 Anfragen richten sich an die gegenüberliegenden Regionen. Das heißt, die nächsten 25 Anfragen von der Ostküste werden von`us-west-2`, und die nächsten 25 Anfragen von der Westküste werden von`us-east-1`.

Das Ergebnis in diesem Szenario ist, dass beide Endpunktgruppen die gleiche Menge an Datenverkehr bedienen. Jeder erhält jedoch eine Mischung aus Traffic aus beiden Regionen.

Port-Überschreibungen

Standardmäßig leitet ein Accelerator Benutzerverkehr mithilfe der Protokoll- und Portbereiche, die Sie beim Erstellen eines Listener angeben, an Endpunkte in AWS Regionen weiter. Wenn Sie beispielsweise einen Listener definieren, der TCP-Datenverkehr auf den Ports 80 und 443 akzeptiert, leitet der Accelerator Datenverkehr an diese Ports auf einem Endpunkt weiter.

Wenn Sie jedoch eine Endpunktgruppe hinzufügen oder aktualisieren, können Sie den Listener-Port überschreiben, der für das Routing von Datenverkehr an die Endpunktgruppen verwendet wird. Sie können beispielsweise eine Port-Überschreibung erstellen, bei der der Listener Benutzerverkehr auf den Ports 80 und 443 empfängt, Ihr Accelerator jedoch den Datenverkehr zu den Ports 1080 bzw. 1443 auf den Endpunkten leitet.

Port-Überschreibungen können Ihnen helfen, Probleme beim Abhören von eingeschränkten Ports zu vermeiden. Es ist sicherer, Anwendungen auszuführen, die keine Superuser-Privilegien (Root) auf Ihren Endpunkten benötigen. In Linux und anderen Unix-ähnlichen Systemen müssen Sie jedoch über Superuser-Berechtigungen verfügen, um eingeschränkte Ports (TCP- oder UDP-Ports unter 1024) zu hören. Durch Zuordnen eines eingeschränkten Ports auf einem Listener zu einem nicht

eingeschränkten Port auf einem Endpunkt können Sie dieses Problem vermeiden. Sie können Datenverkehr auf eingeschränkten Ports akzeptieren, während Sie Anwendungen ohne Root-Zugriff auf Ihre Endpunkte hinter Global Accelerator ausführen. Sie können beispielsweise einen Listener-Port 443 zu einem Endpunkt-Port 8443 überschreiben.

Für jede Portüberschreibung geben Sie einen Listener-Port an, der Datenverkehr von Benutzern akzeptiert, und den Endpunkt-Port an, an den Global Accelerator diesen Datenverkehr weiterleitet. Weitere Informationen finden Sie unter Hinzufügen, Bearbeiten oder Entfernen einer Standard-Endpunktgruppe.

Beachten Sie bei der Erstellung einer Portüberschreibung Folgendes:

- Endpoint-Ports können Listener-Portbereiche nicht überlappen. Die Endpunkt-Ports, die Sie in einer Portüberschreibung angeben, können nicht in einen der Listener-Portbereiche einbezogen werden, die Sie für den Accelerator konfiguriert haben. Angenommen, Sie haben zwei Listener für einen Beschleuniger, und Sie haben die Portbereiche für diese Listener als 100-199 bzw. 200-299 definiert. Wenn Sie Portüberschreibungen erstellen, können Sie keine von Listener-Port 100 bis Endpunkt-Port 210 definieren, z. B. weil der Endpunkt-Port (210) in einem von Ihnen definierten Listener-Portbereich (200-299) enthalten ist.
- Keine doppelten Endpunkt-Ports. Wenn ein Port Override in einem Accelerator einen Endpunktport angibt, können Sie nicht denselben Endpunktport mit Port-Override von einem anderen Listener-Port angeben. Sie können z. B. keine Portüberschreibung von Listener-Port 80 zu Endpunkt-Port 90 zusammen mit einer Überschreibung vom Listener-Port 81 zum Endpunkt-Port 90 angeben.
- Die Health sprüfung verwendet weiterhin den ursprünglichen Port. Wenn Sie eine Portüberschreibung für einen Port angeben, der als Zustandsprüfungsanschluss konfiguriert ist, verwendet die Zustandsprüfung weiterhin den ursprünglichen Port und nicht den Außerkraftsetzungsanschluss. Angenommen, Sie geben Integritätsprüfungen für Listener-Port 80 an, und Sie geben auch eine Portüberschreibung von Listener-Port 80 bis Endpunkt-Port 480 an. Health itätsprüfungen verwenden weiterhin Endpunktport 80. Benutzerverkehr, der über Port 80 eingeht, geht jedoch an Port 480 auf dem Endpunkt.

  Dieses Verhalten gewährleistet die Konsistenz zwischen Network Load Balancer, Application Load Balancer, EC2-Instance und Elastic IP-Adressenendpunkten. Da Network Load Balancers und Application Load Balancers keine Zustandsprüfungs-Ports einem anderen Endpunkt-Ports zuordnen, wenn Sie eine Portüberschreibung in Global Accelerator angeben, wäre es inkonsistent, wenn Global Accelerator Integritätsprüfungs-Ports verschiedenen Endpunkt-Ports für EC2-Instance und Elastic IP zuzuordnen Adressenendpunkte.

- Sicherheitsgruppeneinstellungen müssen den Port-Zugriff zulassen. Stellen Sie sicher, dass Ihre Sicherheitsgruppen den Datenverkehr an den Endpunktports ankommen, die Sie in Portüberschreibungen festgelegt haben. Wenn Sie beispielsweise Listener-Port 443 auf Endpunkt-Port 1433 überschreiben, stellen Sie sicher, dass alle in Ihrer Sicherheitsgruppe festgelegten Portbeschränkungen für diesen Application Load Balancer oder Amazon EC2 Endpunkt eingehenden Datenverkehr auf Port 1433 zulassen.

Zustandsprüfungsoptionen

AWS Global Accelerator sendet regelmäßig Anforderungen an Standard-Endpunkte, um deren Status zu überprüfen. Diese Integritätsprüfungen werden automatisch ausgeführt. Die Anleitungen zum Ermitteln der Integrität jedes Endpunkts und der Zeitpunkt für die Integritätsprüfungen hängen vom Typ der Endpunktressource ab.

> **Important**
>
> Global Accelerator erfordert, dass Ihre Router- und Firewallregeln eingehenden Datenverkehr von den IP-Adressen, die mit Route 53-Integritätsprüfungen verknüpft sind, zulassen, um Integritätsprüfungen für EC2-Instances oder Elastic IP-Adressenendpunkte abzuschließen. Informationen zu den IP-Adressbereichen, die mit Amazon Route 53 Health Checkers verknüpft sind, finden Sie unterZustandsprüfungen für Ihre ZielgruppenimAmazon Route 53 Entwicklerhandbuch.

Sie können die folgenden Integritätsprüfungsoptionen für eine Endpunktgruppe konfigurieren. Wenn Sie Integritätsprüfungsoptionen angeben, verwendet Global Accelerator die Einstellungen für EC2-Instanzen oder Elastic IP-Adressenintegritätsprüfungen, jedoch nicht für Network Load Balancers oder Application Load Balancers.

- Für Application Load Balancer oder Network Load Balancer Endpunkte konfigurieren Sie Integritätsprüfungen für die Ressourcen mithilfe von Elastic Load Balancing Konfigurationsoptionen. Weitere Informationen finden Sie unterZustandsprüfungen für Ihre Zielgruppen. Health itätsprüfungsoptionen, die Sie in Global Accelerator auswählen, wirken sich nicht auf Application Load Balancers oder Network Load Balancers aus, die Sie als Endpunkte hinzugefügt haben.

> **Note**
>
> Wenn Sie über einen Application Load Balancer oder Network Load Balancer verfügen, der mehrere Zielgruppen enthält, betrachtet Global Accelerator den Load Balancer-Endpunkt nur als fehlerfrei, wennEACHZielgruppe hinter dem Load Balancer hat mindestens ein fehlerfreies Ziel. Wenn eine einzelne Zielgruppe für den Lastausgleichsdienst nur fehlerhafte Ziele aufweist, betrachtet Global Accelerator den Endpunkt als fehlerhaft.

- Für EC2-Instanz- oder Elastic IP-Adressenendpunkte, die einem Listener hinzugefügt werden, der mit TCP konfiguriert ist, können Sie den Port angeben, der für Zustandsprüfungen verwendet werden soll. Wenn Sie keinen Port für Integritätsprüfungen angeben, verwendet Global Accelerator standardmäßig den Listener-Port, den Sie für den Accelerator angegeben haben.
- Für EC2-Instanz- oder Elastic IP-Adressenendpunkte mit UDP-Listener verwendet Global Accelerator den Listener-Port und das TCP-Protokoll für Integritätsprüfungen, sodass Sie einen TCP-Server auf Ihrem Endpunkt haben müssen.

> **Note**
>
> Stellen Sie sicher, dass der Port, den Sie für den TCP-Server auf jedem Endpunkt konfiguriert haben, mit dem Port identisch ist, den Sie für die Integritätsprüfung in Global Accelerator angeben. Wenn die Portnummern nicht identisch sind oder Sie keinen TCP-Server für den Endpunkt eingerichtet haben, markiert Global Accelerator den Endpunkt unabhängig von der Integrität des Endpunkts als fehlerhaft.

Health sprüfung

Der Port, der verwendet wird, wenn Global Accelerator die Zustandsprüfungen an den Endpunkten dieser Endpunktgruppe durchführt.

> **Note**
>
> Sie können keine Portüberschreibung für Zustandsprüfungsanschlüsse festlegen.

Health check protocol (Zustandsprüfungsprotokoll)

Das Protokoll, das verwendet wird, wenn Global Accelerator die Zustandsprüfungen an den Endpunkten dieser Endpunktgruppe durchführt.

Health sprüfung

Das Intervall in Sekunden zwischen den einzelnen Zustandsprüfungen für einen Endpunkt.

Schwellenwert-Anzahl

Die Anzahl fortlaufender Zustandsprüfungen, die erforderlich ist, damit ein Ziel als nicht betriebsbereit eingestuft wird.

Jeder Listener leitet Anfragen nur an fehlerfreie Endpunkte weiter. Nachdem Sie einen Endpunkt hinzugefügt haben, muss er eine Zustandsprüfung bestehen, um als fehlerfrei eingestuft zu werden. Nachdem die einzelnen Zustandsprüfungen abgeschlossen wurden, schließt der Listener die Verbindung, die für die Zustandsprüfung eingerichtet wurde.

Endpunkte für Standardbeschleuniger in AWS Global Accelerator

Endpunkte für Standardbeschleuniger in AWS Global Accelerator können Network Load Balancers, Application Load Balancers, Amazon EC2 Instances oder Elastic IP-Adressen sein. Bei Standard-Accelerators dient eine statische IP-Adresse als zentraler Kontaktpunkt für Clients und Global Accelerator verteilt eingehenden Datenverkehr dann an fehlerfreien Endpunkten. Global Accelerator leitet Datenverkehr an Endpunkte weiter, indem der Port (oder Portbereich) verwendet wird, den Sie für den Listener angeben, zu dem die Endpunktgruppe für den Endpunkt gehört.

Jede Endpunktgruppe kann über mehrere Endpunkte verfügen. Sie können jeden Endpunkt mehreren Endpunktgruppen hinzufügen, aber die Endpunktgruppen müssen verschiedenen Listener zugeordnet sein. Eine Ressource muss gültig und aktiv sein, wenn Sie sie als Endpunkt hinzufügen.

Global Accelerator überwacht kontinuierlich die Integrität aller Endpunkte, die in einer Standard-Endpunktgruppe enthalten sind. Der Datenverkehr wird nur an die aktiven Endpunkte weitergeleitet, die fehlerfrei sind. Wenn Global Accelerator über keine fehlerfreien Endpunkte verfügt, an die der Datenverkehr weitergeleitet werden kann, leitet er den Datenverkehr an alle Endpunkte weiter.

Beachten Sie Folgendes für bestimmte Typen von Global Accelerator-Standard-Endpunkten:

Load Balancer Endpunkte

- Ein Application Load Balancer -Endpunkt kann internetorientiert oder internetorientiert sein. Ein Network Load Balancer Endpunkt muss mit dem Internet verbunden sein.

Amazon EC2 Instance-Endpunkte

- Ein EC2-Instance-Endpunkt (sowohl für Standard- als auch für benutzerdefinierte Routing-Beschleuniger) kann nicht einer der folgenden Typen sein: C1, CC2, CC2, CC2, CC2, CC2, CC2, CC2, CC2, CC2, HI2, HI1, HS1, M2, M2, M2, M2, M3 oder T1.
- Nur in einigen AWS Regionen werden EC2-Instances als Endpunkte unterstützt. Eine Liste der unterstützten Regionen finden Sie unter Unterstützte AWS Regionen für die Erhaltung der Client-IP-Adresse.
- Es wird empfohlen, eine EC2-Instance aus Global Accelerator-Endpunktgruppen zu entfernen, bevor Sie die Instance beenden. Wenn Sie eine EC2-Instance beenden, bevor Sie sie aus einer Endpunktgruppe in Global Accelerator entfernen und dann eine weitere Instanz in derselben VPC mit derselben privaten IP-Adresse erstellen und Integritätsprüfungen bestehen, leitet Global Accelerator Datenverkehr an den neuen Endpunkt weiter.

Themen

- Hinzufügen, Bearbeiten oder Entfernen eines Standard-Endpunkts
- Endpoint Gewichtungen
- Hinzufügen von Endpunkten mit Client-IP-Adresserhaltung
- Übergänge von Endpunkten zur Verwendung der Client-IP-Adresserhaltung

Hinzufügen, Bearbeiten oder Entfernen eines Standard-Endpunkts

Sie fügen Endpunkte zu Endpunktgruppen hinzu, damit der Datenverkehr an Ihre Ressourcen weitergeleitet werden kann. Sie können einen Standard-Endpunkt bearbeiten, um die Gewichtung für den Endpunkt zu ändern. Oder Sie können einen Endpunkt aus dem Accelerator entfernen, indem Sie ihn aus einer Endpunktgruppe entfernen. Das Entfernen eines Endpunkts wirkt sich nicht auf den Endpunkt selbst aus, aber Global Accelerator kann den Datenverkehr nicht mehr auf diese Ressource leiten.

Endpunkte in Global Accelerator können Network Load Balancers, Application Load Balancers, Amazon EC2 Instances oder Elastic IP-Adressen sein. Sie müssen zuerst eine dieser Ressourcen erstellen und sie dann als Endpunkt in Global Accelerator hinzufügen. Eine Ressource muss gültig und aktiv sein, wenn Sie sie als Endpunkt hinzufügen.

Sie können Endpunkte basierend auf der Verwendung aus Endpunktgruppen hinzufügen oder entfernen. Wenn beispielsweise der Bedarf an Ihrer Anwendung zunimmt, können Sie mehr Ressourcen erstellen und anschließend einer oder mehreren Endpunktgruppen weitere Endpunkte hinzufügen, um den erhöhten Datenverkehr zu bewältigen. Global Accelerator beginnt, Anfragen an einen Endpunkt weiterzuleiten, sobald Sie ihn hinzugefügt haben und der Endpunkt die ersten Zustandsprüfungen bestanden hat. Sie können Datenverkehr zu Endpunkten verwalten, indem Sie die Gewichtungen auf einem Endpunkt anpassen, um proportional mehr oder weniger Datenverkehr an den Endpunkt zu senden.

Wenn Sie einen Endpunkt mit Client-IP-Adresserhaltung hinzufügen, überprüfen Sie zunächst die Informationen inUnterstützte AWS Regionen für die Erhaltung der Client-IP-AdresseundBeibehalten von Client-IP-Adressen in AWS Global Accelerator.

Sie können Endpunkte aus Ihren Endpunktgruppen entfernen, z. B. wenn Sie Ihre Endpunkte bedienen müssen. Wenn Sie einen Endpunkt entfernen, wird er aus der Endpunktgruppe entfernt. Andernfalls hat dies keine Auswirkungen auf den Endpunkt. Global Accelerator leitet den Datenverkehr nicht mehr an einen Endpunkt, sobald Sie ihn aus einer Endpunktgruppe entfernen. Der Endpunkt wechselt in einen Zustand, in dem er darauf wartet, dass alle aktuellen Anforderungen abgeschlossen sind, sodass keine Unterbrechung für den Clientdatenverkehr besteht, der gerade ausgeführt wird. Sie können den Endpunkt wieder zur Endpunktgruppe hinzufügen, wenn er bereit ist, wieder Anfragen zu erhalten.

In diesem Abschnitt wird beschrieben, wie Sie mit Endpunkten auf der AWS Global Accelerator Konsole arbeiten. Wenn Sie API-Vorgänge mit AWS Global Accelerator verwenden möchten, informieren Sie sich unter derAWS Global Accelerator -API.

So fügen Sie einen Standard-Endpunkt hinzu

1. Öffnen Sie die Global Accelerator-Konsole unterhttps://console.aws.amazon.com/globalaccelerator/home.
2. Klicken Sie auf der-Accelerators-Seiten einen Accelerator aus.
3. In derListenerAbschnitts erstellt, fürListener-IDdie ID eines Listener aus.
4. In derEndpoint GruppenAbschnitts erstellt, fürEndpoint Gruppen-IDWählen Sie die ID der Endpunktgruppe aus, der Sie einen Endpunkt hinzufügen möchten.
5. In der-Endpunkte-Abschnitts erstellt.Fügt einen Endpunkt hinzu.
6. Klicken Sie auf derHinzufügen von Endpunkten-Seiten eine Ressource aus der Dropdown-Liste aus.

Wenn Sie keine AWS Ressourcen besitzen, sind keine Elemente in der Liste enthalten. Um fortzufahren, erstellen Sie AWS Ressourcen wie Load Balancer, Amazon EC2 Instances oder Elastic IP-Adressen. Kehren Sie dann zu den hier beschriebenen Schritten zurück und wählen Sie eine Ressource aus der Liste aus.

7. Optional können Sie beiGewichteine Zahl zwischen 0 und 255 ein, um eine Gewichtung für das Routing von Datenverkehr an diesen Endpunkt festzulegen. Wenn Sie Endpunkten Gewichtungen hinzufügen, konfigurieren Sie Global Accelerator so, dass der Datenverkehr basierend auf den von Ihnen angegebenen Proportionen weitergeleitet wird. Standardmäßig haben alle Endpunkte eine Gewichtung von 128. Weitere Informationen finden Sie unter Endpoint Gewichtungen.
8. Aktivieren Sie optional die Beibehaltung der Client-IP-Adresse für einen Application Load Balancer -Endpunkt, der internetorientiert ist. UNDERBeibehalten von Client-IP-AdresseWählen Sie bei derBeibehalten von Adresse.

   Diese Option ist immer für interne Application Load Balancer er- und EC2-Instance-Endpunkte ausgewählt und nie für Network Load Balancer er- und Elastic IP-Adressenendpunkte ausgewählt. Weitere Informationen finden Sie unter Beibehalten von Client-IP-Adressen in AWS Global Accelerator.

   > **Note**
   >
   > Bevor Sie Datenverkehr an Endpunkte hinzufügen und weiterleiten, die die Client-IP-Adresse beibehalten, stellen Sie sicher, dass alle erforderlichen Sicherheitskonfigurationen, z. B. Sicherheitsgruppen, aktualisiert werden, um die IP-Adresse des Benutzerclients in Zulassungslisten aufzunehmen.

9. Wählen Sie Add endpoint (Endpunkt hinzufügen) aus.

So bearbeiten Sie einen Standard-Endpunkt

Sie können eine Endpunktkonfiguration bearbeiten, um die Gewichtung zu ändern. Weitere Informationen finden Sie unter Endpoint Gewichtungen.

1. Öffnen Sie die Global Accelerator-Konsole unterhttps://console.aws.amazon.com/globalaccelerator/home.
2. Klicken Sie auf der-Accelerators-Seiten einen Accelerator aus.

3. In derListenerAbschnitts erstellt, fürListener-IDdie ID eines Listener aus.
4. In derEndpoint GruppenAbschnitts erstellt, fürEndpoint Gruppen-IDdie ID der Endpunktgruppe aus.
5. Klicken Sie aufBearbeiten des Endpunkts.
6. Klicken Sie auf derBearbeiten des EndpunktsSeite erstellt, und wählen Sie dann die OptionSave.

So entfernen Sie einen Endpunkt:

1. Öffnen Sie die Global Accelerator-Konsole unterhttps://console.aws.amazon.com/globalaccelerator/home.
2. Klicken Sie auf der-Accelerators-Seiten einen Accelerator aus.
3. In derListenerAbschnitts erstellt, fürListener-IDdie ID eines Listener aus.
4. In derEndpoint GruppenAbschnitts erstellt, fürEndpoint Gruppen-IDdie ID der Endpunktgruppe aus.
5. Klicken Sie aufEntfernen von Endpunkt.
6. Wählen Sie im -BestätigungsdialogfeldRemove.

Endpoint Gewichtungen

Eine Gewichtung ist ein Wert, der den Anteil des Datenverkehrs bestimmt, den Global Accelerator an einen Endpunkt in einem Standardbeschleuniger leitet. Endpunkte können Network Load Balancers, Application Load Balancers, Amazon EC2 Instances oder Elastic IP-Adressen sein. Global Accelerator berechnet die Summe der Gewichtungen für die Endpunkte in einer Endpunktgruppe und leitet dann den Datenverkehr auf der Grundlage des Verhältnisses der Gewichtung jedes Endpunkts zur Summe an die Endpunkte weiter.

Mit dem gewichteten Routing können Sie festlegen, wie viel Datenverkehr an eine Ressource in einer Endpunktgruppe weitergeleitet wird. Dies kann auf verschiedene Arten nützlich sein, einschließlich Load Balancing und Testen neuer Versionen einer Anwendung.

Funktionsweise von Endpunktgewichtungen

Wenn Sie Gewichtungen verwenden möchten, ordnen Sie jedem Endpunkt in einer Endpunktgruppe eine relative Gewichtung zu, die dem Volumen an Datenverkehr entspricht, das Sie senden möchten. Standardmäßig beträgt die Gewichtung eines Endpunkts 128, d. h. die Hälfte des Maximalwerts für eine Gewichtung, 255. Global Accelerator sendet Datenverkehr auf Basis der Gewichtung, die Sie

einem Endpunkt zugeordnet haben, an einen Endpunkt. Diese Gewichtung stellt einen Anteil der Gesamtgewichtung für alle Endpunkte in der Gruppe dar:

$$\frac{\text{Weight for a specified endpoint}}{\text{Sum of the weights for all endpoints}}$$

Wenn Sie beispielsweise einen kleinen Teil Ihres Datenverkehrs an einen Endpunkt senden möchten und den Rest an einen anderen Endpunkt, können Sie Gewichtungen von 1 und 255 angeben. Der Endpunkt mit der Gewichtung 1 erhält 1/256 des Datenverkehrs (1/1+255) und der andere Endpunkt erhält 255/256 (255/1+255). Sie können dies Schrittweise durch Änderung der Gewichtungen ändern. Wenn Global Accelerator keinen Datenverkehr mehr an einen Endpunkt senden soll, können Sie die Gewichtung für diese Ressource auf 0 setzen.

Failover für fehlerhafte Endpunkte

Wenn in einer Endpunktgruppe keine fehlerfreien Endpunkte vorhanden sind, die eine Gewichtung größer als Null haben, versucht Global Accelerator, ein Failover auf einen fehlerfreien Endpunkt mit einer Gewichtung größer als Null in einer anderen Endpunktgruppe durchzuführen. Bei diesem Failover ignoriert Global Accelerator die Einstellung für den Datenverkehr. Wenn beispielsweise für eine Endpunktgruppe eine Verkehrswahl auf Null gesetzt ist, schließt Global Accelerator diese Endpunktgruppe in den Failoverversuch ein.

Wenn Global Accelerator nach drei zusätzlichen Endpunktgruppen (d. h. drei AWS Regionen) keinen fehlerfreien Endpunkt mit einer Gewichtung größer als Null findet, leitet er Datenverkehr an einen zufälligen Endpunkt in der Endpunktgruppe weiter, der dem Client am nächsten ist. Das heißt, esÖffnen schlägt fehl.

Beachten Sie Folgendes:

- Bei der für das Failover ausgewählten Endpunktgruppe kann es sich um eine Gruppe handeln, die auf Null gesetzt ist.
- Die nächste Endpunktgruppe ist möglicherweise nicht die ursprüngliche Endpunktgruppe. Dies liegt daran, dass Global Accelerator Wähleinstellungen für den Kontoverkehr berücksichtigt, wenn er die ursprüngliche Endpunktgruppe wählt.

Angenommen, Ihre Konfiguration hat zwei Endpunkte, einen fehlerfreien und einen fehlerhaften Endpunkt, und Sie haben die Gewichtung für jeden von ihnen auf größer als Null festgelegt. In diesem Fall leitet Global Accelerator Datenverkehr an den fehlerfreien Endpunkt weiter. Nun sagen Sie jedoch, dass Sie die Gewichtung des einzigen gesunden Endpunkts auf Null setzen. Global

Accelerator versucht dann drei zusätzliche Endpunktgruppen, um einen fehlerfreien Endpunkt mit einer Gewichtung größer als Null zu finden. Wenn er keinen findet, leitet Global Accelerator Datenverkehr an einen zufälligen Endpunkt in der Endpunktgruppe weiter, der dem Client am nächsten ist.

Hinzufügen von Endpunkten mit Client-IP-Adresserhaltung

Ein Feature, das Sie mit einigen Endpunkttypen (in einigen Regionen) verwenden können, istBeibehalten von Client-IP-Adresse. Mit dieser Funktion behalten Sie die Quell-IP-Adresse des ursprünglichen Clients für Pakete bei, die am Endpunkt ankommen. Sie können diese Funktion mit Application Load Balancer und Amazon EC2 Instance-Endpunkten verwenden. Endpunkte auf benutzerdefinierten Routingbeschleunigern haben immer die Client-IP-Adresse beibehalten. Weitere Informationen finden Sie unter Beibehalten von Client-IP-Adressen in AWS Global Accelerator.

Wenn Sie die Client-IP-Adresserhaltung verwenden möchten, sollten Sie beim Hinzufügen von Endpunkten zu Global Accelerator Folgendes beachten:

Elastic Network-Schnittstelle

Um die Erhaltung der Client-IP-Adressen zu unterstützen, erstellt Global Accelerator elastische Netzwerkschnittstellen in Ihrem AWS Konto — eine für jedes Subnetz, in dem ein Endpunkt vorhanden ist. Weitere Informationen darüber, wie Global Accelerator mit elastischen Netzwerkschnittstellen arbeitet, finden Sie unterBewährte Methoden für die Erhaltung von Client-IP-Adressen.

Endpunkte in privaten Subnetze

Sie können einen Application Load Balancer oder eine EC2-Instance in einem privaten Subnetz mit AWS Global Accelerator ausrichten, aber Sie müssen über eineInternet-Gateway, die an die VPC angeschlossen ist, die die Endpunkte enthält. Weitere Informationen finden Sie unter Sichere VPC Verbindungen in AWS Global Accelerator.

Die Client-IP-Adresse zur Zulassungsliste hinzufügen

Bevor Sie Datenverkehr an Endpunkte hinzufügen und weiterleiten, die die Client-IP-Adresse beibehalten, stellen Sie sicher, dass alle erforderlichen Sicherheitskonfigurationen, z. B. Sicherheitsgruppen, aktualisiert werden, um die IP-Adresse des Benutzerclients in die Zulassungsliste aufzunehmen. ACLs (Network Access Control Lists, ACLs) gelten nur für ausgehenden (ausgehenden) Datenverkehr. Wenn Sie den eingehenden (eingehenden) Datenverkehr filtern müssen, müssen Sie Sicherheitsgruppen verwenden.

Konfigurieren von Netzwerk-Zugriffskontrolllisten (ACLs)

Netzwerk-ACLs, die Ihren VPC -Subnetzen zugeordnet sind, gelten für ausgehenden (ausgehenden) Datenverkehr, wenn die Erhaltung der Client-IP-Adresse im Accelerator aktiviert ist. Damit der Datenverkehr jedoch über Global Accelerator beendet werden kann, müssen Sie die ACL sowohl als eingehende als auch ausgehende Regel konfigurieren.

Um beispielsweise TCP- und UDP-Clients, die einen flüchtigen Quellport verwenden, über Global Accelerator eine Verbindung zu Ihrem Endpunkt herzustellen, verknüpfen Sie das Subnetz Ihres Endpunkts mit einer Netzwerk-ACL, die ausgehenden Datenverkehr zulässt, der zu einem ephemeren TCP- oder UDP-Port bestimmt ist (Portbereich 1024-65535, Ziel 0.0.0/0). Erstellen Sie außerdem eine übereinstimmende eingehende Regel (Portbereich 1024-65535, Quelle 0.0.0/0).

> **Note**
>
> Sicherheitsgruppen und AWS WAF Regeln sind ein zusätzlicher Satz von Funktionen, die Sie zum Schutz Ihrer Ressourcen anwenden können. Mit den eingehenden Sicherheitsgruppenregeln, die Ihren Amazon EC2 Instances und Application Load Balancers zugeordnet sind, können Sie beispielsweise die Zielports steuern, mit denen Clients über Global Accelerator eine Verbindung herstellen können, z. B. Port 80 für HTTP oder Port 443 für HTTPS. Beachten Sie, dass Amazon EC2 Instance-Sicherheitsgruppen für jeden Datenverkehr gelten, der in Ihre Instances eintrifft, einschließlich Datenverkehr von Global Accelerator und jeder öffentlichen oder Elastic IP-Adresse, die Ihrer Instance zugewiesen ist. Verwenden Sie als bewährte Methode private Subnetze, wenn Sie sicherstellen möchten, dass Datenverkehr nur von Global Accelerator bereitgestellt wird. Stellen Sie außerdem sicher, dass die Regeln für eingehende Sicherheitsgruppen so konfiguriert sind, dass der Datenverkehr für Ihre Anwendungen ordnungsgemäß zugelassen oder verweigert wird.

Übergänge von Endpunkten zur Verwendung der Client-IP-Adresserhaltung

Folgen Sie den Anweisungen in diesem Abschnitt, um einen oder mehrere Endpunkte im Accelerator zu Endpunkten zu wechseln, die die Client-IP-Adresse des Benutzers beibehalten. Sie können optional einen Application Load Balancer -Endpunkt oder einen Elastic IP-Adressenendpunkt auf einen entsprechenden Endpunkt (einen Application Load Balancer oder eine EC2-Instanz) umstellen, der über die Erhaltung der Client-IP-Adressen verfügt. Weitere Informationen finden Sie unter Beibehalten von Client-IP-Adressen in AWS Global Accelerator.

Wir raten Ihnen zur Umstellung auf die Verwendung der Client-IP-Adresse langsam. Fügen Sie zunächst neue Application Load Balancer oder EC2-Instance-Endpunkte hinzu, die Sie aktivieren, um die Client-IP-Adresse beizubehalten. Verschieben Sie dann den Datenverkehr langsam von vorhandenen Endpunkten auf die neuen Endpunkte, indem Sie Gewichtungen auf den Endpunkten konfigurieren.

> **Important**
>
> Bevor Sie mit dem Weiterleiten von Datenverkehr an Endpunkte beginnen, die die Client-IP-Adresse beibehalten, müssen Sie sicherstellen, dass alle Konfigurationen, in denen Sie Global Accelerator-Client-IP-Adressen in Zulassungslisten aufgenommen haben, aktualisiert werden, um stattdessen die IP-Adresse des Benutzerclients einzuschließen.

Die Beibehaltung der Client-IP-Adresse ist nur in bestimmten AWS Regionen verfügbar. Weitere Informationen finden Sie unter Unterstützte AWS Regionen für die Erhaltung der Client-IP-Adresse.

In diesem Abschnitt wird beschrieben, wie Sie mit Endpunktgruppen in der AWS Global Accelerator Konsole arbeiten. Wenn Sie API-Operationen mit Global Accelerator verwenden möchten, finden Sie weitere Informationen unterAWS Global Accelerator -API.

Nachdem Sie eine kleine Menge an Datenverkehr auf den neuen Endpunkt mit der Erhaltung der Client-IP-Adresse verschoben haben, testen Sie, um sicherzustellen, dass Ihre Konfiguration wie erwartet funktioniert. Erhöhen Sie dann schrittweise den Anteil des Datenverkehrs zum neuen Endpunkt, indem Sie die Gewichtungen an den entsprechenden Endpunkten anpassen.

Um zu Endpunkten zu wechseln, die Client-IP-Adressen beibehalten, führen Sie zunächst die folgenden Schritte aus, um einen neuen Endpunkt hinzuzufügen, und aktivieren Sie für die mit dem Internet verbundenen Application Load Balancer -Endpunkte die Erhaltung der Client-IP-Adresse. (Die Option zur Erhaltung der Client-IP-Adresse ist immer für interne Application Load Balancers und EC2-Instanzen ausgewählt.)

So fügen Sie einen Endpunkt mit Client-IP-Adresserhaltung hinzu

1. Öffnen Sie die Global Accelerator-Konsole unterhttps://console.aws.amazon.com/globalaccelerator/home.
2. Klicken Sie auf der-Accelerators-Seiten einen Accelerator aus.
3. In derListener-Bereich einen Listener aus.
4. In derGruppe Endpoint-Abschnitt eine Endpunktgruppe aus.

5. In der-Endpunkte-Abschnitts erstellt.Fügt einen Endpunkt hinzu.
6. Klicken Sie auf derHinzufügen von Endpunkten-Seitens auf der-Endpunkteeinen Application Load Balancer-Endpunkt oder einen EC2-Instance-Endpunkt aus.
7. In derGewichteine geringe Zahl im Vergleich zu den Gewichtungen aus, die für Ihre vorhandenen Endpunkte festgelegt werden. Beispiel: Wenn die Gewichtung für einen entsprechenden Application Load Balancer 255 beträgt, können Sie für den neuen Application Load Balancer zunächst eine Gewichtung von 5 eingeben. Weitere Informationen finden Sie unter Endpoint Gewichtungen.
8. Für einen neuen, nach außen gerichteten Application Load Balancer -Endpunkt finden Sie unterBeibehalten von Client-IP-AdresseWählen Sie bei derBeibehalten von Adresse. (Diese Option ist immer für interne Application Load Balancers und EC2-Instanzen ausgewählt.)
9. Wählen Sie Save Changes.

Führen Sie als Nächstes die hier beschriebenen Schritte aus, um die entsprechenden vorhandenen Endpunkte (die Sie durch die neuen Endpunkte durch die Erhaltung der Client-IP-Adresse ersetzen) zu bearbeiten, um die Gewichtung für vorhandene Endpunkte zu reduzieren, sodass weniger Datenverkehr zu ihnen gelangt.

So reduzieren Sie den Datenverkehr für die vorhandenen Endpunkte

1. Klicken Sie auf derGruppe Endpointeinen vorhandenen Endpunkt aus, der keine Client-IP-Adresserhaltung aufweist.
2. Wählen Sie Edit (Bearbeiten) aus.
3. Klicken Sie auf derBearbeiten des Endpunkts-Seitens auf derGewichteine niedrigere Zahl als die aktuelle Zahl ein. Wenn die Gewichtung eines vorhandenen Endpunkts beispielsweise 255 beträgt, können Sie für den neuen Endpunkt eine Gewichtung von 220 eingeben (mit der Erhaltung der Client-IP-Adresse).
4. Wählen Sie Save Changes.

Nachdem Sie mit einem kleinen Teil des ursprünglichen Datenverkehrs getestet haben, indem Sie die Gewichtung für den neuen Endpunkt auf eine niedrige Zahl festgelegt haben, können Sie den gesamten Datenverkehr langsam übergehen, indem Sie weiterhin die Gewichtung für die ursprünglichen und die neuen Endpunkte anpassen.

Angenommen, Sie beginnen mit einem vorhandenen Application Load Balancer mit einer Gewichtung auf 200 und fügen einen neuen Application Load Balancer-Endpunkt hinzu, bei dem die Client-

IP-Adresserhaltung mit einer Gewichtung auf 5 aktiviert ist. Verschieben Sie den Datenverkehr schrittweise vom ursprünglichen Application Load Balancer auf den neuen Application Load Balancer, indem Sie die Gewichtung für den neuen Application Load Balancer erhöhen und die Gewichtung für den ursprünglichen Application Load Balancer verringern. Zum Beispiel:

- Originalgewicht 190/neues Gewicht 10
- Originalgewicht 180/neues Gewicht 20
- Originalgewicht 170/neues Gewicht 30, und so weiter.

Wenn Sie die Gewichtung für den ursprünglichen Endpunkt auf 0 verringert haben, wird der gesamte Datenverkehr (in diesem Beispielszenario) an den neuen Application Load Balancer -Endpunkt weitergeleitet, der die Erhaltung der Client-IP-Adresse umfasst.

Wenn Sie zusätzliche Endpunkte (Application Load Balancers oder EC2-Instanzen) haben, die Sie zur Verwendung der Client-IP-Adresserhaltung wechseln möchten, wiederholen Sie die Schritte in diesem Abschnitt, um sie zu überführen.

Wenn Sie die Konfiguration für einen Endpunkt zurücksetzen müssen, damit der Datenverkehr zum Endpunkt die Client-IP-Adresse nicht erhalten bleibt, können Sie dies jederzeit tun: Erhöhen Sie die Gewichtung für den Endpunkt, dernichtdie Erhaltung der Client-IP-Adresse auf den ursprünglichen Wert haben und die Gewichtung für den Endpunkt verringernmitClient-IP-Adresserhaltung auf 0.

Arbeiten mit benutzerdefinierten Routing-Beschleunigern in AWS Global Accelerator

Dieses Kapitel enthält Verfahren und Empfehlungen zum Erstellen benutzerdefinierter Routing-Beschleuniger in AWS Global Accelerator. Mit einem benutzerdefinierten Routing-Beschleuniger können Sie die Anwendungslogik verwenden, um einen oder mehrere Benutzer einer bestimmten Amazon EC2 Instance unter vielen Zielen direkt zuzuordnen und gleichzeitig die Performance-Verbesserungen beim Routing Ihres Datenverkehrs über Global Accelerator zu erzielen. Dies ist nützlich, wenn Sie eine Anwendung haben, bei der eine Gruppe von Benutzern auf derselben Sitzung interagieren muss, die auf einer bestimmten EC2-Instance und einem bestimmten Port ausgeführt wird, z. B. Spielanwendungen oder Voice over IP (VoIP) -Sitzungen.

Endpunkte für benutzerdefinierte Routingbeschleuniger müssen virtuelle Private Cloud-Subnetze (VPC -Subnetze) sein, und ein benutzerdefinierter Routingbeschleuniger kann Datenverkehr nur an Amazon EC2 Instances in diesen Subnetzen weiterleiten. Wenn Sie einen benutzerdefinierten Routing-Beschleuniger erstellen, können Sie Tausende von Amazon EC2 Instances einschließen, die in einem einzelnen oder mehreren VPC -Subnetzen ausgeführt werden. Weitere Informationen hierzu finden Sie unter Funktionsweise von benutzerdefinierten Routing-Beschleunigern in AWS Global Accelerator.

Wenn Global Accelerator stattdessen automatisch den für Ihre Clients nächstgelegenen fehlerfreien Endpunkt auswählen soll, erstellen Sie einen Standardbeschleuniger. Weitere Informationen finden Sie unter Arbeiten mit Standard-Beschleunigern in AWS Global Accelerator.

Um einen benutzerdefinierten Routing-Accelerator einzurichten, führen Sie Folgendes aus:

1. Überprüfen Sie die Richtlinien und Anforderungen zum Erstellen eines benutzerdefinierten Routing-Accelerators Siehe Richtlinien und Einschränkungen für benutzerdefinierte Routing-Beschleuniger.
2. Erstellen Sie ein VPC -Subnetz Sie können dem Subnetz jederzeit EC2-Instanzen hinzufügen, nachdem Sie das Subnetz zu Global Accelerator hinzugefügt haben.
3. Erstellen Sie einen Accelerator, und wählen Sie die Option für einen benutzerdefinierten Routing-Accelerator
4. Fügen Sie einen Listener hinzu, und geben Sie einen Bereich von Ports an, auf die Global Accelerator überwacht werden soll. Stellen Sie sicher, dass Sie einen großen Bereich mit genügend Ports einschließen, damit Global Accelerator allen Zielen zugeordnet werden kann, die

Sie erwarten. Diese Ports unterscheiden sich von Zielports, die Sie im nächsten Schritt angeben. Weitere Informationen zu den Anforderungen für Listener-Ports finden Sie unterRichtlinien und Einschränkungen für benutzerdefinierte Routing-Beschleuniger.

5. Fügen Sie eine oder mehrere Endpunktgruppen für AWS Regionen hinzu, in denen Sie VPC -Subnetze haben. Für jede Endpunktgruppe geben Sie Folgendes an:
   - Ein Endpunkt-Portbereich, der die Ports an Ihren EC2-Zielinstanzen darstellt, die Datenverkehr empfangen können.
   - Das Protokoll für jeden Zielportbereich: UDP, TCP oder sowohl UDP als auch TCP.
6. Wählen Sie für das Endpunkt-Subnetz eine Subnetz-ID aus. Sie können in jeder Endpunktgruppe mehrere Subnetze hinzufügen, und Subnetze können unterschiedliche Größen haben (bis zu /17).

In den folgenden Abschnitten wird die Arbeit mit benutzerdefinierten Routingbeschleunigern, Listener, Endpunktgruppen und Endpunkten erläutert.

Themen

- Funktionsweise von benutzerdefinierten Routing-Beschleunigern in AWS Global Accelerator
- Richtlinien und Einschränkungen für benutzerdefinierte Routing-Beschleuniger
- Benutzerdefinierte Routing-Beschleuniger in AWS Global Accelerator
- Listener für benutzerdefinierte Routing-Beschleuniger in AWS Global Accelerator
- Endpunktgruppen für benutzerdefinierte Routing-Beschleuniger in AWS Global Accelerator
- VPC -Subnetzendpunkte für benutzerdefinierte Routing-Beschleuniger in AWS Global Accelerator

Funktionsweise von benutzerdefinierten Routing-Beschleunigern in AWS Global Accelerator

Wenn Sie einen benutzerdefinierten Routing-Beschleuniger in AWS Global Accelerator verwenden, können Sie mithilfe der Anwendungslogik einen oder mehrere Benutzer einem bestimmten Ziel unter vielen Zielen direkt zuordnen und gleichzeitig die Leistungsvorteile von Global Accelerator nutzen. Ein benutzerdefinierter Routingbeschleuniger ordnet Listener-Portbereiche EC2-Instance-Zielen in VPC -Subnetzen (Virtual Private Cloud) zu. Dadurch kann Global Accelerator den Datenverkehr deterministisch an eine bestimmte private IP-Adresse und ein Port-Ziel von Amazon EC2 in Ihrem Subnetz weiterleiten.

Sie können beispielsweise einen benutzerdefinierten Routing-Beschleuniger mit einer Online-Echtzeit-Gaming-Anwendung verwenden, in der Sie einer einzigen Sitzung auf einem Amazon EC2 Spielserver mehrere Spieler basierend auf Faktoren zuweisen, die Sie auswählen, wie z. B. geografischer Standort, Spielerfähigkeiten und Spielmodus. Oder Sie haben eine VoIP - oder Social-Media-Anwendung, die mehrere Benutzer einem bestimmten Medienserver für Sprach-, Video- und Messaging-Sitzungen zuweist.

Ihre Anwendung kann eine Global Accelerator-API aufrufen und eine vollständige statische Zuordnung der Global Accelerator-Ports und der zugehörigen Ziel-IP-Adressen und -Ports erhalten. Sie können diese statische Zuordnung speichern und dann vom Matchmaking-Service zum Weiterleiten von Benutzern an bestimmte EC2-Zielinstanzen verwenden. Sie müssen keine Änderungen am Clientsoftware vornehmen, um Global Accelerator mit Ihrer Anwendung nutzen zu können.

Um einen benutzerdefinierten Routingbeschleuniger zu konfigurieren, wählen Sie einen VPC -Subnetzendpunkt aus. Anschließend definieren Sie einen Zielportbereich, dem eingehende Verbindungen zugeordnet werden, damit Ihre Software denselben Port über alle Instanzen hinweg abhören kann. Global Accelerator erstellt eine statische Zuordnung, die es Ihrem Matchmaking-Dienst ermöglicht, eine Ziel-IP-Adresse und Portnummer für eine Sitzung in eine externe IP-Adresse und einen externen Port zu übersetzen, die Sie Benutzern geben.

Der Netzwerk-Stack Ihrer Anwendung funktioniert möglicherweise über ein einziges Transportprotokoll, oder Sie verwenden UDP für die schnelle Bereitstellung und TCP für eine zuverlässige Bereitstellung. Sie können UDP, TCP oder sowohl UDP als auch TCP für jeden Zielportbereich festlegen, um Ihnen maximale Flexibilität zu bieten, ohne die Konfiguration für jedes Protokoll duplizieren zu müssen.

> **Note**
>
> Standardmäßig dürfen alle VPC -Subnetzziele in einem benutzerdefinierten Routingbeschleuniger keinen Datenverkehr empfangen. Dies soll standardmäßig sicher sein und Ihnen auch eine granulare Kontrolle darüber geben, welche privaten EC2-Instance-Destinationen in Ihrem Subnetz Datenverkehr empfangen dürfen. Sie können den Datenverkehr zum Subnetz oder zu bestimmten IP-Adress- und Portkombinationen (Ziel-Sockets) zulassen oder verweigern. Weitere Informationen finden Sie unter Hinzufügen, Bearbeiten oder Entfernen eines VPC -Subnetzendpunkts. Sie können Ziele auch mithilfe der Global Accelerator-API angeben. Weitere Informationen finden Sie unterAllowCustomRoutingTrafficundDenyCustomRoutingTraffic.

Beispiel für die Funktionsweise von benutzerdefiniertem Routing in Global Accelerator

Nehmen wir beispielsweise an, Sie möchten 10.000 Sitzungen unterstützen, bei denen Gruppen von Benutzern interagieren, z. B. Spielesitzungen oder VoIP Anrufsitzungen, über 1.000 Amazon EC2 Instances hinter Global Accelerator. In diesem Beispiel geben wir einen Listener-Portbereich von 10001—20040 und einen Zielportbereich von 81—90 an. Wir werden sagen, dass wir die vier VPC -Subnetze in us-east-1 haben: subnet-1, subnet-2, subnet-3 und subnet-4.

In unserer Beispielkonfiguration hat jedes VPC -Subnetz eine Blockgröße von /24, sodass 251 Amazon EC2 Instances unterstützt werden können. (Fünf Adressen sind reserviert und nicht in jedem Subnetz verfügbar, und diese Adressen werden nicht zugeordnet.) Jeder Server, der auf jeder EC2-Instance ausgeführt wird, bedient die folgenden 10 Ports, die wir für die Zielports in unserer Endpunktgruppe angegeben haben: 81-90. Dies bedeutet, dass wir 2510 Ports (10 x 251) mit jedem Subnetz verbunden sind. Jeder Port kann einer Sitzung zugeordnet werden.

Da wir 10 Zielports für jede EC2-Instance in unserem Subnetz angegeben haben, ordnet Global Accelerator diese intern 10 Listener-Ports zu, die Sie für den Zugriff auf EC2-Instances verwenden können. Um dies einfach zu veranschaulichen, sagen wir, dass es einen Block von Listener-Ports gibt, der mit der ersten IP-Adresse des Endpunktsubnetzes für den ersten Satz von 10 beginnt und dann zur nächsten IP-Adresse für den nächsten Satz von 10 Listener-Ports wechselt.

> **Note**
>
> Das Mapping ist eigentlich nicht so vorhersehbar, aber wir verwenden hier ein sequentielles Mapping, um zu zeigen, wie die Port-Mapping funktioniert. Verwenden Sie die folgenden API-Vorgänge, um die tatsächliche Zuordnung für die Listener-Portbereiche zu ermitteln: ListCustomRoutingPortMappingsundListCustomRoutingPortMappingsByDestination.

In unserem Beispiel ist der erste Listener-Port 10001. Dieser Port ist der ersten Subnetz-IP-Adresse 192.0.2.4 und dem ersten EC2-Port 81 zugeordnet. Der nächste Listener-Port 10002 ist mit der ersten Subnetz-IP-Adresse 192.0.2.4 und dem zweiten EC2-Port 82 verknüpft. In der folgenden Tabelle wird veranschaulicht, wie diese Beispielzuordnung durch die letzte IP-Adresse des ersten VPC -Subnetzes und dann die erste IP-Adresse des zweiten VPC-Subnetzes fortgesetzt wird.

Global Accelerator Listener-Port	VPC -Subnetze	EC2-Instance-Port
10001	192.0.2.4	81
10002	192.0.2.4	82
10003	192.0.2.4	83
10004	192.0.2.4	84
10005	192.0.2.4	85
10006	192.0.2.4	86
10007	192.0.2.4	87
10008	192.0.2.4	88
10009	192.0.2.4	89
10010	192.0.2.4	90
10011	192.0.2.5	81
10012	192.0.2.5	82
10013	192.0.2.5	83
10014	192.0.2.5	84
10015	192.0.2.5	85
10016	192.0.2.5	86
10017	192.0.2.5	87
10018	192.0.2.5	88
10019	192.0.2.5	89
10020	192.0.2.5	90

Global Accelerator Listener-Port	VPC -Subnetze	EC2-Instance-Port
...	...	...
12501	192.0.2.244	81
12502	192.0.2.244	82
12503	192.0.2.244	83
12504	192.0.2.244	84
12505	192.0.2.244	85
12506	192.0.2.244	86
12507	192.0.2.244	87
12508	192.0.2.244	88
12509	192.0.2.244	89
12510	192.0.2.244	90
12511	192.0.3.4	81
12512	192.0.3.4	82
12513	192.0.3.4	83
12514	192.0.3.4	84
12515	192.0.3.4	85
12516	192.0.3.4	86
12517	192.0.3.4	87
12518	192.0.3.4	88
12519	192.0.3.4	89

Global Accelerator Listener-Port	VPC -Subnetze	EC2-Instance-Port
12520	192.0.3.4	90

Richtlinien und Einschränkungen für benutzerdefinierte Routing-Beschleuniger

Beachten Sie beim Erstellen und Arbeiten mit benutzerdefinierten Routing-Beschleunigern in AWS Global Accelerator die folgenden Richtlinien und Einschränkungen.

Amazon EC2 Instance-Ziele

VPC -Subnetzendpunkte in einem benutzerdefinierten Routing-Accelerator können nur EC2-Instances enthalten. Für benutzerdefinierte Routing-Beschleuniger werden keine anderen Ressourcen wie Load Balancer unterstützt.

Die Typen von EC2-Instances, die mit Global Accelerator unterstützt werden, sind inEndpunkte für Standardbeschleuniger in AWS Global Accelerator.

Port-Zuordnungen

Wenn Sie ein VPC -Subnetz hinzufügen, erstellt Global Accelerator eine statische Portzuordnung von Listener-Portbereichen zu den vom Subnetz unterstützten Portbereichen. Die Portzuordnung für ein bestimmtes Subnetz ändert sich nie.

Sie können die Portzuordnungsliste eines benutzerdefinierten Routing-Accelerators programmgesteuert anzeigen. Weitere Informationen finden Sie unter `ListCustomRoutingPortMappings`.

VPC -Subnetzgröße

VPC -Subnetze, die Sie einem benutzerdefinierten Routingbeschleuniger hinzufügen, müssen mindestens /28 und maximal /17 sein.

Listener-Port-Bereiche

Sie müssen genügend Listener-Ports angeben, indem Sie Listener-Portbereiche angeben, um die Anzahl der Ziele in den Subnetzen aufzunehmen, die Sie dem benutzerdefinierten Routing-Beschleuniger hinzufügen möchten. Der Bereich, den Sie beim Erstellen eines Listener angeben, bestimmt, wie viele Listener-Port- und Ziel-IP-Adresskombinationen Sie mit Ihrem

benutzerdefinierten Routingbeschleuniger verwenden können. Für maximale Flexibilität und um die Möglichkeit zu verringern, einen Fehler zu erhalten, dass nicht genügend Listener-Ports verfügbar sind, empfehlen wir, einen großen Portbereich anzugeben.

Global Accelerator weist Portbereiche in Blöcken zu, wenn Sie einem benutzerdefinierten Routingbeschleuniger ein Subnetz hinzufügen. Es wird empfohlen, Listener-Portbereiche linear zuzuweisen und die Bereiche groß genug zu machen, um die Anzahl der Zielports zu unterstützen, die Sie haben möchten. Das heißt, die Anzahl der Ports, die Sie zuweisen sollten, sollte mindestens die Subnetzgröße mal der Anzahl der Zielports und Protokolle (Zielkonfigurationen) sein, die Sie im Subnetz haben.

> **Note**
>
> Für den Algorithmus, den Global Accelerator zum Zuweisen von Portzuordnungen verwendet, müssen Sie möglicherweise weitere Listener-Ports hinzufügen, die über diese Summe hinausgehen.

Nachdem Sie einen Listener erstellt haben, können Sie ihn bearbeiten, um zusätzliche Portbereiche und zugeordnete Protokolle hinzuzufügen. Vorhandene Portbereiche können jedoch nicht verringert werden. Wenn Sie beispielsweise einen Listener-Portbereich von 5.000—10.000 haben, können Sie den Portbereich nicht auf 5900—10.000 ändern, und Sie können den Portbereich nicht auf 5.000—9.900 ändern.

Jeder Listener-Portbereich muss mindestens 16 Ports enthalten. Listeners unterstützen die Ports 1-65535.

Ziel-Port

Es gibt zwei Stellen, an denen Sie Portbereiche für einen benutzerdefinierten Routingbeschleuniger angeben: die Portbereiche, die Sie beim Hinzufügen eines Listener angeben, sowie die Zielportbereiche und -protokolle, die Sie für eine Endpunktgruppe angeben.

- Listener-Port-Bereiche: Die Listener-Ports auf den statischen IP-Adressen von Global Accelerator, mit denen Ihre Clients eine Verbindung herstellen. Global Accelerator ordnet jeden Port einer eindeutigen Ziel-IP-Adresse und einem eindeutigen Port in einem VPC -Subnetz hinter dem Accelerator zu.
- Ziel-Port: Die Gruppen von Zielportbereichen, die Sie für eine Endpunktgruppe angeben (auch als Zielkonfigurationen bezeichnet), sind die EC2-Instance-Ports, die Datenverkehr empfangen.

Um Datenverkehr auf Zielports zu empfangen, müssen die Sicherheitsgruppen, die Ihren EC2-Instances zugeordnet sind, Datenverkehr auf diesen Ports zulassen.

Health sprüfungen und Failover

Global Accelerator führt keine Integritätsprüfungen für benutzerdefinierte Routingbeschleuniger durch und führt kein Failover auf fehlerfreie Endpunkte durch. Der Datenverkehr für benutzerdefinierte Routingbeschleuniger wird unabhängig von der Integrität einer Zielressource deterministisch geroutet.

Der gesamte Datenverkehr wird standardmäßig verweigert

Standardmäßig wird der Datenverkehr, der über einen benutzerdefinierten Routingbeschleuniger geleitet wird, an alle Ziele in Ihrem Subnetz verweigert. Damit Zielinstanzen Datenverkehr empfangen können, müssen Sie den gesamten Datenverkehr zum Subnetz zulassen oder alternativ den Datenverkehr zu bestimmten Instanz-IP-Adressen und -Ports im Subnetz zulassen.

Das Aktualisieren eines Subnetzes oder eines bestimmten Ziels, um Datenverkehr zuzulassen oder zu verweigern, dauert Zeit, bis es über das Internet verbreitet wird. Um festzustellen, ob eine Änderung weitergegeben wurde, können Sie die`DescribeCustomRoutingAccelerator`API-Aktion, um den Accelerator-Status zu überprüfen. Weitere Informationen finden Sie unterDescribeCustomRoutingAccelerator.

AWS CloudFormation wird nicht unterstützt

AWS CloudFormation wird für benutzerdefinierte Routing-Beschleuniger nicht unterstützt.

Benutzerdefinierte Routing-Beschleuniger in AWS Global Accelerator

Abenutzerdefinierter Routing-Acceleratorin AWS Global Accelerator können Sie benutzerdefinierte Anwendungslogik verwenden, um einen oder mehrere Benutzer zu einem bestimmten Ziel unter vielen Zielen zu leiten. Gleichzeitig können Sie das globale AWS Netzwerk nutzen, um die Verfügbarkeit und Leistung Ihrer Anwendung zu verbessern.

Ein benutzerdefinierter Routingbeschleuniger leitet Datenverkehr nur an Ports auf Amazon EC2 Instances weiter, die in VPC -Subnetzen (Virtual Private Cloud) ausgeführt werden. Bei einem benutzerdefinierten Routingbeschleuniger leitet Global Accelerator den Datenverkehr nicht basierend auf der Geoproximation oder dem Zustand des Endpunkts weiter. Weitere Informationen hierzu

finden Sie unter Funktionsweise von benutzerdefinierten Routing-Beschleunigern in AWS Global Accelerator.

Wenn Sie einen Accelerator erstellen, stellt Ihnen Global Accelerator standardmäßig zwei statische IP-Adressen zur Verfügung. Wenn Sie AWS (BYOIP) einen eigenen IP-Adressbereich hinzufügen, können Sie stattdessen statische IP-Adressen aus Ihrem eigenen Pool zuweisen, um sie mit Ihrem Accelerator zu verwenden. Weitere Informationen finden Sie unter Bring Your Own IP Addresses (BYOIP) in AWS Global Accelerator.

> **Important**
>
> Die IP-Adressen werden Ihrem Accelerator so lange zugewiesen, wie er existiert, auch wenn Sie den Accelerator deaktivieren und der Datenverkehr nicht mehr akzeptiert oder weiterleitet. Allerdings, wenn Siedeleteeinen Beschleuniger verwenden, verlieren Sie die statischen IP-Adressen von Global Accelerator, die dem Beschleuniger zugewiesen sind, sodass Sie den Datenverkehr nicht mehr mithilfe dieser Adressen weiterleiten können. Stellen Sie als bewährte Methode sicher, dass Sie über Berechtigungen verfügen, um ein versehentliches Löschen von Beschleunigern zu vermeiden. Sie können IAM-Richtlinien wie tag-basierte Berechtigungen mit Global Accelerator verwenden, um die Benutzer einzuschränken, die über Berechtigungen zum Löschen eines Accelerators verfügen. Weitere Informationen finden Sie unter Tagbasierte Richtlinien.

In diesem Abschnitt wird erläutert, wie Sie einen benutzerdefinierten Routingbeschleuniger in der Global Accelerator-Konsole erstellen, bearbeiten oder löschen. Weitere Informationen zur Verwendung von API-Vorgängen mit Global Accelerator finden Sie imAWS Global Accelerator.

Themen

- Erstellen oder Aktualisieren eines benutzerdefinierten Routing-Accelerators
- Anzeigen Ihrer benutzerdefinierten Routing-Beschleuniger
- Löschen eines benutzerdefinierten Routing-Beschleunigers

Erstellen oder Aktualisieren eines benutzerdefinierten Routing-Accelerators

So erstellen Sie einen benutzerdefinierten Routing-Accelerator

1. Öffnen Sie die Global Accelerator-Konsole unterhttps://console.aws.amazon.com/globalaccelerator/home.
2. Klicken Sie aufAccelerator erstellen.
3. Geben Sie einen Namen für Ihren Accelerator ein.
4. FürAccelerator-TypWählen Sie im MenüBenutzerdefinierte Weiterleitung.
5. Wenn Sie Ihren eigenen IP-Adressbereich in AWS (BYOIP) bereitgestellt haben, können Sie optional statische IP-Adressen für Ihren Accelerator aus diesem Adresspool angeben. Treffen Sie diese Wahl für jede der beiden statischen IP-Adressen für Ihren Beschleuniger.
   - Wählen Sie für jede statische IP-Adresse den IP-Adresspool aus, der verwendet werden soll.
   - Wenn Sie Ihren eigenen IP-Adresspool ausgewählt haben, wählen Sie auch eine spezifische IP-Adresse aus dem Pool. Wenn Sie den Standard-IP-Adresspool von Amazon gewählt haben, weist Global Accelerator Ihrem Beschleuniger eine bestimmte IP-Adresse zu.
6. Optional können Sie ein oder mehrere Tags hinzufügen, um Sie bei der Identifizierung Ihrer Accelerator-Ressourcen zu unterstützen.
7. Klicken Sie aufWeiter, um zu den nächsten Seiten des Assistenten zu gehen, um Listener, Endpunktgruppen und VPC -Subnetzendpunkte hinzuzufügen.

So bearbeiten Sie einen benutzerdefinierten Routing-Accelerator

1. Öffnen Sie die Global Accelerator-Konsole unterhttps://console.aws.amazon.com/globalaccelerator/home.
2. Wählen Sie in der Liste der benutzerdefinierten Routing-Acceleratoren ein Routing-Accelerator und klicken Sie aufBearbeiten.
3. Klicken Sie auf derAccelerator bearbeitenNehmen Sie alle gewünschten Änderungen vor. Beispielsweise können Sie den Beschleuniger deaktivieren, damit Sie ihn löschen können.
4. Wählen Sie Save (Speichern) aus.

Anzeigen Ihrer benutzerdefinierten Routing-Beschleuniger

Sie können auf der -Konsole Informationen zu Ihren benutzerdefinierten Routing-Acceleratoren anzeigen. Informationen zu den programmgesteuerten Beschreibungen der benutzerdefinierten Routingbeschleuniger finden Sie unterListCustomRoutingAcceleratorundDescribeCustomRoutingAccelerator-AAWS Global Accelerator -API-Referenz.

So zeigen Sie Informationen an, die Ihre benutzerdefinierten Routingbeschleuniger

1. Öffnen Sie die Global Accelerator-Konsole unterhttps://console.aws.amazon.com/globalaccelerator/home.
2. Um Details zu einem Accelerator anzuzeigen, wählen Sie ein Accelerator und klicken Sie aufAnzeigen.

Löschen eines benutzerdefinierten Routing-Beschleunigers

Wenn Sie einen benutzerdefinierten Routing-Beschleuniger als Test erstellt haben oder wenn Sie keinen Beschleuniger mehr verwenden, können Sie ihn löschen. Deaktivieren Sie auf der Konsole den Beschleuniger, und Sie können ihn dann löschen. Sie müssen keine Listener und Endpunktgruppen aus dem Accelerator entfernen.

Um einen benutzerdefinierten Routingbeschleuniger mithilfe eines API-Vorgangs anstelle der Konsole zu löschen, müssen Sie zuerst alle Listener und Endpunktgruppen entfernen, die dem Accelerator zugeordnet sind, und dann deaktivieren. Weitere Informationen finden Sie im .DeleteAccelerator-Operation imAWS Global Accelerator.

So deaktivieren Sie einen benutzerdefinierten Routing-Accelerator

1. Öffnen Sie die Global Accelerator-Konsole unterhttps://console.aws.amazon.com/globalaccelerator/home.
2. Wählen Sie in der Liste ein Accelerator aus, das Sie deaktivieren möchten.
3. Wählen Sie Edit (Bearbeiten) aus.
4. Klicken Sie aufDeaktivieren AcceleratorKlicken Sie auf und danach aufSave.

So löschen Sie ein benutzerdefiniertes Routing-Accelerator

1. Öffnen Sie die Global Accelerator-Konsole unterhttps://console.aws.amazon.com/globalaccelerator/home.
2. Wählen Sie in der Liste ein Accelerator aus, das Sie löschen möchten.
3. Wählen Sie Delete.

> **Note**
>
> Wenn Sie den Accelerator nicht deaktiviert haben,Löschennicht verfügbar. Weitere Informationen zum Deaktivieren des Accelerators finden Sie im vorherigen Verfahren.

4. Wählen Sie im Bestätigungsdialogfeld die Option Delete (Löschen).

> **Important**
>
> Wenn Sie einen Accelerator löschen, verlieren Sie die statischen IP-Adressen, die dem Beschleuniger zugewiesen sind, sodass Sie den Datenverkehr nicht mehr mithilfe dieser Adressen weiterleiten können.

Listener für benutzerdefinierte Routing-Beschleuniger in AWS Global Accelerator

Für einen benutzerdefinierten Routingbeschleuniger in AWS Global Accelerator konfigurieren Sie einen Listener, der einen Bereich von Listener-Ports mit zugehörigen Protokollen angibt, die Global Accelerator bestimmten Amazon EC2 Zielinstanzen in Ihren VPC -Subnetzendpunkten zuordnet. Wenn Sie einen VPC -Subnetzendpunkt hinzufügen, erstellt Global Accelerator eine statische Portzuordnung zwischen den Portbereichen, die Sie für den Listener definieren, und den Ziel-IP-Adressen und -Ports im Subnetz. Anschließend können Sie die Port-Zuordnung verwenden, um Ihre statischen IP-Adressen des Beschleunigers zusammen mit einem Listener-Port und Protokoll anzugeben, um den Benutzerverkehr an bestimmte Amazon EC2 Ziel-IP-Adressen und -Ports in Ihrem VPC -Subnetz zu leiten.

Sie definieren einen Listener, wenn Sie Ihren benutzerdefinierten Routing-Accelerator erstellen, und Sie können jederzeit weitere Listener hinzufügen. Jeder Listener kann eine oder mehrere Endpunktgruppen haben, eine für jede AWS Region, in der Sie VPC -Subnetzendpunkte haben.

Ein Listener in einem benutzerdefinierten Routingbeschleuniger unterstützt sowohl TCP- als auch UDP-Protokolle. Sie geben das Protokoll oder die Protokolle für jeden Zielportbereich an, den Sie definieren: UDP, TCP oder sowohl UDP als auch TCP.

Weitere Informationen finden Sie unter Funktionsweise von benutzerdefinierten Routing-Beschleunigern in AWS Global Accelerator.

Hinzufügen, Bearbeiten oder Entfernen eines benutzerdefinierten Routinglisteners

In diesem Abschnitt wird erläutert, wie Sie mit benutzerdefinierten Routing-Listener auf der AWS Global Accelerator Konsole arbeiten. Weitere Informationen zur Verwendung von API-Vorgängen mit AWS Global Accelerator finden Sie imAWS Global Accelerator -API.

Hinzufügen eines Listeners für einen benutzerdefinierten Routing-Accelerator

Der Bereich, den Sie beim Erstellen eines Listener angeben, legt fest, wie viele Listener-Port- und Ziel-IP-Adresskombinationen Sie mit Ihrem benutzerdefinierten Routingbeschleuniger verwenden können. Für maximale Flexibilität wird empfohlen, dass Sie einen großen Portbereich angeben. Jeder von Ihnen angegebene Listener-Portbereich muss mindestens 16 Ports enthalten.

> **Note**
>
> Nachdem Sie einen Listener erstellt haben, können Sie ihn bearbeiten, um zusätzliche Portbereiche und zugeordnete Protokolle hinzuzufügen. Vorhandene Portbereiche können jedoch nicht verringert werden.

1. Öffnen Sie die Global Accelerator-Konsole unterhttps://console.aws.amazon.com/globalaccelerator/home.
2. Klicken Sie auf derAcceleratorsWählen Sie einen benutzerdefinierten Routing-Accelerator aus.
3. Wählen Sie Add listener (Listener hinzufügen) aus.
4. Klicken Sie auf derHinzufügen des ListenersGeben Sie den Listener-Portbereich ein, den Sie mit dem Accelerator verknüpfen möchten.

   Listener unterstützen die Ports 1-65535. Für maximale Flexibilität mit einem benutzerdefinierten Routing-Beschleuniger empfehlen wir, einen großen Portbereich anzugeben.
5. Wählen Sie Add listener (Listener hinzufügen) aus.

So bearbeiten Sie einen Listener für einen benutzerdefinierten Routing-Accelerator

Wenn Sie einen Listener für einen benutzerdefinierten Routingbeschleuniger bearbeiten, beachten Sie, dass Sie zusätzliche Portbereiche und zugeordnete Protokolle hinzufügen, vorhandene Portbereiche vergrößern oder Protokolle ändern können. Sie können jedoch keine vorhandenen Portbereiche verringern.

1. Öffnen Sie die Global Accelerator-Konsole unterhttps://console.aws.amazon.com/globalaccelerator/home.
2. Klicken Sie auf derAcceleratorsWählen Sie einen Accelerator aus.
3. Wählen Sie einen Listener aus und wählen Sie dannListener bearbeiten.
4. Klicken Sie auf derListener bearbeitendie gewünschten Änderungen an vorhandenen Portbereichen oder Protokollen oder fügen Sie neue Portbereiche hinzu.

   Beachten Sie, dass Sie den Bereich eines vorhandenen Portbereichs nicht verringern können.
5. Wählen Sie Save (Speichern) aus.

So entfernen Sie einen Listener

1. Öffnen Sie die Global Accelerator-Konsole unterhttps://console.aws.amazon.com/globalaccelerator/home.
2. Klicken Sie auf derAcceleratorsWählen Sie einen Accelerator aus.
3. Wählen Sie einen Listener aus und wählen Sie dannRemove.
4. Klicken Sie im Bestätigungsdialogfeld aufRemove.

Endpunktgruppen für benutzerdefinierte Routing-Beschleuniger in AWS Global Accelerator

Mit einem benutzerdefinierten Routing Accelerator in AWS Global Accelerator definiert eine Endpunktgruppe die Ports und Protokolle, für die Amazon EC2 Instances in Ihren VPC -Subnetzen (Virtual Private Cloud) Datenverkehr akzeptieren.

Sie erstellen eine Endpunktgruppe für Ihren benutzerdefinierten Routing-Beschleuniger für jede AWS Region, in der sich Ihre VPC -Subnetze und EC2-Instances befinden. Jede Endpunktgruppe in einem benutzerdefinierten Routingbeschleuniger kann über mehrere VPC -Subnetzendpunkte verfügen.

Ebenso können Sie jede VPC mehreren Endpunktgruppen hinzufügen, aber die Endpunktgruppen müssen verschiedenen Listener zugeordnet sein.

Für jede Endpunktgruppe geben Sie einen Satz von einem oder mehreren Portbereichen an, die die Ports enthalten, an die Sie den Datenverkehr auf den EC2-Instances in der Region leiten möchten. Für jeden Portbereich der Endpunktgruppe geben Sie das zu verwendende Protokoll an: UDP, TCP oder sowohl UDP als auch TCP. Dies bietet maximale Flexibilität für Sie, ohne für jedes Protokoll Gruppen von Portbereichen duplizieren zu müssen. Sie haben beispielsweise einen Spieleserver mit Gaming-Traffic, der über UDP auf Ports 808080-8090 läuft, während Sie auch einen Server haben, der auf Chatnachrichten über TCP auf Port 80 wartet.

Weitere Informationen hierzu finden Sie unter Funktionsweise von benutzerdefinierten Routing-Beschleunigern in AWS Global Accelerator.

Hinzufügen, Bearbeiten oder Entfernen einer Endpunktgruppe für einen benutzerdefinierten Routing-Accelerator

Sie arbeiten mit einer Endpunktgruppe für Ihren benutzerdefinierten Routingbeschleuniger in der AWS Global Accelerator Konsole oder mithilfe eines API-Vorgangs. Sie können jederzeit VPC - Subnetzendpunkte zu einer Endpunktgruppe hinzufügen oder aus dieser entfernen.

In diesem Abschnitt wird erläutert, wie Sie mit Endpunktgruppen für Ihren benutzerdefinierten Routing-Beschleuniger in der AWS Global Accelerator Konsole arbeiten. Weitere Informationen zur Verwendung von API-Vorgängen mit Global Accelerator finden Sie imAWS Global Accelerator -API.

So fügen Sie eine Endpunktgruppe für einen benutzerdefinierten Routing-Accelerator hinzu

1. Öffnen Sie die Global Accelerator-Konsole unterhttps://console.aws.amazon.com/globalaccelerator/home.
2. Klicken Sie auf derAcceleratorsWählen Sie einen benutzerdefinierten Routing-Accelerator aus.
3. In derListenerAbschnitts erstellt, fürListener-IDWählen Sie die ID des Listener aus, dem Sie eine Endpunktgruppe hinzufügen möchten.
4. Klicken Sie aufHinzufügen von Endpunktgruppen.
5. Geben Sie im Abschnitt für einen Listener eine Region für die Endpunktgruppe an.
6. FürSets von Ports und ProtokollenPortbereiche und Protokolle für Ihre Amazon EC2 Instances ein.

   - den Wert einVom Hafenund einZum Portdie Option zum Angeben eines Bereichs an Ports.

- Geben Sie für jeden Portbereich das Protokoll bzw. die Protokolle für diesen Bereich an.

  Der Portbereich muss keine Teilmenge des Listener-Portbereichs sein, aber es muss genügend Gesamtanschlüsse im Listener-Portbereich vorhanden sein, um die Gesamtanzahl der Ports zu unterstützen, die Sie für die Endpunktgruppen in Ihrem benutzerdefinierten Routingbeschleuniger angeben.

7. Wählen Sie Save (Speichern) aus.
8. Wählen Sie alternativ die OptionHinzufügen von EndpunktgruppenHinzufügen zusätzlicher Endpunktgruppen für diesen Listener Sie können auch einen anderen Listener auswählen und Endpunktgruppen hinzufügen.
9. Klicken Sie aufHinzufügen von Endpunktgruppen.

So bearbeiten Sie eine Endpunktgruppe für einen benutzerdefinierten Routing-Accelerator

1. Öffnen Sie die Global Accelerator-Konsole unterhttps://console.aws.amazon.com/globalaccelerator/home.
2. Klicken Sie auf derAcceleratorsWählen Sie einen benutzerdefinierten Routing-Accelerator aus.
3. In derListenerAbschnitts erstellt, fürListener-IDWählen Sie die ID des Listener aus, dem die Endpunktgruppe zugeordnet ist.
4. Klicken Sie aufBearbeiten von Endpunktgruppen.
5. Klicken Sie auf derBearbeiten von Endpunktgruppendie Region, den Bereich der Ports oder das Protokoll für einen Bereich von Ports.
6. Wählen Sie Save (Speichern) aus.

So entfernen Sie einen benutzerdefinierten Routing-Accelerator

1. Öffnen Sie die Global Accelerator-Konsole unterhttps://console.aws.amazon.com/globalaccelerator/home.
2. Klicken Sie auf derAcceleratorsWählen Sie einen Accelerator aus.
3. In derListenerWählen Sie einen Listener aus und wählen Sie dannRemove.
4. In derEndpunktgruppenWählen Sie eine Endpunktgruppe aus, und wählen Sie dannRemove.
5. Wählen Sie im -BestätigungsdialogfeldRemove.

VPC -Subnetzendpunkte für benutzerdefinierte Routing-Beschleuniger in AWS Global Accelerator

Endpunkte für benutzerdefinierte Routingbeschleuniger sind virtuelle Private Cloud-Subnetze (VPC -Subnetze), die Datenverkehr über einen Beschleuniger empfangen können. Jedes Subnetz kann ein oder mehrere Amazon EC2 Instance-Ziele enthalten. Wenn Sie einen Subnetzendpunkt hinzufügen, generiert Global Accelerator eine neue Portzuordnung. Anschließend können Sie die Global Accelerator-API verwenden, um eine statische Liste aller Portzuordnungen für das Subnetz abzurufen, mit der Sie Datenverkehr an die IP-Adressen der Ziel-EC2-Instanz im Subnetz weiterleiten können. Weitere Informationen finden Sie unterListCustomRoutingPortMappings.

Sie können Datenverkehr nur auf EC2-Instances in den Subnetzen leiten, nicht auf andere Ressourcen wie Load Balancer (im Gegensatz zu Standardbeschleuniger). Die unterstützten EC2-Instanztypen sind inEndpunkte für Standardbeschleuniger in AWS Global Accelerator.

Weitere Informationen hierzu finden Sie unter Funktionsweise von benutzerdefinierten Routing-Beschleunigern in AWS Global Accelerator.

Beachten Sie Folgendes, wenn Sie VPC -Subnetze für Ihren benutzerdefinierten Routingbeschleuniger hinzufügen:

- Standardmäßig kann Datenverkehr, der über einen benutzerdefinierten Routingbeschleuniger geleitet wird, an keinem Ziel in Ihrem Subnetz ankommen. Damit Zielinstanzen Datenverkehr empfangen können, müssen Sie den gesamten Datenverkehr zum Subnetz zulassen oder alternativ den Datenverkehr zu bestimmten Instanz-IP-Adressen und -Ports (Ziel-Sockets) im Subnetz aktivieren.

  > **Important**
  >
  > Das Aktualisieren eines Subnetzes oder eines bestimmten Ziels, um Datenverkehr zuzulassen oder zu verweigern, dauert Zeit, bis es über das Internet verbreitet wird. Um zu ermitteln, ob eine Änderung weitergegeben wurde, können Sie die`DescribeCustomRoutingAccelerator`API-Aktion, um den Accelerator-Status zu überprüfen. Weitere Informationen finden Sie unterDescribeCustomRoutingAccelerator.

- Da VPC -Subnetze die Client-IP-Adresse beibehalten, sollten Sie die relevanten Sicherheits- und Konfigurationsinformationen überprüfen, wenn Sie Subnetze als Endpunkte für benutzerdefinierte

Routingbeschleuniger hinzufügen. Weitere Informationen finden Sie unter Hinzufügen von Endpunkten mit Client-IP-Adresserhaltung.

Hinzufügen, Bearbeiten oder Entfernen eines VPC -Subnetzendpunkts

Sie fügen virtuelle Private Cloud-Subnetzendpunkte (VPC) zu Endpunktgruppen in Ihren benutzerdefinierten Routingbeschleunigern hinzu, sodass Sie den Benutzerverkehr an Amazon EC2 Zielinstanzen im Subnetz weiterleiten können.

Wenn Sie EC2-Instances aus dem Subnetz hinzufügen und entfernen oder Datenverkehr zu EC2-Zielen aktivieren oder deaktivieren, ändern Sie, ob diese Ziele Datenverkehr empfangen können. Die Port-Zuordnung von Global Accelerator ändert sich jedoch nicht.

Um Datenverkehr zu einigen Zielen im Subnetz, aber nicht zu allen, zuzulassen, geben Sie IP-Adressen für jede EC2-Instance ein, die Sie zulassen möchten, zusammen mit den Ports auf der Instance, die Sie Datenverkehr empfangen möchten. Die IP-Adressen, die Sie angeben, müssen für EC2-Instances im Subnetz sein. Sie können einen Port oder einen Bereich von Ports angeben, die für das Subnetz zugeordnet sind.

Sie können das VPC -Subnetz aus dem Accelerator entfernen, indem Sie es aus einer Endpunktgruppe entfernen. Das Entfernen eines Subnetzes wirkt sich nicht auf das Subnetz selbst aus, aber Global Accelerator kann den Datenverkehr nicht mehr an das Subnetz oder an die darin Amazon EC2 Instances leiten. Darüber hinaus wird Global Accelerator die Portzuordnung für das VPC -Subnetz zurückfordern, um sie potenziell für neue Subnetze zu verwenden, die Sie hinzufügen.

In den Schritten in diesem Abschnitt wird erläutert, wie Sie VPC -Subnetzendpunkte in der AWS Global Accelerator Konsole hinzufügen, bearbeiten oder entfernen. Weitere Informationen zur Verwendung von API-Vorgängen mit AWS Global Accelerator finden Sie imAWS Global Accelerator - API.

So fügen Sie einen VPC -Subnetzendpunkt hinzu

1. Öffnen Sie die Global Accelerator-Konsole unterhttps://console.aws.amazon.com/globalaccelerator/home.
2. Klicken Sie auf derAcceleratorsWählen Sie einen benutzerdefinierten Routing-Accelerator aus.
3. In derListenerAbschnitts erstellt, fürListener-IDdie ID eines Listener aus.
4. In derEndpunktgruppenAbschnitts erstellt, fürGruppen-IDdie ID der Endpunktgruppe (AWS Region) aus, der Sie den VPC -Subnetzendpunkt hinzufügen möchten.

5. In der-EndpunkteAbschnitts erstellt.Hinzufügen von Endpoint.
6. Klicken Sie auf derHinzufügen von EndpunktenSeite, für-Endpunktein VPC -Subnetz aus.

   Wenn Sie keine VPCs haben, sind keine Elemente in der Liste aufgeführt. Um fortzufahren, fügen Sie mindestens eine VPC hinzu, kehren Sie dann zu den hier beschriebenen Schritten zurück, und wählen Sie eine VPC aus der Liste aus.
7. Für den hinzugefügten VPC -Subnetzendpunkt können Sie festlegen, dass Datenverkehr zu allen Zielen im Subnetz zugelassen oder verweigert werden soll, oder Sie können Datenverkehr nur für bestimmte EC2-Instanzen und Ports zulassen. Standardmäßig wird der Datenverkehr zu allen Zielen im Subnetz verweigert.
8. Wählen Sie Add endpoint (Endpunkt hinzufügen) aus.

So erlauben oder verweigern Sie Datenverkehr zu bestimmten Zielen

Sie können die VPC -Subnetz-Port-Zuordnung für einen Endpunkt bearbeiten, um Datenverkehr zu bestimmten EC2-Instanzen und Ports (Ziel-Sockets) in einem Subnetz zuzulassen oder zu verweigern.

1. Öffnen Sie die Global Accelerator-Konsole unterhttps://console.aws.amazon.com/globalaccelerator/home.
2. Klicken Sie auf derAcceleratorsWählen Sie einen benutzerdefinierten Routing-Accelerator aus.
3. In derListenerAbschnitts erstellt, fürListener-IDdie ID eines Listener aus.
4. In derEndpunktgruppenAbschnitts erstellt, fürGruppen-IDdie ID der Endpunktgruppe (AWS Region) des VPC -Subnetzendpunkts aus, den Sie bearbeiten möchten.
5. Wählen Sie Choose an endpoint subnet aus und wählen Sie dannView details (Details anzeigen).
6. Klicken Sie auf der-EndpunktSeite, unterPort-ZuweisungenWählen Sie eine IP-Adresse aus und klicken Sie dann aufBearbeiten.
7. Geben Sie die Ports ein, für die Sie den Datenverkehr aktivieren möchten, und wählen Sie dann die OptionDiese Ziele zulassen.

So lassen oder verweigern Sie ALLEN Datenverkehr zu einem Subnetz

Sie können einen Endpunkt aktualisieren, um Datenverkehr zu allen Zielen im VPC -Subnetz zuzulassen oder zu verweigern.

1. Öffnen Sie die Global Accelerator-Konsole unterhttps://console.aws.amazon.com/globalaccelerator/home.
2. Klicken Sie auf derAcceleratorsWählen Sie einen benutzerdefinierten Routing-Accelerator aus.
3. In derListenerAbschnitts erstellt, fürListener-IDdie ID eines Listener aus.
4. In derEndpunktgruppenAbschnitts erstellt, fürGruppen-IDdie ID der Endpunktgruppe (AWS Region) des VPC -Subnetzendpunkts aus, den Sie aktualisieren möchten.
5. Klicken Sie aufAllen Datenverkehr zulassen/verweigern.
6. Wählen Sie eine Option, um den gesamten Datenverkehr zuzulassen oder den gesamten Datenverkehr zu verweigern, und wählen SieSave.

So entfernen Sie einen Endpunkt:

1. Öffnen Sie die Global Accelerator-Konsole unterhttps://console.aws.amazon.com/globalaccelerator/home.
2. Klicken Sie auf derAcceleratorsWählen Sie einen benutzerdefinierten Routing-Accelerator aus.
3. In derListenerAbschnitts erstellt, fürListener-IDdie ID eines Listener aus.
4. In derEndpunktgruppenAbschnitts erstellt, fürGruppen-IDdie ID der Endpunktgruppe (AWS Region) des VPC -Subnetzendpunkts aus, den Sie entfernen möchten.
5. Klicken Sie aufEndpoint entfernen.
6. Wählen Sie im BestätigungsdialogfeldRemove.

DNS-Adressierung und benutzerdefinierte Domänen in AWS Global Accelerator

In diesem Kapitel wird erläutert, wie AWS Global Accelerator DNS-Routing durchführt und Informationen zur Verwendung einer benutzerdefinierten Domäne mit Global Accelerator enthält.

Themen

- Support für DNS-Adressierung in Global Accelerator
- Weiterleiten von benutzerdefinierten Domain-Traffic an Ihren Accelerator
- Bring Your Own IP Addresses (BYOIP) in AWS Global Accelerator

Support für DNS-Adressierung in Global Accelerator

Wenn Sie ein benutzerdefiniertes Routing oder einen Standardbeschleuniger erstellen, stellt Global Accelerator zwei statische IP-Adressen für Sie bereit. Er weist Ihrem Accelerator außerdem einen standardmäßigen DNS-Namen (Domain Name System) zu, ähnlich wie`a1234567890abcdef.awsglobalaccelerator.com`, die auf die statischen IP-Adressen verweist. Die statischen IP-Adressen werden global mit Anycast vom AWS Edge-Netzwerk zu Ihren Endpunkten beworben. Sie können die statischen IP-Adressen oder den DNS-Namen Ihres Beschleunigers verwenden, um Datenverkehr an Ihren Beschleuniger weiterzuleiten. DNS-Server und DNS-Resolver verwenden ein Roundrobin, um den DNS-Namen für einen Accelerator aufzulösen. Daher wird der Name in die statischen IP-Adressen des Accelerators aufgelöst, die von Amazon Route 53 in zufälliger Reihenfolge zurückgegeben werden. Clients verwenden in der Regel die erste IP-Adresse, die zurückgegeben wird.

> **Note**
>
> Global Accelerator erstellt zwei Pointer (PTR) -Datensätze, die die statischen IP-Adressen eines Beschleunigers dem entsprechenden von Global Accelerator generierten DNS-Namen zuordnen, um die umgekehrte DNS-Suche zu unterstützen. Dies wird auch als umgekehrte gehostete Zone bezeichnet. Beachten Sie, dass der DNS-Name, den Global Accelerator für Sie generiert, nicht konfigurierbar ist und Sie keine PTR-Einträge erstellen können, die auf Ihren benutzerdefinierten Domänennamen verweisen. Global Accelerator erstellt auch

keine PTR-Einträge für statische IP-Adressen aus einem IP-Adressbereich, den Sie in AWS (BYOIP) bereitstellen.

Weiterleiten von benutzerdefinierten Domain-Traffic an Ihren Accelerator

In den meisten Szenarien können Sie DNS so konfigurieren, dass Ihr benutzerdefinierter Domänenname verwendet wird (z. B.`www.example.com`) mit Ihrem Accelerator verwenden, anstatt die zugewiesenen statischen IP-Adressen oder den standardmäßigen DNS-Namen zu verwenden. Erstellen Sie zunächst mithilfe von Amazon Route 53 oder einem anderen DNS-Anbieter einen Domänennamen, und fügen Sie dann DNS-Einträge mit Ihren Global Accelerator IP-Adressen hinzu oder aktualisieren Sie diese. Oder Sie können Ihren benutzerdefinierten Domänennamen dem DNS-Namen für Ihren Accelerator zuordnen. Schließen Sie die DNS-Konfiguration ab, und warten Sie, bis die Änderungen über das Internet übertragen werden. Wenn ein Client eine Anforderung mit Ihrem benutzerdefinierten Domänennamen sendet, löst der DNS-Server diesen Namen in die IP-Adressen (in zufälliger Reihenfolge) oder in den DNS-Namen für Ihren Accelerator auf.

Um Ihren benutzerdefinierten Domänennamen mit Global Accelerator zu verwenden, wenn Sie Route 53 als DNS-Dienst verwenden, erstellen Sie einen Aliaseintrag, der Ihren benutzerdefinierten Domänennamen auf den DNS-Namen verweist, der Ihrem Beschleuniger zugewiesen ist. Ein Alias-Datensatz ist eine Route 53-Erweiterung von DNS. Er funktioniert ähnlich wie ein CNAME-Datensatz, jedoch können Sie einen Alias-Datensatz sowohl für die Stammdomäne (z. B.`example.com`und für Subdomains, wie`www.example.com`. Weitere Informationen finden Sie unterWählen zwischen Alias- und Nicht-Alias-DatensätzenEr finden Sie im Amazon Route 53-Entwicklerhandbuch.

Um Route 53 mit einem Aliasdatensatz für einen Beschleuniger einzurichten, befolgen Sie die Anleitung im folgenden Thema: Alias-ZielEr finden Sie im Amazon Route 53-Entwicklerhandbuch. Um die Informationen für Global Accelerator anzuzeigen, scrollen Sie auf derAlias-Zielangezeigten.

Bring Your Own IP Addresses (BYOIP) in AWS Global Accelerator

AWS Global Accelerator verwendet statische IP-Adressen als Einstiegspunkte für Ihre Beschleuniger. Diese IP-Adressen sind Anycast von AWS Edge-Standorten. Standardmäßig stellt Global Accelerator statische IP-Adressen aus demAmazon-IP-Adresspool. Anstatt die von Global Accelerator bereitgestellten IP-Adressen zu verwenden, können Sie diese Einstiegspunkte als IPv4-Adressen aus

Ihren eigenen Adressbereichen konfigurieren. In diesem Thema wird erläutert, wie Sie Ihre eigenen IP-Adressbereiche mit Global Accelerator verwenden.

Sie können einen Teil oder alle öffentlichen IPv4-Adressbereiche von Ihrem lokalen Netzwerk zu Ihrem AWS Konto zur Verwendung mit Global Accelerator bringen. Die Adressbereiche gehören weiterhin Ihnen, werden jedoch von AWS im Internet veröffentlicht.

Sie können die IP-Adressen, die Sie AWS für einen AWS-Service mitteilen, nicht mit einem anderen Service verwenden. In den Schritten in diesem Kapitel wird beschrieben, wie Sie Ihren eigenen IP-Adressbereich nur in AWS Global Accelerator verwenden. Schritte zum Verwenden Ihres eigenen IP-Adressbereichs für die Verwendung in Amazon EC2 finden Sie unterBring Your Own IP Addresses (BYOIP)im Amazon EC2 Benutzerhandbuch.

> **Important**
>
> Bevor Sie ihn über AWS veröffentlichen, müssen Sie den IP-Adressbereich nicht mehr anderweitig veröffentlichen. Wenn ein IP-Adressbereich mehrfach vernetzt ist (d. h., der Bereich wird von mehreren Dienstleistern gleichzeitig beworben), können wir nicht garantieren, dass der Datenverkehr zum Adressbereich in unser Netzwerk eintritt oder dass Ihr BYOIP-Werbeworkflow erfolgreich abgeschlossen wird.

Nachdem Sie einen Adressbereich zu AWS gebracht haben, erscheint er in Ihrem Konto als Adresspool. Wenn Sie einen Accelerator erstellen, können Sie ihm eine IP-Adresse aus Ihrem Bereich zuweisen. Global Accelerator weist Ihnen eine zweite statische IP-Adresse aus einem Amazon-IP-Adressbereich zu. Wenn Sie zwei IP-Adressbereiche zu AWS bringen, können Sie Ihrem Beschleuniger eine IP-Adresse aus jedem Bereich zuweisen. Diese Einschränkung liegt daran, dass Global Accelerator für hohe Verfügbarkeit jeden Adressbereich einer anderen Netzwerkzone zuweist.

Um Ihren eigenen IP-Adressbereich mit Global Accelerator zu verwenden, überprüfen Sie die Anforderungen, und führen Sie dann die Schritte in diesem Thema aus.

Themen

- Requirements
- Bereiten Sie sich darauf vor, Ihren IP-Adressbereich in Ihr AWS Konto einzubinden: Autorisierung
- Bereitstellen des Adressbereichs für die Verwendung mit AWS Global Accelerator
- Veröffentlichen des Adressbereichs über AWS
- Aufheben der Bereitstellung des Adressbereichs

- Erstellen Sie einen Beschleuniger mit Ihren IP-Adressen

Requirements

Sie können bis zu zwei qualifizierte IP-Adressbereiche für AWS Global Accelerator pro AWS-Konto bereitstellen.

Um sich zu qualifizieren, muss Ihr IP-Adressbereich die folgenden Voraussetzungen erfüllen:

- Der IP-Adressbereich muss bei einem der folgenden regionalen Internet Registry (RIRs) registriert sein: American Registry for Internet Numbers (ARIN), Réseaux IP Européens Network Coordination Centre (RIPE) oder Asia-Pacific Network Information Centre (APNIC). Der Adressbereich muss für ein Unternehmen oder eine juristische Person registriert sein. Es kann nicht für eine Einzelperson registriert werden.
- Der spezifischste Adressbereich, den Sie aufnehmen können, ist /24. Die ersten 24 Bits der IP-Adresse geben die Netzwerknummer an. Beispielsweise ist 198.51.100 die Netzwerknummer für die IP-Adresse 198.51.100.0.
- Die IP-Adressen im Adressbereich müssen über einen sauberen Verlauf verfügen. Das heißt, sie können keinen schlechten Ruf haben oder mit böswilligem Verhalten in Verbindung gebracht werden. Wir behalten uns das Recht vor, den IP-Adressbereich abzulehnen, wenn wir die Reputation des IP-Adressbereichs untersuchen und feststellen, dass er eine IP-Adresse enthält, die keine saubere Historie hat.

Außerdem benötigen wir die folgenden Zuweisungs- und Zuweisungsnetztypen oder -status, je nachdem, wo Sie Ihren IP-Adressbereich registriert haben:

- ARINE:`Direct Allocation`und`Direct Assignment`Netzwerk-Typen
- REIF:`ALLOCATED PA`,`LEGACY`, und`ASSIGNED PI`Zuteilungsstatus
- APNIC:`ALLOCATED PORTABLE`und`ASSIGNED PORTABLE`Zuteilungsstatus

Bereiten Sie sich darauf vor, Ihren IP-Adressbereich in Ihr AWS Konto einzubinden: Autorisierung

Um sicherzustellen, dass nur Sie Ihren IP-Adressraum zu Amazon bringen können, benötigen wir zwei Berechtigungen:

- Sie müssen Amazon autorisieren, den IP-Adressbereich anzukündigen.
- Sie müssen nachweisen, dass Sie Eigentümer des IP-Adressbereichs sind und daher die Befugnis haben, ihn an AWS zu übermitteln.

> **Note**
>
> Wenn Sie BYOIP verwenden, um AWS einen IP-Adressbereich zu übertragen, können Sie den Besitz dieses Adressbereichs nicht auf ein anderes Konto oder Unternehmen übertragen, während wir ihn bewerben. Sie können einen IP-Adressbereich auch nicht direkt von einem AWS Konto auf ein anderes Konto übertragen. Um das Eigentum zu übertragen oder zwischen AWS Konten zu übertragen, müssen Sie die Bereitstellung des Adressbereichs aufheben. Anschließend muss der neue Besitzer die Schritte ausführen, um den Adressbereich seinem AWS-Konto hinzuzufügen.

Um Amazon zu autorisieren, den IP-Adressbereich anzukündigen, senden Sie Amazon eine signierte Autorisierungsnachricht. Verwenden Sie eine ROA (Route Origin Authorization), um diese Berechtigung bereitzustellen. Eine ROA ist eine kryptografische Angabe über Ihre Routenankündigungen, die Sie über Ihre regionale Internet Registry (RIR) erstellen. Eine ROA enthält den IP-Adressbereich, die Autonomous System Numbers (ASNs), die den IP-Adressbereich veröffentlichen dürfen, sowie das Ablaufdatum. Der ROA autorisiert Amazon, einen IP-Adressbereich unter einem bestimmten Autonomous System (AS) zu veröffentlichen.

Ein ROA autorisiert Ihr AWS Konto nicht, den IP-Adressbereich in AWS einzubinden. Um diese Autorisierung bereitzustellen, müssen Sie ein selbstsigniertes X.509-Zertifikat in den Registry Data Access Protocol (RDAP) -Bemerkungen für den IP-Adressbereich veröffentlichen. Das Zertifikat enthält einen öffentlichen Schlüssel, den AWS zur Verifizierung der von Ihnen angegebene Autorisierungssignatur verwendet. Bewahren Sie den privaten Schlüssel sicher auf und verwenden Sie ihn, um die Autorisierungsnachricht zu signieren.

In den folgenden Abschnitten finden Sie detaillierte Schritte zum Ausführen dieser Autorisierungsaufgaben. Die Befehle in diesen Schritten werden von Linux unterstützt. Wenn Sie Windows verwenden, können Sie auf dieWindows-Subsystem für Linux, um Linux-Befehle auszuführen.

Schritte zur Bereitstellung der Autorisierung

- Schritt 1: Erstellen eines ROA-Objekts

- Schritt 2: Erstellen eines selbstsignierten X.509-Zertifikats
- Schritt 3: Erstellen einer signierten Autorisierungsnachricht

Schritt 1: Erstellen eines ROA-Objekts

Erstellen Sie ein ROA-Objekt, um Amazon ASN 16509 zu autorisieren, Ihren IP-Adressbereich sowie die ASNs zu veröffentlichen, die derzeit autorisiert sind, den IP-Adressbereich zu veröffentlichen. Der ROA muss die IP-Adresse enthalten, die Sie in AWS einbinden möchten. Sie müssen die maximale Länge auf /24 festlegen.

Weitere Informationen zum Erstellen einer ROA-Anforderung finden Sie in den folgenden Abschnitten, je nachdem, wo Sie Ihren IP-Adressbereich registriert haben:

- ARINE: ROA-Anforderungen
- REIF: Verwalten von RoAS
- APNIC: Routenmanagement

Schritt 2: Erstellen eines selbstsignierten X.509-Zertifikats

Erstellen Sie ein key pair und ein selbstsigniertes X.509-Zertifikat, und fügen Sie das Zertifikat dann zu dem RDAP-Datensatz für Ihre RIR hinzu. In den folgenden Schritten wird beschrieben, wie Sie diese Aufgaben ausführen.

> **Note**
>
> Die`openssl`Für die -Befehle in diesen Schritten ist OpenSSL Version 1.0.2 oder höher erforderlich.

So erstellen Sie ein X.509-Zertifikat und fügen es hinzu

1. Erzeugen Sie ein 2048-Bit-RSAkey pair mit dem folgenden Befehl.

   ```
   openssl genrsa -out private.key 2048
   ```

2. Erstellen Sie mit dem folgenden Befehl ein öffentliches X.509-Zertifikat aus dem key pair.

   ```
   openssl req -new -x509 -key private.key -days 365 | tr -d "\n" > publickey.cer
   ```

In diesem Beispiel läuft das Zertifikat nach 365 Tagen ab und ist dann nicht mehr vertrauenswürdig. Stellen Sie beim Ausführen des -Befehls sicher, dass Sie den`-days`auf den gewünschten Wert für den korrekten Ablauf. Wenn Sie dazu aufgefordert werden, andere Informationen einzugeben, können Sie die Standardwerte übernehmen.

3. Aktualisieren Sie den RDAP-Datensatz für Ihre RIR mit dem X.509-Zertifikat, indem Sie die folgenden Schritte ausführen (abhängig von Ihrer RIR).

   1. Zeigen Sie Ihr Zertifikat mit dem folgenden Befehl an.

      ```
      cat publickey.cer
      ```

   2. Fügen Sie das Zertifikat wie folgt hinzu:

      > **Important**
      >
      > Stellen Sie sicher, dass Sie den`-----BEGIN CERTIFICATE-----`und`-----END CERTIFICATE-----`aus dem Zertifikat.

      - Fügen Sie für ARIN das Zertifikat im`Public Comments`für Ihren IP-Adressbereich.
      - Fügen Sie für RIPE das Zertifikat als neue`descr`für den IP-Adressbereich.
      - Senden Sie für APNIC den öffentlichen Schlüssel in einer E-Mail an`helpdesk@apnic.net`Um den von APNIC autorisierten Kontakt für die IP-Adressen zu veröffentlichen, bitten Sie, ihn manuell zur`remarks`-Feld.

Schritt 3: Erstellen einer signierten Autorisierungsnachricht

Erstellen Sie die signierte Autorisierungsnachricht, damit Amazon Ihren IP-Adressbereich ankündigen kann.

Das Format der Nachricht ist wie folgt, wobei der`YYYYMMDD`Datum ist das Ablaufdatum der Nachricht.

```
1|aws|aws-account|address-range|YYYYMMDD|SHA256|RSAPSS
```

So erstellen Sie die signierte Autorisierungsnachricht

1. Erstellen Sie eine Klartext-Autorisierungsnachricht und speichern Sie sie in einer Variablen mit dem Namen`text_message`, wie das folgende Beispiel zeigt. Ersetzen Sie die vorgegebene Kontonummer, den IP-Adressbereich und das Ablaufdatum durch Ihre eigenen Werte.

```
text_message="1|aws|123456789012|203.0.113.0/24|20191201|SHA256|RSAPSS"
```

2. Signieren Sie die Autorisierungsnachricht in`text_message`Verwenden Sie das key pair, das Sie im vorherigen Abschnitt erstellt haben.
3. Speichern Sie die Nachricht in einer Variablen mit dem Namen`signed_message`, wie das folgende Beispiel zeigt.

```
signed_message=$(echo $text_message | tr -d "\n" | openssl dgst -sha256 -sigopt
      rsa_padding_mode:pss -sigopt rsa_pss_saltlen:-1 -sign private.key -keyform
 PEM | openssl base64 |
      tr -- '+=/' '-_~' | tr -d "\n")
```

Bereitstellen des Adressbereichs für die Verwendung mit AWS Global Accelerator

Wenn Sie einen Adressbereich für die Verwendung mit AWS bereitstellen, bestätigen Sie, dass Sie den Adressbereich besitzen und autorisieren Amazon, ihn zu veröffentlichen. Wir überprüfen, ob der Adressbereich Ihnen gehört.

Sie müssen Ihren Adressbereich mithilfe der CLI- oder Global Accelerator-API-Vorgänge bereitstellen. Diese Funktionalität ist nicht in der AWS Konsole verfügbar.

Um den Adressbereich bereitzustellen, verwenden Sie den folgendenProvisionByoipCidr-Befehl. Die`--cidr-authorization-context`Der Parameter verwendet die Variablen, die Sie im vorherigen Abschnitt erstellt haben und nicht die ROA-Nachricht.

```
aws globalaccelerator provision-byoip-cidr --cidr address-range --cidr-authorization-
context Message="$text_message",Signature="$signed_message"
```

Im Folgenden finden Sie ein Beispiel für die Bereitstellung eines Adressbereichs.

```
aws globalaccelerator provision-byoip-cidr
```

```
    --cidr 203.0.113.25/24
    --cidr-authorization-context Message="$text_message",Signature="$signed_message"
```

Die Bereitstellung eines Adressbereichs ist eine asynchrone Operation. Daher gibt der Aufruf sofort Daten zurück. Der Adressbereich kann jedoch erst verwendet werden, wenn sich der Status von`PENDING_PROVISIONING`auf`READY`. Es kann bis zu 3 Wochen dauern, bis der Bereitstellungsprozess abgeschlossen ist. Um den Status der von Ihnen bereitgestellten Adressbereiche zu überwachen, verwenden Sie die folgendenListbyoIPCIDRs-Befehl:

```
aws globalaccelerator list-byoip-cidrs
```

Eine Liste der Zustände für einen IP-Adressbereich finden Sie unterByoIPCIDR.

Wenn Ihr IP-Adressbereich bereitgestellt wird, wird die`State`den von zurückgegebenen`list-byoip-cidrs`ist`READY`. Zum Beispiel:

```
{
    "ByoipCidrs": [
        {
            "Cidr": "203.0.113.0/24",
            "State": "READY"
        }
    ]
}
```

Veröffentlichen des Adressbereichs über AWS

Nachdem der Adressbereich bereitgestellt wurde, kann er veröffentlicht werden. Sie müssen den genauen Adressbereich ankündigen, den Sie bereitgestellt haben. Sie können nur einen Teil des bereitgestellten Adressbereichs ankündigen. Darüber hinaus müssen Sie die Veröffentlichung Ihres IP-Adressbereichs nicht mehr anderweitig veröffentlichen, bevor Sie ihn über AWS veröffentlichen.

Sie müssen Ihren Adressbereich mithilfe der CLI- oder Global Accelerator-API-Vorgänge bewerben (oder die Werbung beenden). Diese Funktionalität ist nicht in der AWS Konsole verfügbar.

> **Important**
>
> Stellen Sie sicher, dass Ihr IP-Adressbereich von AWS angekündigt wird, bevor Sie eine IP-Adresse aus Ihrem Pool mit Global Accelerator verwenden.

Um den Adressbereich zu veröffentlichen, verwenden Sie den folgendenWerbenYOIPCIDR-Befehl.

```
aws globalaccelerator advertise-byoip-cidr --cidr address-range
```

Im Folgenden finden Sie ein Beispiel für die Anforderung von Global Accelerator, einen Adressbereich anzukündigen.

```
aws globalaccelerator advertise-byoip-cidr --cidr 203.0.113.0/24
```

Um den Status der von Ihnen angekündigten Adressbereiche zu überwachen, verwenden Sie die folgendenListbyoIPCIDRs-Befehl.

```
aws globalaccelerator list-byoip-cidrs
```

Wenn Ihr IP-Adressbereich angekündigt wird, wird die`State`den von zurückgegebenen`list-byoip-cidrs`ist`ADVERTISING`. Zum Beispiel:

```
{
    "ByoipCidrs": [
        {
            "Cidr": "203.0.113.0/24",
            "State": "ADVERTISING"
        }
    ]
}
```

Um die Veröffentlichung für den Adressbereich einzustellen, verwenden Sie den folgenden`withdraw-byoip-cidr`-Befehl.

> **Important**
>
> Um die Werbung für Ihren Adressbereich zu beenden, müssen Sie zunächst alle Beschleuniger entfernen, die über statische IP-Adressen verfügen, die aus dem Adresspool zugewiesen werden. Informationen zum Löschen eines Accelerators über die Konsole oder mithilfe von API-Vorgängen finden Sie unterLöscht eines Accelerators.

```
aws globalaccelerator withdraw-byoip-cidr --cidr address-range
```

Im Folgenden finden Sie ein Beispiel für die Anforderung von Global Accelerator, einen Adressbereich zurückzuziehen.

```
aws globalaccelerator withdraw-byoip-cidr
    --cidr 203.0.113.25/24
```

Aufheben der Bereitstellung des Adressbereichs

Um die Verwendung Ihres Adressbereichs mit AWS einzustellen, müssen Sie zunächst alle Beschleuniger entfernen, die über statische IP-Adressen verfügen, die aus dem Adresspool zugewiesen sind, und stoppen die Veröffentlichung Ihres Adressbereichs. Nachdem Sie diese Schritte ausgeführt haben, können Sie die Bereitstellung des Adressbereichs aufheben.

Sie müssen die Werbung beenden und die Bereitstellung Ihres Adressbereichs mithilfe der CLI- oder Global Accelerator-API-Vorgänge aufheben. Diese Funktionalität ist nicht in der AWS Konsole verfügbar.

Schritt 1: Löschen Sie alle zugeordneten Beschleuniger.Informationen zum Löschen eines Accelerators über die Konsole oder mithilfe von API-Vorgängen finden Sie unterLöscht eines Accelerators.

Schritt 2. Aufheben der Veröffentlichung für den Adressbereich. Um die Veröffentlichung für den Bereich einzustellen, verwenden Sie den folgendenAuszahlungYIPCIDR-Befehl.

```
aws globalaccelerator withdraw-byoip-cidr --cidr address-range
```

Schritt 3. Aufheben der Bereitstellung des Adressbereichs. Um die Bereitstellung des Bereichs aufzuheben, verwenden Sie die folgendenDeProvisionbyIPCIDR-Befehl.

```
aws globalaccelerator deprovision-byoip-cidr --cidr address-range
```

Erstellen Sie einen Beschleuniger mit Ihren IP-Adressen

Jetzt können Sie einen Beschleuniger mit Ihren IP-Adressen erstellen. Wenn Sie einen Adressbereich zu AWS gebracht haben, können Sie Ihrem Beschleuniger eine IP-Adresse zuweisen. Wenn Sie

zwei Adressbereiche mitgebracht haben, können Sie Ihrem Accelerator eine IP-Adresse aus jedem Adressbereich zuweisen.

Sie haben mehrere Möglichkeiten, einen Accelerator mit eigenen IP-Adressen für die statischen IP-Adressen zu erstellen:

- Verwenden Sie die Global Accelerator-Konsole, um einen Beschleuniger zu erstellen. Weitere Informationen finden Sie unter Erstellen oder Aktualisieren eines Standard-Beschleunigers und Erstellen oder Aktualisieren eines benutzerdefinierten Routing-Accelerators.
- Verwenden Sie die Global Accelerator-API, um einen Accelerator zu erstellen. Weitere Informationen einschließlich Beispielen für die Verwendung der CLI finden Sie unterCreateAcceleratorundCreateCustomRoutingAcceleratorIn der AWS Global Accelerator -API-Referenz.

Beibehalten von Client-IP-Adressen in AWS Global Accelerator

Ihre Optionen für die Beibehaltung und den Zugriff auf die Client-IP-Adresse für AWS Global Accelerator hängen von den Endpunkten ab, die Sie mit Ihrem Accelerator eingerichtet haben. Es gibt zwei Arten von Endpunkten, die die Quell-IP-Adresse des Clients in eingehenden Paketen beibehalten können: Application Load Balancers und Amazon EC2 Instances

- Wenn Sie einen mit dem Internet verbundenen Application Load Balancer als Endpunkt mit Global Accelerator verwenden, ist die Client-IP-Adresserhaltung für neue Beschleuniger standardmäßig aktiviert. Dies bedeutet, dass die Quell-IP-Adresse des ursprünglichen Clients für Pakete, die am Load Balancer ankommen, beibehalten wird. Sie können die Option deaktivieren, wenn Sie den Beschleuniger erstellen oder den Beschleuniger später bearbeiten.
- Wenn Sie einen internen Application Load Balancer oder eine EC2-Instanz mit Global Accelerator verwenden, ist für den Endpunkt immer die Client-IP-Adresserhaltung aktiviert.

> **Note**
>
> Global Accelerator unterstützt keine Client-IP-Adresserhaltung für Network Load Balancer und Elastic IP-Adressenendpunkte.

Beachten Sie beim Hinzufügen der Client-IP-Adresse Folgendes:

- Bevor Sie Datenverkehr an Endpunkte hinzufügen und weiterleiten, die die Client-IP-Adresse beibehalten, stellen Sie sicher, dass alle erforderlichen Sicherheitskonfigurationen, z. B. Sicherheitsgruppen, aktualisiert werden, um die IP-Adresse des Benutzerclients in Zulassungslisten aufzunehmen.
- Die Erhaltung der Client-IP-Adresse wird nur in bestimmten AWS Regionen unterstützt. Weitere Informationen finden Sie unter Unterstützte AWS Regionen für die Erhaltung der Client-IP-Adresse.

Themen

- So aktivieren Sie die Erhaltung der Client-IP-Adresse
- Die Vorteile der Client-IP-Adresse

- So bleibt die Client-IP-Adresse in AWS Global Accelerator erhalten
- Bewährte Methoden für die Erhaltung von Client-IP-Adressen
- Unterstützte AWS Regionen für die Erhaltung der Client-IP-Adresse

So aktivieren Sie die Erhaltung der Client-IP-Adresse

Wenn Sie einen neuen Accelerator erstellen, wird die Client-IP-Adresserhaltung standardmäßig für unterstützte Endpunkte aktiviert.

Achten Sie auf Folgendes:

- Interne Application Load Balancers und EC2-Instanzen haben die Client-IP-Adresserhaltung immer aktiviert. Sie können die Option für diese Endpunkte nicht deaktivieren.
- Wenn Sie die AWS Konsole zum Erstellen eines neuen Beschleunigers verwenden, ist die Option für die Erhaltung der Client-IP-Adresse standardmäßig für Application Load Balancer -Endpunkte aktiviert. Sie können die Option jederzeit deaktivieren, wenn Sie die Client-IP-Adresse für einen mit dem Internet verbundenen Application Load Balancer -Endpunkt nicht beibehalten möchten.
- Wenn Sie die AWS CLI oder eine API-Aktion verwenden, um einen neuen Beschleuniger zu erstellen und die Option für die Erhaltung der Client-IP-Adresse nicht angeben, ist die Beibehaltung der Client-IP-Adresse für Application Load Balancer -Endpunkte standardmäßig aktiviert.
- Global Accelerator unterstützt keine Client-IP-Adresserhaltung für Network Load Balancer und Elastic IP-Adressenendpunkte.

Bei vorhandenen Beschleunigern können Sie Endpunkte ohne Client-IP-Adresserhaltung auf Endpunkte umstellen, bei denen die Client-IP-Adresse beibehalten wird. Vorhandene Application Load Balancer -Endpunkte können auf neue Application Load Balancer -Endpunkte umgestellt werden, und vorhandene Elastic IP-Adressenendpunkte können auf EC2-Instance-Endpunkte umgestellt werden. (Network Load Balancer -Endpunkte unterstützen keine Client-IP-Adresserhaltung.) Für den Übergang zu den neuen Endpunkten empfiehlt es sich, den Datenverkehr langsam von einem vorhandenen Endpunkt auf einen neuen Endpunkt zu verschieben, der über die Erhaltung der Client-IP-Adresse verfügt. Gehen Sie folgendermaßen vor:

- Fügen Sie für vorhandene Application Load Balancer-Endpunkte zunächst zu Global Accelerator einen doppelten Application Load Balancer -Endpunkt hinzu, der dieselben Backends abzielt. Wenn es sich um einen Application Load Balancer mit dem Internet handelt, aktivieren Sie die Erhaltung der Client-IP-Adresse für diesen Endpunkt. Passen Sie dann die Gewichtungen auf den

Endpunkten an, um den Datenverkehr langsam vom Load Balancer zu verschieben, dernichtdie Erhaltung der Client-IP-Adressen für den Load Balancer aktiviert habenmitDie Client-IP-Adresse erhalten.

- Bei einem vorhandenen Elastic IP-Adressenendpunkt können Sie Datenverkehr auf einen EC2-Instance-Endpunkt verschieben, wobei die Client-IP-Adresse beibehalten wird. Fügen Sie zunächst Global Accelerator einen EC2-Instance-Endpunkt hinzu, und passen Sie dann die Gewichtungen auf den Endpunkten an, um den Datenverkehr langsam vom Elastic IP-Adressenendpunkt auf den EC2-Instance-Endpunkt zu verschieben.

Eine Schritt-für-Schritt-Anleitung finden Sie unterÜbergänge von Endpunkten zur Verwendung der Client-IP-Adresserhaltung.

Die Vorteile der Client-IP-Adresse

Bei Endpunkten, für die keine Client-IP-Adresserhaltung aktiviert ist, ersetzen die vom Global Accelerator-Dienst im Edge-Netzwerk verwendeten IP-Adressen die IP-Adresse des anfragenden Benutzers als Quelladresse in den ankommenden Paketen. Die Verbindungsinformationen des ursprünglichen Clients, z. B. die IP-Adresse des Clients und der Port des Clients, werden nicht beibehalten, wenn der Datenverkehr zu Systemen hinter einem Beschleuniger weitergeleitet wird. Dies funktioniert gut für viele Anwendungen, insbesondere solche, die für alle Benutzer wie öffentliche Websites verfügbar sind.

Für andere Anwendungen möchten Sie jedoch möglicherweise auf die ursprüngliche Client-IP-Adresse zugreifen, indem Sie Endpunkte mit Client-IP-Adresserhaltung verwenden. Wenn Sie beispielsweise über die Client-IP-Adresse verfügen, können Sie Statistiken basierend auf Client-IP-Adressen erfassen. Sie können auch IP-adressbasierte Filter wieSicherheitsgruppen auf Application Load Balancer, um Datenverkehr zu filtern. Sie können Logik, die spezifisch für die IP-Adresse eines Benutzers ist, in Ihren Anwendungen anwenden, die auf den Web-Tierservern hinter diesem Application Load Balancer -Endpunkt ausgeführt werden, indem Sie die`X-Forwarded-For`-Header, der die ursprünglichen IP-Adressinformationen des Clients enthält. Sie können die Client-IP-Adresserhaltung auch in Sicherheitsgruppenregeln in den Sicherheitsgruppen verwenden, die Ihrem Application Load Balancer zugeordnet sind. Weitere Informationen finden Sie unter So bleibt die Client-IP-Adresse in AWS Global Accelerator erhalten. Für EC2-Instance-Endpunkte wird die ursprüngliche Client-IP-Adresse beibehalten.

Für Endpunkte, die keine Client-IP-Adresserhaltung haben, können Sie nach der Quell-IP-Adresse filtern, die Global Accelerator verwendet, wenn der Datenverkehr vom Edge weiterleitet. Sie können

Informationen zu den Quell-IP-Adressen (bei denen es sich auch um Client-IP-Adressen handelt, wenn die Client-IP-Adresserhaltung aktiviert ist) eingehender Pakete anzeigen, indem Sie die Global Accelerator-Flussprotokolle überprüfen. Weitere Informationen finden Sie unter Standort- und IP-Adressbereiche von Global Accelerator-Edge-Servern und Flow-Protokolle in AWS Global Accelerator.

So bleibt die Client-IP-Adresse in AWS Global Accelerator erhalten

AWS Global Accelerator behält die Quell-IP-Adresse des Clients für Amazon EC2 Instances und Application Load Balancers unterschiedlich bei:

- Für einen EC2-Instance-Endpunkt wird die IP-Adresse des Clients für den gesamten Datenverkehr beibehalten.
- Für einen Application Load Balancer-Endpunkt mit Client-IP-Adresserhaltung arbeitet Global Accelerator zusammen mit dem Application Load Balancer, um eine`X-Forwarded`Header,`X-Forwarded-For`, das die IP-Adresse des ursprünglichen Clients enthält, damit Ihre Webebene darauf zugreifen kann.

Die HTTP-Anforderungen und -Antworten verwenden Header-Felder, um Informationen über HTTP-Nachrichten zu senden. Header-Felder sind durch einen Doppelpunkt getrennte Name/Wert-Paare, die durch eine Zeilenumschaltung und einen Zeilenvorschub getrennt sind. Ein Standardsatz von HTTP-Header-Feldern ist in RFC 2616,Nachrichtenkopfzeilen. Es sind auch Nicht-Standard-HTTP-Header verfügbar, die weithin von den Anwendungen verwendet werden. Einige der Nicht-Standard-HTTP-Header besitzen ein`X-Forwarded`Präfix.

Da ein Application Load Balancer eingehende TCP-Verbindungen beendet und neue Verbindungen zu Ihren Back-End-Zielen erstellt, werden Client-IP-Adressen nicht bis zum Zielcode (z. B. Instanzen, Container oder Lambda Code) beibehalten. Die Quell-IP-Adresse, die Ihre Ziele im TCP-Paket sehen, ist die IP-Adresse des Application Load Balancer. Ein Application Load Balancer behält jedoch die ursprüngliche Client-IP-Adresse bei, indem er sie von der Antwortadresse des ursprünglichen Pakets entfernt und in einen HTTP-Header einfügt, bevor er die Anforderung über eine neue TCP-Verbindung an Ihr Backend sendet.

Die`X-Forwarded-For`Request-Header ist wie folgt formatiert:

```
X-Forwarded-For: client-ip-address
```

Im folgenden Beispiel wird ein`X-Forwarded-For`-Anforderungs-Header für einen Client mit der IP-Adresse 203.0.113.7.

```
X-Forwarded-For: 203.0.113.7
```

Bewährte Methoden für die Erhaltung von Client-IP-Adressen

Wenn Sie die Client-IP-Adresserhaltung in AWS Global Accelerator verwenden, beachten Sie die Informationen und Best Practices in diesem Abschnitt für elastische Netzwerkschnittstellen und Sicherheitsgruppen.

Um die Erhaltung der Client-IP-Adressen zu unterstützen, erstellt Global Accelerator elastische Netzwerkschnittstellen in Ihrem AWS Konto — eine für jedes Subnetz, in dem ein Endpunkt vorhanden ist. Eine Elastic Network-Schnittstelle ist eine logische Netzwerkkomponente in einer VPC, die eine virtuelle Netzwerkkarte darstellt. Global Accelerator verwendet diese elastischen Netzwerkschnittstellen, um Datenverkehr zu den Endpunkten zu leiten, die hinter einem Beschleuniger konfiguriert sind. Die unterstützten Endpunkte für das Routing von Datenverkehr auf diese Weise sind Application Load Balancers (intern und internetorientiert) und Amazon EC2 Instances.

> **Note**
>
> Wenn Sie einen internen Application Load Balancer oder einen EC2-Instance-Endpunkt in Global Accelerator hinzufügen, können Sie den Internetverkehr direkt zum und vom Endpunkt in Virtual Private Clouds (VPCs) übertragen, indem Sie ihn in einem privaten Subnetz ansprechen. Weitere Informationen finden Sie unter Sichere VPC Verbindungen in AWS Global Accelerator.

Wie Global Accelerator elastische Netzwerkschnittstellen verwendet

Wenn ein Application Load Balancer mit aktivierter Client-IP-Adresserhaltung aktiviert ist, bestimmt die Anzahl der Subnetze, in denen sich der Load Balancer befindet, die Anzahl der elastischen Netzwerkschnittstellen, die Global Accelerator in Ihrem Konto erstellt. Global Accelerator erstellt eine elastic network interface für jedes Subnetz, das mindestens eine elastic network interface des Application Load Balancer enthält, die von einem Accelerator in Ihrem Konto geleitet wird.

Die Funktionsweise wird anhand der folgenden Beispiele deutlich:

- Beispiel 1: Wenn ein Application Load Balancer über elastische Netzwerkschnittstellen in Subnetz A und Subnetz B verfügt und Sie dann den Load Balancer als Beschleuniger-Endpunkt hinzufügen, erstellt Global Accelerator zwei elastische Netzwerkschnittstellen, eine in jedem Subnetz.
- Beispiel 2: Wenn Sie beispielsweise ein ALB1 mit elastischen Netzwerkschnittstellen in SubNetA und SubNetB zu Accelerator1 hinzufügen und dann ein ALB2 mit elastischen Netzwerkschnittstellen im Subnetz A und Subnetz B zu Accelerator2 hinzufügen, erstellt Global Accelerator nur zwei elastische Netzwerkschnittstellen: eine in SubNetA und eine in SubNetB.
- Beispiel 3: Wenn Sie Accelerator1 ein ALB1 mit elastischen Netzwerkschnittstellen in SubNetA und SubNetB hinzufügen und dann ein ALB2 mit elastischen Netzwerkschnittstellen in SubNetA und SubNetC zu Accelerator2 hinzufügen, erstellt Global Accelerator drei elastische Netzwerkschnittstellen: eine in SubNetA, eine in SubNetB und eine in SubNetC. Die elastic network interface in SubNetA liefert Datenverkehr sowohl für Accelerator1 als auch Accelerator2.

Wie in Beispiel 3 gezeigt, werden elastische Netzwerkschnittstellen über Beschleuniger hinweg wiederverwendet, wenn Endpunkte im selben Subnetz hinter mehreren Beschleunigern platziert werden.

Die logischen elastischen Netzwerkschnittstellen, die Global Accelerator erstellt, stellen keinen einzelnen Host, einen Durchsatzengpass oder einen einzelnen Fehlerpunkt dar. Wie andere AWS -Services, die als einzelne elastic network interface in einer Availability Zone oder einem Subnetz — Services wie einem NAT-Gateway (Network Address Translation) oder einem Network Load Balancer — erscheinen, wird Global Accelerator als horizontal skalierter, hoch verfügbarer Service implementiert.

Bewerten Sie die Anzahl der Subnetze, die von Endpunkten in Ihren Beschleunigern verwendet werden, um die Anzahl der elastischen Netzwerkschnittstellen zu ermitteln, die Global Accelerator erstellt. Bevor Sie einen Accelerator erstellen, stellen Sie sicher, dass genügend IP-Adressspeicherkapazität für die erforderlichen elastischen Netzwerkschnittstellen vorhanden ist, mindestens eine freie IP-Adresse pro relevantes Subnetz. Wenn Sie nicht genügend freien IP-Adressraum haben, müssen Sie ein Subnetz erstellen oder verwenden, das über ausreichenden freien IP-Adressraum für Ihren Application Load Balancer und die zugehörigen elastischen Netzwerkschnittstellen von Global Accelerator verfügt.

Wenn Global Accelerator feststellt, dass keine elastic network interface von keinem der Endpunkte in Beschleunigern in Ihrem Konto verwendet wird, löscht Global Accelerator die Schnittstelle.

Von Global Accelerator erstellte Sicherheitsgruppen

Lesen Sie die folgenden Informationen und bewährten Methoden, wenn Sie mit Global Accelerator und Sicherheitsgruppen arbeiten.

- Global Accelerator erstellt Sicherheitsgruppen, die seinen elastischen Netzwerkschnittstellen zugeordnet sind. Obwohl das System dies nicht verhindert, sollten Sie keine Sicherheitsgruppeneinstellungen für diese Gruppen bearbeiten.
- Global Accelerator löscht keine von ihm erstellten Sicherheitsgruppen. Global Accelerator löscht jedoch eine elastic network interface, wenn sie von keinem der Endpunkte in Beschleunigern in Ihrem Konto verwendet wird.
- Sie können die von Global Accelerator erstellten Sicherheitsgruppen als Quellgruppe in anderen von Ihnen verwalteten Sicherheitsgruppen verwenden, aber Global Accelerator leitet den Datenverkehr nur an die Ziele weiter, die Sie in Ihrer VPC angeben.
- Wenn Sie die Sicherheitsgruppenregeln ändern, die von Global Accelerator erstellt wurden, wird der Endpunkt möglicherweise fehlerhaft. Wenden Sie sich in diesem Fall an denAWS SupportWenn Sie Hilfe benötigen.
- Global Accelerator erstellt für jede VPC eine bestimmte Sicherheitsgruppe. Elastische Netzwerkschnittstellen, die für die Endpunkte innerhalb einer bestimmten VPC erstellt werden, verwenden alle dieselbe Sicherheitsgruppe, unabhängig davon, mit welchem Subnetz eine elastic network interface verknüpft ist.

Unterstützte AWS Regionen für die Erhaltung der Client-IP-Adresse

Sie können die Erhaltung der Client-IP-Adresse für AWS Global Accelerator in den folgenden AWS-Regionen aktivieren.

Name der Region	Region
US East (Ohio)	`us-east-2`
US East (N. Virginia)	`us-east-1`
US West (N. California)	`us-west-1 (except AZ usw1-az2)`

Name der Region	Region
US West (Oregon)	`us-west-2`
Africa (Cape Town)	`af-south-1`
Asia Pacific (Hong Kong)	`ap-east-1`
Asia Pacific (Mumbai)	`ap-south-1`
Asia Pacific (Osaka)	`ap-northeast-3`
Asia Pacific (Singapore)	`ap-southeast-1`
Asia Pacific (Sydney)	`ap-southeast-2`
Asia Pacific (Tokyo)	`ap-northeast-1 (except AZ apne1-az3)`
Asia Pacific (Seoul)	`ap-northeast-2`
Canada (Central)	`ca-central-1 (except AZ cac1-az3)`
Europe (Frankfurt)	`eu-central-1`
Europe (Ireland)	`eu-west-1`
Europe (London)	`eu-west-2`
Europe (Milan)	`eu-south-1`
Europe (Paris)	`eu-west-3`
Europe (Stockholm)	`eu-north-1`
Middle East (Bahrain)	`me-south-1`
South America (São Paulo)	`sa-east-1`

Protokollieren und Überwachen in

Sie können Flow-Protokollieren und AWS CloudTrail verwenden, um Ihren Accelerator in AWS Global Accelerator zu überwachen, Datenverkehrsmuster zu analysieren und Probleme mit Ihren Listener und -Endpunkte beheben.

Themen

- Flow-Protokolle in AWS Global Accelerator
- Verwenden von Amazon CloudWatch mit AWS Global Accelerator
- Verwenden von AWS CloudTrail zum Protokollieren von API-Aufrufen von AWS Global Accelerator

Flow-Protokolle in AWS Global Accelerator

Mit Flow-Protokollen können Sie Informationen zum Datenverkehr über die IP-Adresse zu und von Netzwerkschnittstellen in Ihrem Accelerator in AWS Global Accelerator erfassen. Flow-Protokolldaten werden in Amazon S3 veröffentlicht, wo Sie Ihre Daten abrufen und anzeigen können, nachdem Sie ein Flow-Protokoll erstellt haben.

Flow-Protokolle können Ihnen bei einer Reihe von Aufgaben helfen. Sie können beispielsweise Probleme beheben, wenn bestimmter Datenverkehr keinen Endpunkt erreicht, was es Ihnen wiederum ermöglicht, übermäßig beschränkende Sicherheitsgruppenregeln zu erkennen. Sie können auch Flow-Protokolle als Sicherheitstool verwenden, um den Datenverkehr zu überwachen, der Ihre Endpunkte erreicht.

Ein Flow-Protokolldatensatz repräsentiert einen Netzwerk-Flow in Ihrem Flow-Protokoll. Jeder Datensatz erfasst den Netzwerk-Flow für ein bestimmtes 5-Tupel für einen bestimmten Erfassungszeitraum. Ein 5-Tupel besteht aus fünf verschiedenen Werten, die Quelle, Ziel und Protokoll für einen IP-Flow angeben. Der Erfassungszeitraum ist die Zeitdauer, in der der Flow-Protokoll-Service Daten erfasst, bevor diese in Flow-Protokolldatensätzen veröffentlicht werden. Das Erfassungsfenster beträgt etwa 10 Sekunden, kann jedoch auch bis zu 1 Minute dauern.

Bei der Verwendung von Flow-Protokollen fallen Gebühren für CloudWatch Logs an, selbst wenn Protokolle direkt in Amazon S3 veröffentlicht werden. Weitere Informationen finden Sie unterProtokolle an S3 übermittelnumPreise für Amazon CloudWatch.

Themen

- Veröffentlichen von Flow-Protokollen auf Amazon S3

- Zeitplan der Dateizustellung von Protokolldateien
- Syntax des Flow-Protokolldat

Veröffentlichen von Flow-Protokollen auf Amazon S3

Flow-Protokolle für AWS Global Accelerator werden in Amazon S3 in einem von Ihnen angegebenen S3-Bucket veröffentlicht. Flow-Protokolldatensätze werden in einer Reihe von Protokolldateiobjekten veröffentlicht, die im -Bucket gespeichert sind.

Informationen zum Erstellen eines Amazon S3-Buckets für die Verwendung mit Flow-Protokollen finden Sie unter Erstellen eines Buckets im Amazon Simple Storage Service Handbuch "Erste Schritte".

Dateien für Flow-Protokolle

Flow-Protokolle erfassen Flow-Protokolldatensätze, fassen sie in Protokolldateien zusammen und veröffentlichen die Protokolldateien in 5-Minuten-Intervallen in dem Amazon S3-Bucket. Jede Protokolldatei enthält Flow-Protokolldatensätze für den in den letzten fünf Minuten aufgezeichneten IP-Adressverkehr.

Die maximale Dateigröße für eine Protokolldatei beträgt 75 MB. Wenn die Protokolldatei die Dateigrößenbeschränkung innerhalb des 5-Minuten-Zeitraums erreicht, fügt das Flow-Protokoll keine weiteren Flow-Protokollsätze hinzu, veröffentlicht sie im Amazon S3 Bucket und erstellt dann eine neue Protokolldatei.

Protokolldateien werden in dem angegebenen Amazon S3-Bucket gespeichert. Dazu wird eine Ordnerstruktur verwendet, die von der ID des Flow-Protokolls, der Region und dem Erstellungsdatum bestimmt wird. Die Bucket-Ordnerstruktur verwendet das folgende Format:

```
s3-bucket_name/s3-bucket-prefix/AWSLogs/aws_account_id/globalaccelerator/region/yyyy/
mm/dd/
```

Ebenso wird der Name der Protokolldatei anhand der ID des Flow-Protokolls, der Region sowie dem Datum und der Uhrzeit der Erstellung bestimmt. Dateinamen müssen das folgende Format verwenden:

```
aws_account_id_globalaccelerator_accelerator_id_flow_log_id_timestamp_hash.log.gz
```

Beachten Sie Folgendes zur Ordner- und Dateinamenstruktur für Protokolldateien:

- Der Zeitstempel verwendet das Format `YYYYMMDDTHHmmZ`.
- Wenn Sie Schrägstrich (/) für das S3-Bucket-Präfix angeben, enthält die Protokolldatei-Bucket-Ordnerstruktur einen doppelten Schrägstrich (//) wie folgt:

```
s3-bucket_name//AWSLogs/aws_account_id
```

Das folgende Beispiel zeigt die Ordnerstruktur und den Dateinamen einer Protokolldatei für ein vom AWS Konto erstelltes Flow-Protokoll`123456789012`für einen Beschleuniger mit der ID`1234abcd-abcd-1234-abcd-1234abcdefgh`, am 23. November 2018 um 00:05 UTC:

```
my-s3-bucket/prefix1/AWSLogs/123456789012/globalaccelerator/us-
west-2/2018/11/23/123456789012_globalaccelerator_1234abcd-abcd-1234-
abcd-1234abcdefgh_20181123T0005Z_1fb1234.log.gz
```

Eine einzelne Flow-Protokolldatei enthält interleaved Einträge mit mehreren 5-Tupel-Datensätzen, d. h.`client_ip`,`client_port`,`accelerator_ip`,`accelerator_port`,`protocol`. Um alle Flow-Protokolldateien für den Accelerator anzuzeigen, suchen Sie nach Einträgen, die von der`accelerator_id`und Ihre`account_id`.

IAM-Rollen zum Veröffentlichen von Flow-Protokollen in Amazon S3

Ein IAM-Prinzipal, wie z. B. ein IAM-Benutzer, muss über ausreichende Berechtigungen zum Veröffentlichen von Flow-Protokollen im Amazon S3 Bucket verfügen. Die IAM-Richtlinie muss die folgende Berechtigungen umfassen:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DeliverLogs",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogDelivery",
                "logs:DeleteLogDelivery"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowGlobalAcceleratorService",
            "Effect": "Allow",
```

```
            "Action": [
                "globalaccelerator:*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "s3Perms",
            "Effect": "Allow",
            "Action": [
                "s3:GetBucketPolicy",
                "s3:PutBucketPolicy"
            ],
            "Resource": "*"
        }
    ]
}
```

Amazon S3-Bucket-Berechtigungen für Flow-Protokolle

Standardmäßig sind Amazon S3 Buckets und die darin enthaltenen Objekte privat. Nur der Bucket-Besitzer kann auf den Bucket und die darin gespeicherten Objekte zugreifen. Der Bucket-Besitzer kann jedoch anderen Ressourcen und Benutzern Zugriffsberechtigungen gewähren, indem er eine Zugriffsrichtlinie schreibt.

Wenn der Benutzer, der das Flow-Protokoll erstellt, den Bucket besitzt, fügt der Dienst automatisch die folgende Richtlinie an den Bucket an, um dem Flow-Protokoll die Berechtigung zum Veröffentlichen von Protokollen darin zu erteilen:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryWrite",
            "Effect": "Allow",
            "Principal": {"Service": "delivery.logs.amazonaws.com"},
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::bucket_name/optional_folder/AWSLogs/account_id/
*",
            "Condition": {"StringEquals": {"s3:x-amz-acl": "bucket-owner-full-
control"}}
        },
        {
```

```
            "Sid": "AWSLogDeliveryAclCheck",
            "Effect": "Allow",
            "Principal": {"Service": "delivery.logs.amazonaws.com"},
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::bucket_name"
        }
    ]
}
```

Wenn der Benutzer, der das Flow-Protokoll erstellt, nicht Eigentümer des Buckets ist, hat er keine `GetBucketPolicy`- und `PutBucketPolicy`-Berechtigungen für den Bucket und das Flow-Protokoll kann nicht erstellt werden. In diesem Fall muss der Bucket-Besitzer dem Bucket die vorherige Richtlinie manuell hinzufügen und die AWS Konto-ID des Erstellers des Flow-Protokolls angeben. Weitere Informationen finden Sie unterWie füge ich eine S3-Bucket-Richtlinie hinzu?imHandbuch „Erste Schritte“ für Amazon Simple Storage Service. Wenn der Bucket Flow-Protokolle von mehreren Konten erhält, fügen Sie der `AWSLogDeliveryWrite`-Richtlinienanweisung für jedes Konto einen `Resource`-Elementeintrag hinzu.

Die folgende Bucket-Richtlinie beispielsweise gestattet den AWS Konten 123123123123 und 456456456456, Flow-Protokolle in einem Ordner namens`flow-logs`In einem -Bucket mit dem Namen`log-bucket`:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryWrite",
            "Effect": "Allow",
            "Principal": {"Service": "delivery.logs.amazonaws.com"},
            "Action": "s3:PutObject",
            "Resource": [
             "arn:aws:s3:::log-bucket/flow-logs/AWSLogs/123123123123/*",
             "arn:aws:s3:::log-bucket/flow-logs/AWSLogs/456456456456/*"
             ],
            "Condition": {"StringEquals": {"s3:x-amz-acl": "bucket-owner-full-
control"}}
        },
        {
            "Sid": "AWSLogDeliveryAclCheck",
            "Effect": "Allow",
            "Principal": {"Service": "delivery.logs.amazonaws.com"},
            "Action": "s3:GetBucketAcl",
```

```
            "Resource": "arn:aws:s3:::log-bucket"
        }
    ]
}
```

> **Note**
>
> Wir empfehlen, dass Sie die`AWSLogDeliveryAclCheck`und`AWSLogDeliveryWrite`-Berechtigungen an den Protokollbereitstellungs-Service-Prinzipal statt einzelnen AWS Konten-ARNs.

Erforderliche CMK-Schlüsselrichtlinie zur Verwendung mit SSE-KMS Buckets

Wenn Sie serverseitige Verschlüsselung für Ihren Amazon S3-Bucket unter Verwendung von AWS KMS-verwalteten Schlüsseln (SSE-KMS) mit einem vom Kunden verwalteten Kundenmasterschlüssel (Customer Master Key, CMK) aktiviert haben, müssen Sie der Schlüsselrichtlinie für Ihren CMK Folgendes hinzufügen, damit die Flow-Protokolle Protokolldateien in den Bucket schreiben können:

```
{
    "Sid": "Allow AWS Global Accelerator Flow Logs to use the key",
    "Effect": "Allow",
    "Principal": {
        "Service": [
            "delivery.logs.amazonaws.com"
        ]
    },
    "Action": "kms:GenerateDataKey*",
    "Resource": "*"
}
```

Amazon S3-Protokolldateiberechtigungen

Zusätzlich zu den erforderlichen Bucket-Richtlinien verwendet Amazon S3 Zugriffskontrolllisten (ACLs), um den Zugriff auf die durch ein Flow-Protokoll erzeugten Protokolldateien zu verwalten. Standardmäßig hat der Bucket-Eigentümer `FULL_CONTROL`-Berechtigungen für jede Protokolldatei. Der Protokollbereitstellungseigentümer hat keine Berechtigungen, wenn er nicht gleichzeitig der Bucket-Eigentümer ist. Das Konto für die Protokollbereitstellung hat `READ`- und `WRITE`-Berechtigungen. Weitere Informationen finden Sie unter[Zugriffskontrolllisten (ACL) – Übersicht]imHandbuch „Erste Schritte“ für Amazon Simple Storage Service.

Aktivieren Sie die Veröffentlichung von Flow-Protokollen in Amazon S3

Führen Sie die Schritte in diesem Verfahren aus, um Flussprotokolle in AWS Global Accelerator zu aktivieren.

So aktivieren Sie Flow-Protokolle in AWS Global Accelerator

1. Erstellen Sie einen Amazon S3 Bucket für Ihre Flow-Protokolle in Ihrem AWS Konto.
2. Fügen Sie die erforderliche IAM-Richtlinie für den AWS Benutzer hinzu, der die Flow-Protokolle aktiviert. Weitere Informationen finden Sie unter IAM-Rollen zum Veröffentlichen von Flow-Protokollen in Amazon S3.
3. Führen Sie den folgenden AWS CLI-Befehl mit dem Amazon S3 Bucket-Namen und dem Präfix aus, das Sie für Ihre Protokolldateien verwenden möchten:

```
aws globalaccelerator update-accelerator-attributes
       --accelerator-arn
 arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-
abcd-1234abcdefgh
       --region us-west-2
       --flow-logs-enabled
       --flow-logs-s3-bucket s3-bucket-name
       --flow-logs-s3-prefix s3-bucket-prefix
```

Verarbeiten von Flow-Protokolldatensätzen in Amazon S3

Die Protokolldateien werden komprimiert. Wenn Sie die Protokolldateien unter Verwendung der Amazon S3-Konsole öffnen, werden sie dekomprimiert und die Flow-Protokolldatensätze werden angezeigt. Wenn Sie die Dateien herunterladen, müssen Sie sie dekomprimieren, um die Flow-Protokolldatensätze anzuzeigen.

Zeitplan der Dateizustellung von Protokolldateien

AWS Global Accelerator kann mehrmals pro Stunde Protokolldateien für Ihren konfigurierten Accelerator bereitstellen. Im Allgemeinen enthält eine Protokolldatei Informationen zu den Anfragen, die Ihr Accelerator während eines bestimmten Zeitraums erhalten hat. Normalerweise übermittelt Global Accelerator die Protokolldatei für diesen Zeitraum innerhalb einer Stunde, nachdem Ereignisse im Protokoll erfasst werden, an Ihren Amazon S3 Bucket. Einige oder auch alle Protokolldateieinträge für einen bestimmten Zeitraum können manchmal um bis zu 24 Stunden verzögert werden.

Wenn es zu einer Verzögerung kommt, speichert Global Accelerator die Protokolleinträge in einer Protokolldatei, in der die Dateinamen das Datum und die Uhrzeit des Zeitraums enthalten, in dem die Anfragen aufgetreten sind, und nicht die Daten des Zeitraums, in dem die Datei übermittelt wurde.

Beim Erstellen einer Protokolldatei fasst Global Accelerator Informationen für Ihren Accelerator von allen Edge-Standorten zusammen, die während des von der Protokolldatei abgedeckten Zeitraums Anfragen erhalten haben.

Ca. vier Stunden, nachdem die Protokollierung aktiviert wurde, beginnt Global Accelerator damit, regelmäßig Protokolldateien zu übermitteln. Möglicherweisen erhalten Sie ein paar Protokolldateien auch schon vorher.

> **Note**
>
> Wenn während eines bestimmten Zeitraums keine Benutzer mit Ihrem Accelerator verbunden sind, erhalten Sie keine Protokolldateien für diesen Zeitraum.

Syntax des Flow-Protokolldat

Ein Flow-Protokolldatensatz ist eine durch Leerzeichen getrennte Zeichenfolge im folgenden Format:

```
<version> <aws_account_id> <accelerator_id> <client_ip>
<client_port> <accelerator_ip> <accelerator_port> <endpoint_ip>
<endpoint_port> <protocol> <ip_address_type> <packets>
<bytes> <start_time> <end_time> <action> <log-status>
<globalaccelerator_source_ip> <globalaccelerator_source_port>
<endpoint_region> <globalaccelerator_region> <direction> <vpc_id>
```

Das Format Version 1.0 enthält nicht den VPC Bezeichner,`vpc_id`. Das Format Version 2.0-Format, das`vpc_id`, wird generiert, wenn Global Accelerator Datenverkehr an einen Endpunkt mit der Erhaltung der Client-IP-Adresse sendet.

Die folgende Tabelle beschreibt die Felder eines Flow-Protokolldatensatzes.

Feld	Beschreibung
`version`	Die Version der Flow Logs.

Feld	Beschreibung
`aws_account_id`	Die AWS-Kontonummer für das Flow-Protokoll
`accelerator_id`	Die ID des Accelerators, für den der Datenverkehr aufgezeichnet wird.
`client_ip`	Die IPv4-Quelladresse.
`client_port`	Der Quellport.
`accelerator_ip`	IP-Adresse des Accelerators
`accelerator_port`	Der Hafen des Beschleunigers.
`endpoint_ip`	Ziel-IP-Adresse des Datenverkehrs
`endpoint_port`	Der Zielport des Datenverkehrs
`protocol`	Die IANA-Protokollnummer des Datenverkehrs. Weitere Informationen finden Sie unter Zugewiesene IP-Nummern.
`ip_address_type`	IPv4
`packets`	Die Anzahl der Pakete, die während des Erfassungszeitraums übertragen wurden
`bytes`	Die Anzahl der Byte, die während des Erfassungszeitraums übertragen wurden
`start_time`	Der Anfangszeitpunkt des Erfassungszeitraums in Unix-Sekunden
`end_time`	Der Endzeitpunkt des Erfassungszeitraums in Unix-Sekunden

Feld	Beschreibung
`action`	Die Aktion im Zusammenhang mit dem Datenverkehr • `ACCEPT`: Der erfasste Datenverkehr wurde von den Sicherheitsgruppen oder Netzwerk-ACLs zugelassen. Der Wert ist derzeit immer ACCEPT.
`log-status`	Der Protokollstatus des Flow-Protokolls: • `OK`: Daten werden normal auf den ausgewählten Zielen protokolliert. • `NODATA`: Es gab während des Erfassungszeitraums keinen Datenverkehr von oder zur Netzwerkschnittstelle. • `SKIPDATA`: Einige Flow-Protokolldatensätze wurden im Erfassung szeitraum übersprungen. Dies kann an internen Kapazitätsbeschränkungen oder einem internen Fehler liegen.
`globalaccelerator_source_ip`	Die IP-Adresse, die von der Global Accelerator-Netzwerkschnittstelle verwendet wird.
`globalaccelerator_source_port`	Der Port, der von der Global Accelerator-Netzwerkschnittstelle verwendet wird.
`endpoint_region`	Die AWS Region, in der sich der Endpunkt befindet.
`globalaccelerator_region`	Der Edge-Standort (Anwesenheitsort), an dem die Anfrage verarbeitet wurde. Jeder Edge-Standort hat einen Code aus drei Buchstaben und eine willkürlich zugewiesene Zahl, z. B. DFW3. Der Code aus drei Buchstaben entspricht dem Code der International Air Transport Association für einen Flughafen in der Nähe des Edge-Standorts. (Diese Abkürzungen ändern sich möglicherweise in der Zukunft.)

Feld	Beschreibung
`direction`	Die Richtung des Verkehrs. Bezeichnet den Datenverkehr, der in das Global Accelerator-Netzwerk (`INGRESS`) oder zum Client zurückkehren (`EGRESS`) enthalten.
`vpc_id`	Der VPC Bezeichner. In der Version 2.0-Flussprotokolle enthalten, wenn Global Accelerator Datenverkehr an einen Endpunkt mit der Erhaltung der Client-IP-Adresse sendet.

Wenn ein Feld nicht für einen bestimmten Datensatz gilt, wird für diesen Eintrag ein '-' angezeigt.

Verwenden von Amazon CloudWatch mit AWS Global Accelerator

AWS Global Accelerator veröffentlicht Datenpunkte in Amazon CloudWatch für Ihre Accelerator. CloudWatch ermöglicht Ihnen, Statistiken zu diesen Datenpunkten als geordneten Satz von Zeitreihendaten, bekannt als-Metriken. Sie können sich eine Metrik als eine zu überwachende Variable und die Datenpunkte als die Werte dieser Variable im Laufe der Zeit vorstellen. Sie können beispielsweise Datenverkehr über einen Accelerator über einen bestimmten Zeitraum überwachen. Jeder Datenpunkt verfügt über einen zugewiesenen Zeitstempel und eine optionale Maßeinheit.

Mit den Metriken können Sie überprüfen, ob Ihr System die erwartete Leistung zeigt. Sie können z. B. einen CloudWatch-Alarm erstellen, um eine bestimmte Metrik zu überwachen, und eine Aktion einleiten (z. B. Senden einer Benachrichtigung an eine E-Mail-Adresse), wenn die Metrik außerhalb eines für Sie akzeptablen Bereichs liegt.

Global Accelerator meldet nur dann Metriken an CloudWatch, wenn Anfragen über den Accelerator geleitet werden. Wenn Anfragen über den Accelerator geleitet werden, misst Global Accelerator diese und sendet seine Metriken in 60 Sekunden-Intervallen. Wenn keine Anfragen über den Accelerator erfolgen oder keine Daten für eine Metrik vorliegen, wird die Metrik nicht gemeldet.

Weitere Informationen finden Sie im Amazon CloudWatch-Benutzerhandbuch.

Inhalt

- Metriken für Global Accelerator —
- Metrikdimensionen für Acceleratoren
- Statistiken für Global Accelerator Metriken

- Anzeigen von CloudWatch Metriken für Ihre Accelerators

Metriken für Global Accelerator —

Der `AWS/GlobalAccelerator`-Namespace enthält die folgenden Metriken.

Metrik	Beschreibung
`NewFlowCount`	Die Gesamtanzahl neuer TCP-und UDP-Datenflüsse (oder Verbindungen), die zwischen Clients und Endpunkten in dem Zeitraum eingerichtet wurden. Berichtkriterien: Ein Wert ungleich Null. Statistiken: Die einzige nützliche Statistik ist`Sum`. Dimensions • `Accelerator` • `Accelerator, Listener` • `Accelerator, Listener, EndpointGroup` • `Accelerator, SourceRegion` • `Accelerator, DestinationEdge` • `Accelerator, TransportProtocol` • `Accelerator, AcceleratorIPAddress`
`ProcessedBytesIn`	Die Gesamtanzahl der eingehenden Bytes, die vom Accelerator verarbeitet wurden, einschließlich der TCP/IP-Header. Diese Anzahl umfasst den gesamten Datenverkehr zu Endpunkten. Berichtkriterien: Ein Wert ungleich Null. Statistiken: Die einzige nützliche Statistik ist`Sum`. Dimensions • `Accelerator` • `Accelerator, Listener`

Metrik	Beschreibung
	• `Accelerator, Listener, EndpointGroup` • `Accelerator, SourceRegion` • `Accelerator, DestinationEdge` • `Accelerator, TransportProtocol` • `Accelerator, AcceleratorIPAddress`
`ProcessedBytesOut`	Die Gesamtanzahl der ausgehenden Bytes, die vom Accelerator verarbeitet werden, einschließlich der TCP/IP-Header. Diese Anzahl umfasst Datenverkehr von Endpunkten abzüglich des Datenverkehrs für Zustandsprüfungen. Berichtkriterien: Ein Wert ungleich Null. Statistiken: Die einzige nützliche Statistik ist`Sum`. Dimensions • `Accelerator` • `Accelerator, Listener` • `Accelerator, Listener, EndpointGroup` • `Accelerator, SourceRegion` • `Accelerator, DestinationEdge` • `Accelerator, TransportProtocol` • `Accelerator, AcceleratorIPAddress`

Metrikdimensionen für Acceleratoren

Verwenden Sie die nachstehenden Dimensionen, um die Metriken für den Accelerator zu filtern.

Dimension	Beschreibung
`Accelerator`	Filtert die Metrikdaten nach Accelerator. Geben Sie den Beschleun iger mit der Beschleuniger-ID an (dem letzten Teil des Beschleuniger-ARN). Wenn der ARN beispielsweise folgenden Namen hat:`arn:aws:g`

Dimension	Beschreibung
	`lobalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-abcd-1234abcdefgh` geben Sie Folgendes an:**`1234abcd-abcd-1234-abcd-1234abcdefgh`** .
`Listener`	Filtert die Metrikdaten nach Listener. Geben Sie den Listener anhand der Listener-ID (dem letzten Teil des Listener ARN) an. Wenn der ARN beispielsweise folgenden Namen hat:`arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-abcd-1234abcdefgh/listener/0123wxyz` geben Sie Folgendes an:**`0123wxyz`**.
`EndpointGroup`	Filtert die Metrikdaten nach der Endpunktgruppe. Geben Sie die Endpunktgruppe nach der AWS Region an, z. B.**`us-east-1`** (alle Kleinbuchstaben).
`SourceRegion`	Filtert die Metrikdaten nach Quellregion, d. h. der geografische Bereich der AWS Regionen, in denen Ihre Anwendungsendpunkte ausgeführt werden. Der Quellbereich ist einer der folgenden Optionen: • NA — Vereinigte Staaten und Kanada • EU — Europa • AP — Asien-Pazifik* • KR — Südkorea • IN — Indien — Indien • AU — Australien • ME — Naher Osten • SA — Südamerika *Ohne Südkorea und Indien

Dimension	Beschreibung
`DestinationEdge`	Filtert die Metrikdaten nach Zieledge, d. h. dem geografischen Bereich der AWS Edge-Standorte, die den Clientdatenverkehr bedienen. Der Zielrand ist einer der folgenden Optionen: • NA — Vereinigte Staaten und Kanada • EU — Europa • AP — Asien-Pazifik* • KR — Südkorea • IN — Indien — Indien • AU — Australien • ME — Naher Osten • SA — Südamerika • ZA — Südafrika *Ohne Südkorea und Indien
`Transport Protocol`	Filtert die Metrikdaten nach dem Transportprotokoll: UDP oder TCP.
`Accelerator IPAddress`	Filtert die Metrikdaten nach der IP-Adresse des Accelerator, d. h. einer der statischen IP-Adressen, die einem Accelerator zugewiesen wurden.

Statistiken für Global Accelerator Metriken

CloudWatch stellt Statistiken basierend auf den von Global Accelerator veröffentlichten Metrik-Datenpunkten bereit. Statistiken sind Aggregationen von Metrikdaten über einen bestimmten Zeitraum. Wenn Sie Statistiken anfordern, wird der zurückgegebene Datenstrom durch den Metriknamen und die Dimension identifiziert. Eine Dimension ist ein Name-Wert-Paar, durch das eine Metrik eindeutig identifiziert wird. Sie können beispielsweise die verarbeiteten Bytes für einen Accelerator anfordern, bei dem die Bytes von AWS Edge-Standorten in Europa bereitgestellt werden (Zieledge ist „EU“).

Im Folgenden finden Sie Beispiele für Metrik-/Dimensionskombinationen, die Sie möglicherweise nützlich finden:

- Zeigen Sie die Menge des Datenverkehrs an, der von jeder Ihrer beiden Accelerator-IP-Adressen bereitgestellt wird (z. B. ProcessedBytesOut), um zu überprüfen, ob Ihre DNS-Konfiguration korrekt ist.
- Zeigen Sie die geografische Verteilung Ihres Benutzerverkehrs an und überwachen Sie, wie viel davon lokal (z. B. Nordamerika nach Nordamerika) oder global (z. B. Australien oder Indien nach Nordamerika) ist. Um dies zu bestimmen, zeigen Sie die Metriken ProcessedBytesin oder ProcessedBytesOut an, wobei die Dimensionen DestinationEdge und SourceRegion auf bestimmte Werte festgelegt sind.

Anzeigen von CloudWatch Metriken für Ihre Accelerators

Sie können die CloudWatch Metriken für Ihre Accelerators über die CloudWatch-Konsole oder die AWS CLI anzeigen. In der Konsole werden Metriken als Überwachungsdiagramme angezeigt. Die Überwachungsdiagramme zeigen Datenpunkte nur dann an, wenn der Accelerator aktiv ist und Anfragen erhält.

Sie müssen CloudWatch Metriken für Global Accelerator in der Region USA West (Oregon) sowohl in der Konsole als auch bei Verwendung der AWS CLI anzeigen. Wenn Sie die AWS Befehlszeilenschnittstelle verwenden, geben Sie die Region USA West (Oregon) für Ihren Befehl an, indem Sie den folgenden Parameter angeben:`--region us-west-2`.

So zeigen Sie Metriken mit der CloudWatch-Konsole an:

1. Öffnen Sie die CloudWatch Konsole unterhttps://us-west-2.console.aws.amazon.com/cloudwatch/home?region=us-west-2.
2. Wählen Sie im Navigationsbereich Metrics aus.
3. Wählen Sie das ausGlobalAccelerator-Namespace.
4. (Optional) Um eine Metrik für alle Dimensionen anzuzeigen, geben Sie den Namen in das Suchfeld ein.

So zeigen Sie Metriken mit der AWS-Befehlszeilenschnittstelle (CLI) an

Verwenden Sie den folgenden list-metrics-Befehl, um die verfügbaren Metriken aufzuführen:

```
aws cloudwatch list-metrics --namespace AWS/GlobalAccelerator --region us-west-2
```

So rufen Sie die Statistiken für eine Metrik mithilfe der AWS Befehlszeilenschnittstelle ab:

Verwenden Sie folgende Informationen:get-metric-statistics-Befehl, um Statistiken für eine bestimmte Metrik und Dimension abzurufen. Beachten Sie, dass CloudWatch jede eindeutige Kombination von Dimensionen als separate Metrik behandelt. Sie können keine Statistiken abrufen, die Kombinationen von Dimensionen verwenden, die nicht speziell veröffentlicht wurden. Sie müssen die gleichen Dimensionen angeben, die bei der Erstellung der Metriken verwendet wurden.

Im folgenden Beispiel wird die gesamte verarbeitete Bytes pro Minute für den Accelerator aufgeführt, der vom Zielrand Nordamerika (NA) aus bedient.

```
aws cloudwatch get-metric-statistics --namespace AWS/GlobalAccelerator \
--metric-name ProcessedBytesIn \
--region us-west-2 \
--statistics Sum --period 60 \
--dimensions Name=Accelerator,Value=1234abcd-abcd-1234-abcd-1234abcdefgh
 Name=DestinationEdge,Value=NA \
--start-time 2019-12-18T20:00:00Z --end-time 2019-12-18T21:00:00Z
```

Das folgende Beispiel zeigt die Ausgabe des Befehls:

```
{
    "Label": "ProcessedBytesIn",
    "Datapoints": [
        {
            "Timestamp": "2019-12-18T20:45:00Z",
            "Sum": 2410870.0,
            "Unit": "Bytes"
        },
        {
            "Timestamp": "2019-12-18T20:47:00Z",
            "Sum": 0.0,
            "Unit": "Bytes"
        },
        {
            "Timestamp": "2019-12-18T20:46:00Z",
            "Sum": 0.0,
            "Unit": "Bytes"
        },
```

```
        {
            "Timestamp": "2019-12-18T20:42:00Z",
            "Sum": 1560.0,
            "Unit": "Bytes"
        },
        {
            "Timestamp": "2019-12-18T20:48:00Z",
            "Sum": 0.0,
            "Unit": "Bytes"
        },
        {
            "Timestamp": "2019-12-18T20:43:00Z",
            "Sum": 1343.0,
            "Unit": "Bytes"
        },
        {
            "Timestamp": "2019-12-18T20:49:00Z",
            "Sum": 0.0,
            "Unit": "Bytes"
        },
        {
            "Timestamp": "2019-12-18T20:44:00Z",
            "Sum": 35791560.0,
            "Unit": "Bytes"
        }
    ]
}
```

Verwenden von AWS CloudTrail zum Protokollieren von API-Aufrufen von AWS Global Accelerator

AWS Global Accelerator ist in AWS CloudTrail integriert, einen Service, der die Aktionen eines Benutzers, einer Rolle oder eines AWS in Global Accelerator protokolliert. CloudTrail erfasst alle API-Aufrufe für Global Accelerator als Ereignisse, einschließlich Aufrufen von der Global Accelerator-Konsole und von Code-Aufrufen an die Global Accelerator-API. Wenn Sie einen Trail erstellen, aktivieren Sie die kontinuierliche Bereitstellung von CloudTrail -Ereignissen an einen Amazon S3 Bucket, einschließlich Ereignissen für Global Accelerator. Auch wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse in der CloudTrail-Konsole in Event history (Ereignisverlauf) anzeigen.

Weitere Informationen zu CloudTrail finden Sie im AWS CloudTrail User Guide.

Informationen zu Global Accelerator

CloudTrail wird beim Erstellen Ihres AWS-Kontos für Sie aktiviert. Die in Global Accelerator auftretenden Aktivitäten werden als CloudTrail -Ereignis zusammen mit anderen AWS -Serviceereignissen inEreignisverlauf. Sie können die neusten Ereignisse in Ihr(em) AWS-Konto anzeigen, suchen und herunterladen. Weitere Informationen finden Sie unter Anzeigen von Ereignissen mit dem CloudTrail -API-Ereignisverlauf.

Erstellen Sie für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem AWS Konto (einschließlich Ereignissen für Global Accelerator) einen Trail. Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3-Bucket. Wenn Sie einen Pfad in der Konsole anlegen, gilt dieser standardmäßig für alle Regionen. Der Pfad protokolliert Ereignisse aus allen Regionen in der AWS-Partition und stellt die Protokolldateien in dem Amazon S3-Bucket bereit, den Sie angeben. Darüber hinaus können Sie andere AWS-Services konfigurieren, um die in den CloudTrail-Protokollen erfassten Ereignisdaten weiter zu analysieren und entsprechend zu agieren. Weitere Informationen finden Sie unter den folgenden Themen:

- Übersicht zum Erstellen eines Pfads
- Von CloudTrail unterstützte Services und Integrationen
- Konfigurieren von Amazon SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail-Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail-Protokolldateien aus mehreren Konten

Alle Global Accelerator-Accelerator-Aktionen werden von CloudTrail protokolliert. Sie sind in derAWS Global Accelerator-API-Referenz. Zum Beispiel werden durch Aufrufe`CreateAccelerator`,`ListAccelerators`und`UpdateAccelerator`-Vorgänge generieren Einträge in den CloudTrail -Protokolldateien.

Jedes Event oder jeder Protokolleintrag enthält Informationen über den Ersteller der Anfrage. Anhand der Identitätsinformationen zur Benutzeridentität können Sie Folgendes bestimmen:

- Ob die Anfrage mit Root- oder IAM-Benutzeranmeldeinformationen ausgeführt wurde
- Ob die Anfrage mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen föderierten Benutzer ausgeführt wurde
- Ob die Anforderung von einem anderen AWS-Service getätigt wurde

Weitere Informationen finden Sie unter CloudTrail userIdentity-Element.

Grundlagen der Global Accelerator-Protokolldateieinträge

Ein Trail ist eine Konfiguration, durch die Ereignisse als Protokolldateien an den von Ihnen angegebenen Amazon S3-Bucket übermittelt werden. Jede CloudTrail-Protokolldatei im JSON-Format enthält einen oder mehrere Einträge. Ein Protokolleintrag stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält unter anderem Informationen über die angeforderte Aktion, etwaige Parameter und das Datum und die Uhrzeit der Aktion. Die Protokolleinträge folgen keiner bestimmten Reihenfolge, sie sind kein geordnetes Stacktrace der API-Aufrufe.

Das folgende Beispiel zeigt einen CloudTrail -Protokolleintrag, der die folgenden Global Accelerator-Aktionen enthält:

- Auflisten der Beschleuniger für ein Konto:`eventName`ist`ListAccelerators`.
- Erstellen eines Listeners:`eventName`ist`CreateListener`.
- Aktualisieren eines Listeners:`eventName`ist`UpdateListener`.
- Beschreibung eines Listeners:`eventName`ist`DescribeListener`.
- Auflisten der Listener für ein Konto:`eventName`ist`ListListeners`.
- Löschen eines Listeners:`eventName`ist`DeleteListener`.

```
{
  "Records": [
    {
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/smithj",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2018-11-17T21:02:36Z"
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "A1B2C3D4E5F6G7EXAMPLE",
            "arn": "arn:aws:iam::111122223333:user/smithj",
            "accountId": "111122223333",
```

```
            "userName": "smithj"
          }
        }
      },
      "eventTime": "2018-11-17T21:03:14Z",
      "eventSource": "globalaccelerator.amazonaws.com",
      "eventName": "ListAccelerators",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.50",
      "userAgent": "aws-cli/1.16.34 Python/2.7.10 Darwin/16.7.0 botocore/1.12.24",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "083cae81-28ab-4a66-862f-096e1example",
      "eventID": "fe8b1c13-8757-4c73-b842-fe2a3example",
      "eventType": "AwsApiCall",
      "recipientAccountId": "111122223333"
    },
    {
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/smithj",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2018-11-17T21:02:36Z"
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "A1B2C3D4E5F6G7EXAMPLE",
            "arn": "arn:aws:iam::111122223333:user/smithj",
            "accountId": "111122223333",
            "userName": "smithj"
          }
        }
      },
      "eventTime": "2018-11-17T21:04:49Z",
      "eventSource": "globalaccelerator.amazonaws.com",
      "eventName": "CreateListener",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.50",
```

```
      "userAgent": "aws-cli/1.16.34 Python/2.7.10 Darwin/16.7.0 botocore/1.12.24",
      "requestParameters": {
        "acceleratorArn":
 "arn:aws:globalaccelerator::111122223333:accelerator/0339bfd6-13bc-4d45-
a114-5d7fexample",
        "portRanges": [
          {
            "fromPort": 80,
            "toPort": 80
          }
        ],
        "protocol": "TCP"
      },
      "responseElements": {
        "listener": {
          "listenerArn":
 "arn:aws:globalaccelerator::111122223333:accelerator/0339bfd6-13bc-4d45-
a114-5d7fexample/listener/abcde1234",
          "portRanges": [
            {
              "fromPort": 80,
              "toPort": 80
            }
          ],
          "protocol": "TCP",
          "clientAffinity": "NONE"
        }
      },
      "requestID": "6090509a-5a97-4be6-8e6a-7d73example",
      "eventID": "9cab44ef-0777-41e6-838f-f249example",
      "eventType": "AwsApiCall",
      "recipientAccountId": "111122223333"
    },
    {
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/smithj",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
```

```
            "creationDate": "2018-11-17T21:02:36Z"
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "A1B2C3D4E5F6G7EXAMPLE",
            "arn": "arn:aws:iam::111122223333:user/smithj",
            "accountId": "111122223333",
            "userName": "smithj"
          }
        }
      },
      "eventTime": "2018-11-17T21:03:52Z",
      "eventSource": "globalaccelerator.amazonaws.com",
      "eventName": "CreateAccelerator",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.50",
      "userAgent": "aws-cli/1.16.34 Python/2.7.10 Darwin/16.7.0 botocore/1.12.24",
      "requestParameters": {
        "name": "cloudTrailTest"
      },
      "responseElements": {
        "accelerator": {
          "acceleratorArn":
 "arn:aws:globalaccelerator::111122223333:accelerator/0339bfd6-13bc-4d45-
a114-5d7fexample",
          "name": "cloudTrailTest",
          "ipAddressType": "IPV4",
          "enabled": true,
          "ipSets": [
            {
              "ipFamily": "IPv4",
              "ipAddresses": [
                "192.0.2.213",
                "192.0.2.200"
              ]
            }
          ],
          "status": "IN_PROGRESS",
          "createdTime": "Nov 17, 2018 9:03:52 PM",
          "lastModifiedTime": "Nov 17, 2018 9:03:52 PM"
        }
      },
      "requestID": "d2d7f300-2f0b-4bda-aa2d-e67d6e4example",
      "eventID": "11f9a762-8c00-4fcc-80f9-848a29example",
```

```
      "eventType": "AwsApiCall",
      "recipientAccountId": "111122223333"
    },
    {
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/smithj",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2018-11-17T21:02:36Z"
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "A1B2C3D4E5F6G7EXAMPLE",
            "arn": "arn:aws:iam::111122223333:user/smithj",
            "accountId": "111122223333",
            "userName": "smithj"
          }
        }
      },
      "eventTime": "2018-11-17T21:05:27Z",
      "eventSource": "globalaccelerator.amazonaws.com",
      "eventName": "UpdateListener",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.50",
      "userAgent": "aws-cli/1.16.34 Python/2.7.10 Darwin/16.7.0 botocore/1.12.24",
      "requestParameters": {
        "listenerArn":
 "arn:aws:globalaccelerator::111122223333:accelerator/0339bfd6-13bc-4d45-
a114-5d7fexample/listener/abcde1234",
        "portRanges": [
          {
            "fromPort": 80,
            "toPort": 80
          },
          {
            "fromPort": 81,
            "toPort": 81
          }
```

```
        ]
      },
      "responseElements": {
        "listener": {
          "listenerArn":
 "arn:aws:globalaccelerator::111122223333:accelerator/0339bfd6-13bc-4d45-
a114-5d7fexample/listener/abcde1234",
          "portRanges": [
            {
              "fromPort": 80,
              "toPort": 80
            },
            {
              "fromPort": 81,
              "toPort": 81
            }
          ],
          "protocol": "TCP",
          "clientAffinity": "NONE"
        }
      },
      "requestID": "008ef93c-b3a3-44b4-afb3-768example",
      "eventID": "85958f0d-63ff-4a2c-99e3-6ffbexample",
      "eventType": "AwsApiCall",
      "recipientAccountId": "111122223333"
    },
    {
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/smithj",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2018-11-17T21:02:36Z"
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "A1B2C3D4E5F6G7EXAMPLE",
            "arn": "arn:aws:iam::111122223333:user/smithj",
            "accountId": "111122223333",
```

```
            "userName": "smithj"
          }
        }
      },
      "eventTime": "2018-11-17T21:06:05Z",
      "eventSource": "globalaccelerator.amazonaws.com",
      "eventName": "DescribeListener",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.50",
      "userAgent": "aws-cli/1.16.34 Python/2.7.10 Darwin/16.7.0 botocore/1.12.24",
      "requestParameters": {
        "listenerArn":
 "arn:aws:globalaccelerator::111122223333:accelerator/0339bfd6-13bc-4d45-
a114-5d7fexample/listener/abcde1234"
      },
      "responseElements": null,
      "requestID": "9980e368-82fa-40da-95a3-4b0example",
      "eventID": "885a02e9-2a60-4626-b1ba-57285example",
      "eventType": "AwsApiCall",
      "recipientAccountId": "111122223333"
    },
    {
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/smithj",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2018-11-17T21:02:36Z"
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "A1B2C3D4E5F6G7EXAMPLE",
            "arn": "arn:aws:iam::111122223333:user/smithj",
            "accountId": "111122223333",
            "userName": "smithj"
          }
        }
      },
      "eventTime": "2018-11-17T21:05:47Z",
```

```
      "eventSource": "globalaccelerator.amazonaws.com",
      "eventName": "ListListeners",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.50",
      "userAgent": "aws-cli/1.16.34 Python/2.7.10 Darwin/16.7.0 botocore/1.12.24",
      "requestParameters": {
        "acceleratorArn":
 "arn:aws:globalaccelerator::111122223333:accelerator/0339bfd6-13bc-4d45-
a114-5d7fexample"
      },
      "responseElements": null,
      "requestID": "08e4b0f7-689b-4c84-af2d-47619example",
      "eventID": "f4fb8e41-ed21-404d-af9d-037c4example",
      "eventType": "AwsApiCall",
      "recipientAccountId": "111122223333"
    },
    {
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/smithj",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2018-11-17T21:02:36Z"
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "A1B2C3D4E5F6G7EXAMPLE",
            "arn": "arn:aws:iam::111122223333:user/smithj",
            "accountId": "111122223333",
            "userName": "smithj"
          }
        }
      },
      "eventTime": "2018-11-17T21:06:24Z",
      "eventSource": "globalaccelerator.amazonaws.com",
      "eventName": "DeleteListener",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.50",
      "userAgent": "aws-cli/1.16.34 Python/2.7.10 Darwin/16.7.0 botocore/1.12.24",
```

```
      "requestParameters": {
        "listenerArn":
 "arn:aws:globalaccelerator::111122223333:accelerator/0339bfd6-13bc-4d45-
a114-5d7fexample/listener/abcde1234"
      },
      "responseElements": null,
      "requestID": "04d37bf9-3e50-41d9-9932-6112example",
      "eventID": "afedb874-2e21-4ada-b1b0-2ddb2example",
      "eventType": "AwsApiCall",
      "recipientAccountId": "111122223333"
    }
  ]
}
```

Sicherheit von AWS Global Accelerator

Cloud-Sicherheit hat bei AWS höchste Priorität. Als AWS-Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die zur Erfüllung der Anforderungen von Organisationen entwickelt wurden, für die Sicherheit eine kritische Bedeutung hat.

Sicherheit ist eine übergreifende Verantwortlichkeit zwischen AWS und Ihnen. Im Modell der übergreifenden Verantwortlichkeit wird Folgendes mit „Sicherheit der Cloud“ bzw. „Sicherheit in der Cloud“ umschrieben:

- Sicherheit der Cloud – AWS ist zuständig für den Schutz der Infrastruktur, die AWS-Services in der AWS Cloud ausführt. AWS stellt Ihnen außerdem Services bereit, die Sie sicher verwenden können. Die Wirksamkeit unserer Sicherheitsfunktionen wird regelmäßig von externen Prüfern im Rahmen von AWS-Compliance-Programmen getestet und überprüft. Weitere Informationen zu den Compliance-Programmen, die für Global Accelerator gelten, finden Sie unterAWS-Services in Scope nach Compliance-Programm.
- Sicherheit in der Cloud – Ihr Verantwortungsumfang wird durch den AWS-Service bestimmt, den Sie verwenden. In Ihre Verantwortung fallen außerdem weitere Faktoren, wie z. B. die Vertraulichkeit der Daten, die Anforderungen Ihrer Organisation sowie geltende Gesetze und Vorschriften.

Diese Dokumentation beschreibt, wie Sie das Modell der übergreifenden Verantwortlichkeit bei der Verwendung von Global Accelerator anwenden können. Die folgenden Themen veranschaulichen, wie Sie Global Accelerator so konfigurieren, dass Ihre Sicherheitsziele erfüllt sind.

Themen

- Identity and Access Management für AWS Global Accelerator
- Sichere VPC Verbindungen in AWS Global Accelerator
- Protokollieren und überwachen in AWS Global Accelerator
- Compliance-Validierung für AWS Global Accelerator
- Ausfallsicherheit in AWS Global Accelerator
- Sicherheit der Infrastruktur in AWS Global Accelerator

Identity and Access Management für AWS Global Accelerator

AWS Identity and Access Management (IAM) ist ein AWS -Service, der es einem Administrator ermöglicht, den Zugriff auf AWS-Ressourcen, einschließlich AWS Global Accelerator Ressourcen, sicher zu steuern. Administratoren verwenden IAM, um zu steuern, werauthentifiziert(angemeldet) undAuthorized(hat Berechtigungen), um Global Accelerator-Ressourcen zu verwenden. IAM ist eine Funktion, die ohne zusätzliche Gebühren in Ihrem AWS Konto enthalten ist.

> **Important**
>
> Wenn Sie mit IAM nicht vertraut sind, lesen Sie die Informationen auf dieser Seite und dann unterErste Schritte mit IAM. Weitere Informationen zur Authentifizierung und Zugriffskontrolle finden Sie unterWas ist Authentifizierung?,Was ist Zugriffskontrolle?, undWas sind Richtlinien?.

Themen

- Konzepte und Begriffe
- Erforderliche Berechtigungen für den Konsolenzugriff, die Authentifizierungsverwaltung und die Zugriffssteuerung
- Funktionsweise von Global Accelerator mit IAM
- Fehlerbehebung bei der Authentifizierung und Zugriffskontrolle

Konzepte und Begriffe

Authentifizierung— Um sich bei AWS anzumelden, müssen Sie eine der folgenden Optionen verwenden: Root-Benutzeranmeldeinformationen (nicht empfohlen), IAM-Benutzeranmeldeinformationen oder temporäre Anmeldeinformationen mit IAM-Rollen. Weitere Informationen zu diesen Entitys finden Sie unter Was ist Authentifizierung?.

Zugriffskontrolle— AWS Administratoren verwenden Richtlinien zum Steuern des Zugriffs auf AWS-Ressourcen, wie z. B. Beschleuniger in Global Accelerator. Weitere Informationen hierzu finden Sie unter Was ist Zugriffskontrolle? und Was sind Richtlinien?.

> **Important**
>
> Alle Ressourcen in einem Konto gehören diesem Konto, unabhängig davon, wer diese Ressourcen erstellt hat. Sie müssen Zugang erhalten, um eine Ressource zu erstellen. Nur weil Sie eine Ressource erstellt haben, bedeutet das jedoch nicht, dass Sie automatisch vollen Zugriff auf diese Ressource haben. Ein Administrator muss explizit Berechtigungen für jede Aktion erteilen, die Sie ausführen möchten. Dieser Administrator kann Ihre Berechtigungen jederzeit wieder aufheben.

Um die Grundlagen der Funktionsweise von IAM zu verstehen, schauen Sie sich die folgenden Begriffe an:

Ressourcen

AWS -Services wie Global Accelerator und IAM umfassen typischerweise Objekte, die Ressourcen genannt werden. In den meisten Fällen können Sie diese Ressourcen erstellen, verwalten und aus dem Service löschen. Zu den IAM-Ressourcen gehören Benutzer, Gruppen, Rollen und Richtlinien:

Benutzer

Ein IAM-Benutzer stellt die Person oder Anwendung dar, die ihre Anmeldeinformationen für die Interaktion mit AWS verwendet. Ein Benutzer besteht aus einem Namen und einem Passwort zur Anmeldung bei der AWS Management Console sowie bis zu zwei Zugriffsschlüsseln, die mit der AWS-CLI oder AWS-API verwendet werden können.

Gruppen

Eine IAM-Gruppe ist eine Auswahl von IAM-Benutzern. Mithilfe von Gruppen können Administratoren Berechtigungen für Mitgliederbenutzer angeben. Dies erleichtert den Administrator die Verwaltung von Berechtigungen für mehrere Benutzer.

Rollen

Einer Rolle eine IAM-Rolle sind keine langfristigen Anmeldeinformationen (Passwörter oder Zugriffsschlüssel) zugeordnet. Eine Rolle kann bei Bedarf von jedem angenommen werden, der dazu berechtigt ist. Ein IAM-Benutzer kann eine Rolle annehmen, um vorübergehend verschiedene Berechtigungen für eine bestimmte Aufgabe zu erlangen. Verbundene Benutzer können eine Rolle übernehmen, indem sie einen externen Identitätsanbieter verwenden, der

der Rolle zugeordnet ist. Einige AWS -Services können davon ausgehen, dass-ServicerolleSie können in Ihrem Namen auf AWS Ressourcen zugreifen.

Richtlinien

Richtlinien sind JSON-Dokumente, die die Berechtigungen für das Objekt definieren, mit dem sie verbunden sind. AWS unterstütztIdentitätsbasierte -RichtlinienAnfügen von Identitäten (Benutzern, Gruppen oder Rollen). Einige AWS -Services ermöglichen es Ihnen,Ressourcenbasierte -RichtlinienUm zu steuern, was ein Prinzipal (Person oder Anwendung) mit dieser Ressource machen kann. Ressourcenbasierte Richtlinien werden von Global Accelerator nicht unterstützt.

Identitäten

Identitäten sind IAM-Ressourcen, für die Sie Berechtigungen definieren können. Dies sind beispielsweise Benutzer, Gruppen und Rollen.

Entitäten

Entitys sind IAM-Ressourcen, die Sie für die Authentifizierung verwenden. Dies sind beispielsweise Benutzer und Rollen.

Prinzipale

Prinzipale In AWS ist ein Prinzipal eine Person oder Anwendung, die eine Entity verwendet, um sich anzumelden und Anforderungen an AWS zu senden. Als Prinzipal können Sie die AWS Management Console, die AWS-CLI oder die AWS-API verwenden, um einen Vorgang auszuführen (z. B. Löschen eines Accelerators). Dies erstellt eine Anforderung für diese Operation. Ihre Anfrage gibt eine Aktion, eine Ressource, einen Prinzipal und ein Prinzipalkonto an und enthält alle zusätzlichen Informationen zu Ihrer Anfrage. Alle diese Informationen stellen AWS bereitcontextfür Ihre Anfrage. AWS prüft alle Richtlinien, die für den Kontext Ihrer Anfrage gelten. AWS autorisiert die Anfrage nur, wenn sämtliche Teile der Anfrage gemäß der Richtlinien zulässig sind.

Informationen zum Anzeigen eines Diagramms des Authentifizierungs- und Zugriffskontrollprozesses finden Sie unterGrundlegendes zur Funktionsweise von IAMimIAM-Benutzerhandbuch. Weitere Informationen darüber, wie AWS bestimmt, ob eine Anfrage zulässig ist, finden Sie unterAuswertungslogik für RichtlinienimIAM-Benutzerhandbuch.

Erforderliche Berechtigungen für den Konsolenzugriff, die Authentifizierungsverwaltung und die Zugriffssteuerung

Zum Verwenden des Global Accelerator oder zur Verwaltung der Autorisierung und der Zugriffskontrolle für sich selbst oder andere Personen benötigen Sie die richtigen Berechtigungen.

Erforderliche Berechtigungen zum Erstellen eines Global Accelerator Accelerators

Um einen AWS Global Accelerator Accelerator zu erstellen, müssen Benutzer über die Berechtigung verfügen, serviceverknüpfte Rollen zu erstellen, die dem Global Accelerator zugeordnet sind.

Um sicherzustellen, dass Benutzer über die richtigen Berechtigungen zum Erstellen von Beschleunigern in Global Accelerator verfügen, fügen Sie dem Benutzer eine Richtlinie wie die folgenden an.

> **Note**
>
> Wenn Sie eine identitätsbasierte Berechtigungsrichtlinie erstellen, die restriktiver ist, können Benutzer mit dieser Richtlinie keine Accelerator erstellen.

```
{
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": "globalaccelerator.amazonaws.com"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/
globalaccelerator.amazonaws.com/AWSServiceRoleForGlobalAccelerator*"
    }
```

Erforderliche Berechtigungen für die Verwendung der Global Accelerator-Konsole

Um auf die AWS Global Accelerator Konsole zugreifen zu können, müssen Sie über einen Mindestsatz von Berechtigungen verfügen, mit dem Sie Details zu den Global Accelerator-Ressourcen in Ihrem AWS Konto auflisten und anzeigen können. Wenn Sie eine identitätsbasierte Berechtigungsrichtlinie erstellen, die restriktiver als die mindestens erforderlichen Berechtigungen ist, funktioniert die Konsole für Entitäten mit dieser Richtlinie nicht wie vorgesehen.

Um sicherzustellen, dass diese Entitäten dennoch die Global Accelerator Console oder API-Aktionen verwenden können, fügen Sie dem -Benutzer auch eine der folgenden von AWS verwalteten Richtlinien an, wie unterErstellen von Richtlinien auf der Registerkarte "JSON":

```
        GlobalAcceleratorReadOnlyAccess
        GlobalAcceleratorFullAccess
```

Fügen Sie die erste Richtlinie,`GlobalAcceleratorReadOnlyAccess`, wenn Benutzer nur Informationen in der Konsole anzeigen oder Aufrufe an die AWS CLI oder die API tätigen müssen, die`List*`oder .`Describe*`verwenden.

Fügen Sie die zweite Richtlinie`GlobalAcceleratorFullAccess`an Benutzer, die Beschleuniger erstellen oder Aktualisierungen vornehmen müssen. Die Vollzugriffsrichtlinie umfasstFULLBerechtigungen für Global Accelerator sowieBeschreibenBerechtigungen für Amazon EC2 und Elastic Load Balancing.

> **Note**
>
> Wenn Sie eine identitätsbasierte Berechtigungsrichtlinie erstellen, die nicht die erforderlichen Berechtigungen für Amazon EC2 und Elastic Load Balancing enthält, können Benutzer mit dieser Richtlinie keine Amazon EC2- und Elastic Load Balancing-Ressourcen zu Accelerators hinzufügen.

Im Folgenden finden Sie die Richtlinie für den vollständigen Zugriff:

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

```
                "globalaccelerator:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeInstances",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeSubnets",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DeleteSecurityGroup",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/AWSServiceName": "GlobalAccelerator"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSecurityGroup",
                "ec2:DescribeSecurityGroups"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "elasticloadbalancing:DescribeLoadBalancers",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": [
```

```
                "arn:aws:ec2:*:*:security-group/*",
                "arn:aws:ec2:*:*:network-interface/*"
            ]
        }
    ]
}
```

Erforderliche Berechtigungen für die Authentifizierungsverwaltung

Um Ihre eigenen Anmeldeinformationen wie Passwort, Zugriffsschlüssel und Multifaktor-Authentifizierungs (MFA)-Geräte zu verwalten, muss Ihnen Ihr Administrator die erforderlichen Berechtigungen erteilen. Die Richtlinie mit diesen Berechtigungen finden Sie unter Berechtigen Sie Benutzern, ihre Anmeldeinformationen selbst zu verwalten.

Als AWS Administrator benötigen Sie vollen Zugriff auf IAM, damit Sie Benutzer, Gruppen, Rollen und Richtlinien in IAM erstellen und verwalten können. Verwenden Sie die OptionAdministratorAccessVon AWS verwaltete Richtlinie, die vollen Zugriff auf alle AWS umfasst. Diese Richtlinie bietet keinen Zugriff auf die AWS Fakturierung und die Kostenverwaltungskonsole und erlaubt Aufgaben, die AWS-Kontowurzel-Benutzeranmeldeinformationen erfordern. Weitere Informationen finden Sie unterAWS Aufgaben, die AWS Kontostammbenutzer erfordernimAllgemeine AWS-Referenz.

> **Warning**
>
> Nur ein Benutzer mit Administratorrechten sollte vollen Zugriff auf AWS haben. Jeder, für den diese Richtlinie gilt, hat die Berechtigung, die Authentifizierung und die Zugriffskontrolle vollständig zu verwalten, zusätzlich zur Änderung aller Ressourcen in AWS. Informationen zum Erstellen dieses Benutzers finden Sie unter Erstellen Sie Ihren IAM-Admin-Benutzer.

Für die Zugriffskontrolle erforderliche Berechtigungen

Wenn Ihr Administrator Ihnen IAM-Benutzeranmeldeinformationen zur Verfügung gestellt hat, hat er Ihrem IAM-Benutzer Richtlinien zugewiesen, die festlegen, auf welche Ressourcen Sie zugreifen können. Zum Anzeigen der Richtlinien, die Ihrer Benutzeridentität in der AWS Management Console zugewiesen wurden, benötigen Sie folgende Berechtigungen:

```
{
    "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": "ListUsersViewGroupsAndPolicies",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Wenn Sie zusätzliche Berechtigungen benötigen, bitten Sie Ihren Administrator, Ihre Richtlinien zu aktualisieren, damit Sie auf die von Ihnen benötigten Aktionen zugreifen können.

Funktionsweise von Global Accelerator mit IAM

Services können auf verschiedene Weise mit IAM arbeiten:

Aktionen

Global Accelerator unterstützt die Verwendung von Aktionen in einer Richtlinie. Dadurch kann ein Administrator steuern, ob eine Entity einen Vorgang in Global Accelerator durchführen kann. Um

beispielsweise einer Entität zu erlauben, die`GetPolicy`AWS API-Vorgang, um eine Richtlinie anzuzeigen, muss ein Administrator eine Richtlinie zuweisen, die die`iam:GetPolicy`Aktion

Mit der folgenden -Beispielrichtlinie kann ein Benutzer die`CreateAccelerator`, um programmgesteuert einen Beschleuniger für Ihr AWS Konto zu erstellen:

```
{
   "Version": "2018-08-08",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "globalaccelerator:CreateAccelerator"
         ],
         "Resource":"*"
      }
   ]
}
```

Berechtigungen auf Ressourcenebene

Global Accelerator unterstützt Berechtigungen auf Ressourcenebene. Berechtigungen auf Ressourcenebene ermöglichen es Ihnen, ARNs zu verwenden, um einzelne Ressourcen in der Richtlinie festzulegen.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien werden von Global Accelerator nicht unterstützt. Bei ressourcenbasierten Richtlinien können Sie eine Richtlinie an eine Ressource innerhalb des Services anfügen. Ressourcenbasierte Richtlinien umfassen eine`Principal`-Element verwenden, um anzugeben, welche IAM-Identitäten auf diese Ressource zugreifen können.

Tagbasierte Autorisierung

Global Accelerator unterstützt autorisierungsbasierte Tags. Mit dieser Funktion können Sie Ressourcen-Tags in der Bedingung einer Richtlinie verwenden.

Temporäre Anmeldeinformationen

Global Accelerator unterstützt temporäre Anmeldeinformationen. Mit temporären Anmeldeinformationen können Sie sich über einen Verbund anmelden, eine IAM-Rolle oder eine kontenübergreifende Rolle übernehmen. Temporäre

Sicherheitsanmeldeinformationen erhalten Sie durch Aufrufen von AWS STS API-Operationen wie`AssumeRole`oder .`GetFederationToken`.

Serviceverknüpfte Rollen

Global Accelerator unterstützt serviceverknüpfte Rollen. Diese Funktion ermöglicht einem Service das Annehmen einer serviceverknüpften Rolle in Ihrem Namen. Diese Rolle gewährt dem Service Zugriff auf Ressourcen in anderen Services, um eine Aktion in Ihrem Namen auszuführen. Serviceverknüpfte Rollen werden in Ihrem IAM-Konto angezeigt und gehören zum Service. Ein IAM-Administrator kann die Berechtigungen für serviceverknüpfte Rollen anzeigen, aber nicht bearbeiten.

Servicerollen

Service-Rollen werden von Global Accelerator nicht unterstützt. Diese Funktion ermöglicht einem Service das Annehmen einer Servicerolle in Ihrem Namen. Diese Rolle gewährt dem Service Zugriff auf Ressourcen in anderen Services, um eine Aktion in Ihrem Namen auszuführen. Servicerollen werden in Ihrem IAM-Konto angezeigt und gehören zum Konto. Dies bedeutet, dass ein IAM-Administrator die Berechtigungen für diese Rolle ändern kann. Dies kann jedoch die Funktionalität des Services beeinträchtigen.

Fehlerbehebung bei der Authentifizierung und Zugriffskontrolle

Verwenden Sie die folgenden Informationen, um häufige Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit IAM auftreten können.

Themen

- Ich bin nicht zur Ausführung einer Aktion in Global Accelerator autorisiert
- Ich bin Administrator und möchte anderen den Zugriff auf Global Accelerator ermöglichen
- Ich möchte IAM verstehen, ohne ein Experte zu werden

Ich bin nicht zur Ausführung einer Aktion in Global Accelerator autorisiert

Wenn die AWS Managementkonsole Ihnen mitteilt, dass Sie nicht zur Ausführung einer Aktion autorisiert sind, müssen Sie sich an den Administrator wenden, der Ihnen Ihren Benutzernamen und Ihr Passwort mitgeteilt hat.

Das folgende Beispiel tritt auf, wenn ein IAM-Benutzer namens`my-user-name`versucht, die -Konsole zum Ausführen des`globalaccelerator:CreateAccelerator`-Aktion, hat aber keine Berechtigungen:

```
User: arn:aws:iam::123456789012:user/my-user-name is not authorized to perform: aws-globalaccelerator:CreateAccelerator on resource: my-example-accelerator
```

Bitten Sie in diesem Fall Ihren Administrator, Ihre Richtlinien zu aktualisieren, damit Sie auf die`my-example-accelerator`Verwenden der -Ressource`aws-globalaccelerator:CreateAccelerator`Aktion

Ich bin Administrator und möchte anderen den Zugriff auf Global Accelerator ermöglichen

Um anderen Personen oder einer Anwendung Zugriff auf Global Accelerator zu gewähren, müssen Sie eine IAM-Entität (Benutzer oder Rolle) für die Person oder Anwendung erstellen, die Zugriff benötigt. Diese verwendet dann die Anmeldeinformationen für diese Entität, um auf AWS zuzugreifen. Anschließend müssen Sie der Entität eine Richtlinie anfügen, die dieser die korrekten Berechtigungen in Global Accelerator gewährt.

Informationen zu den ersten Schritten finden Sie unter Erste Schritte mit IAM.

Ich möchte IAM verstehen, ohne ein Experte zu werden

Weitere Informationen zu IAM-Begriffen, -Konzepten und -Verfahren finden Sie in den folgenden Themen:

- Was ist Authentifizierung?
- Was ist Zugriffskontrolle?
- Was sind Richtlinien?

Tagbasierte Richtlinien

Wenn Sie IAM-Richtlinien entwerfen, können Sie detaillierte Berechtigungen festlegen, indem sie den Zugriff auf bestimmte Ressourcen gewähren. Mit zunehmender Anzahl der Ressourcen, die Sie verwalten, wird diese Aufgabe erschwert. Durch Markieren von Beschleunigern und Verwenden von Tags in Richtlinienanweisungsbedingungen lässt sich diese Aufgabe vereinfachen. Sie erteilen Massenzugriff auf einen beliebigen Beschleuniger mit einem bestimmten Tag. Anschließend wenden

Sie dieses Tag wiederholt auf relevante Accelerators an, wenn Sie den Accelerator erstellen oder den Accelerator zu einem späteren Zeitpunkt aktualisieren.

> **Note**
>
> Das Verwenden von Tags in Bedingungen ist eine Möglichkeit zur Kontrolle des Zugriffs auf Ressourcen und Anfragen. Weitere Informationen zum Tagging in Global Accelerator finden Sie unterTaggen in AWS Global Accelerator.

Tags können einer Ressource angehängt oder in der Anfrage an Services weitergeleitet werden, die das Markieren unterstützen. In Global Accelerator können nur Beschleuniger Tags enthalten. Wenn Sie eine IAM-Richtlinie erstellen, können Sie Tag-Bedingungsschlüssel verwenden, um Folgendes zu kontrollieren:

- Welche Benutzer Aktionen für einen Accelerator ausführen können, basierend auf bereits vorhandenen Tags.
- Welche Tags in der Anforderung einer Aktion übergeben werden können.
- Ob bestimmte Tag-Schlüssel in einer Anforderung verwendet werden können.

Weitere Informationen zur vollständigen Syntax und Semantik der Tag-Bedingungsschlüssel finden Sie unterSteuern des Zugriffs mit IAM-TagsimIAM-Benutzerhandbuch.

Zum Beispiel kann der Global Accelerator`GlobalAcceleratorFullAccess`Die verwaltete Benutzerrichtlinie gewährt Benutzern die uneingeschränkte Berechtigung, eine globale Accelerator-Aktion auf allen Ressourcen auszuführen. Mit der folgenden Richtlinie wird Benutzern die Berechtigung verweigert, alle Aktionen des globalen Accelerators für alleProduktion-Accelerators. Der Administrator eines Kunden muss diese IAM-Richtlinie nicht autorisierten IAM-Benutzern hinzufügen, zusätzlich zu der verwalteten Benutzerrichtlinie.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Deny",
         "Action":"*",
         "Resource":"*",
         "Condition":{
            "ForAnyValue:StringEquals":{
```

```
                "aws:RequestTag/stage":"prod"
            }
        }
    },
    {
        "Effect":"Deny",
        "Action":"*",
        "Resource":"*",
        "Condition":{
            "ForAnyValue:StringEquals":{
                "aws:ResourceTag/stage":"prod"
            }
        }
    }
  ]
}
```

Serviceverknüpfte Rolle für Global Accelerator

AWS Global Accelerator verwendet ein AWS Identity and Access Management (IAM)Service-verknüpfte -Rolle. Eine serviceverknüpfte Rolle ist ein spezieller Typ von IAM-Rolle, der direkt mit einem Service verknüpft ist. Serviceverknüpfte Rollen werden vom Service vordefiniert und beinhalten alle Berechtigungen, die dieser zum Aufrufen anderer AWS-Services in Ihrem Namen benötigt.

Global Accelerator verwendet die folgende IAM-serviceverknüpfte Rolle:

- AWSServiceRoleForGlobalAccelerator— Global Accelerator verwendet diese Rolle, damit Global Accelerator Ressourcen erstellen und verwalten kann, die für die Erhaltung der Client-IP-Adressen erforderlich sind.

Global Accelerator erstellt automatisch eine Rolle namens AWSServiceRoleForGlobalAccelerator, wenn die Rolle zum ersten Mal zur Unterstützung eines Global Accelerator-API-Vorgangs erforderlich ist. Die Rolle „AWSServiceRoleForGlobalAccelerator“ ermöglicht es Global Accelerator, Ressourcen zu erstellen und zu verwalten, die für die Erhaltung der Client-IP-Adressen erforderlich sind. Diese Rolle ist für die Verwendung von Beschleunigern in Global Accelerator erforderlich. Der ARN für die Rolle „AWSServiceRoleForGlobalAccelerator“ sieht folgendermaßen aus:

```
arn:aws:iam::123456789012:role/aws-service-role/
globalaccelerator.amazonaws.com/AWSServiceRoleForGlobalAccelerator
```

Eine serviceverknüpfte Rolle vereinfacht das Einrichten und Verwenden von Global Accelerator, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. Global Accelerator definiert die Berechtigungen seiner servicegebundenen Rolle. Nur Global Accelerator kann die Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Die Berechtigungsrichtlinie kann an keine andere IAM-Entität angefügt werden.

Sie müssen alle verknüpften Ressourcen des globalen Accelerators entfernen, bevor Sie eine serviceverknüpfte Rolle löschen können. Dies trägt zum Schutz Ihrer Global Accelerator-Ressourcen bei. Es wird sichergestellt wird, dass Sie keine serviceverknüpfte Rolle entfernen, die noch für den Zugriff auf aktive Ressourcen erforderlich ist.

Informationen zu anderen Services, die serviceverknüpfte Rollen unterstützen, finden Sie unter AWS-Services, die mit IAM funktionieren. Suchen Sie nach den Services, für die Ja in der Spalte Serviceverknüpfte Rolle angegeben ist.

Berechtigungen für serviceverknüpfte Rollen für Global Accelerator

Global Accelerator verwendet eine serviceverknüpfte Rolle namens.AWSServiceRoleForGlobalAccelerator. In den folgenden Abschnitten werden die Berechtigungen für die Rolle beschrieben.

Berechtigungen von serviceverknüpften Rollen

Diese serviceverknüpfte Rolle ermöglicht es Global Accelerator, EC2 Elastic Network Interfaces und Sicherheitsgruppen zu verwalten und Fehler zu diagnostizieren.

Die serviceverknüpfte Rolle „AWSServiceRoleForGlobalAccelerator“ vertraut dem folgenden Service, um die Rolle zu übernehmen:

- `globalaccelerator.amazonaws.com`

Mit der Rollenberechtigungsrichtlinie kann Global Accelerator die folgenden Aktionen für die angegebenen Ressourcen ausführen, wie in der Richtlinie dargestellt:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
```

```
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeInstances",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeSubnets",
                "ec2:DescribeRegions",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DeleteSecurityGroup",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/AWSServiceName": "GlobalAccelerator"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSecurityGroup",
                "ec2:DescribeSecurityGroups"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "elasticloadbalancing:DescribeLoadBalancers",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": [
                "arn:aws:ec2:*:*:security-group/*",
                "arn:aws:ec2:*:*:network-interface/*"
            ]
        }
    ]
}
```

Sie müssen Berechtigungen konfigurieren, damit eine IAM-Entität (z. B. ein Benutzer, eine Gruppe oder eine Rolle) die mit dem Global Accelerator verknüpfte Rolle löschen kann. Weitere Informationen finden Sie unter Berechtigungen für serviceverknüpfte Rollen im IAM-Benutzerhandbuch.

Erstellen der serviceverknüpften Rolle für Global Accelerator

Sie erstellen die serviceverknüpfte Rolle für Global Accelerator nicht manuell. Wenn Sie das erste Mal eine Rolle erstellen, erstellt der Service die Rolle automatisch für Sie. Wenn Sie Ihre Global Accelerator -Ressourcen entfernen und die serviceverknüpfte Rolle löschen, erstellt der Service die Rolle automatisch wieder, wenn Sie eine neue Accelerator erstellen.

Bearbeiten der serviceverknüpften Rolle Global Accelerator

Global Accelerator erlaubt Ihnen nicht, die serviceverknüpfte Rolle AWSServiceRoleForGlobalAccelerator zu bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach der Erstellung einer serviceverknüpften Rolle durch den Service nicht bearbeitet werden. Sie können jedoch die Beschreibung einer Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Löschen der serviceverknüpften Rolle für Global Accelerator

Wenn Sie Global Accelerator nicht mehr benötigen, empfehlen wir, die serviceverknüpfte Rolle zu löschen. Auf diese Weise haben Sie keine ungenutzten Entitäten, die nicht aktiv überwacht oder verwaltet werden. Sie müssen jedoch die Global Accelerator-Ressourcen in Ihrem Konto bereinigen, bevor Sie die Rollen manuell löschen können.

Nachdem Sie die Beschleuniger deaktiviert und gelöscht haben, können Sie die serviceverknüpfte Rolle löschen. Weitere Informationen zum Löschen von Beschleunigern finden Sie unterErstellen oder Aktualisieren eines Standard-Beschleunigers.

> **Note**
>
> Wenn Sie Ihre Accelerators deaktiviert und gelöscht haben, aber Global Accelerator die Aktualisierung nicht abgeschlossen hat, schlägt das Löschen der serviceverknüpften Rolle möglicherweise fehl. Wenn das passiert, warten Sie einige Minuten, und wiederholen Sie die Schritte zum Löschen der serviceverknüpften Rolle.

So löschen Sie die serviceverknüpfte Rolle für manuell

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich der IAM Console Roles aus. Aktivieren Sie dann das Kontrollkästchen neben dem Rollennamen, den Sie löschen möchten, nicht den Namen oder die Zeile selbst.
3. Wählen Sie für Role actions oben auf der Seite Delete role aus.
4. Überprüfen Sie im Bestätigungsdialogfeld die letzten Service-Zugriffsdaten, die zeigen, wann jede der ausgewählten Rollen zuletzt auf den AWS-Service zugegriffen hat. Auf diese Weise können Sie leichter bestätigen, ob die Rolle derzeit aktiv ist. Wenn Sie fortfahren möchten, wählen Sie Yes, Delete aus, um die serviceverknüpfte Rolle zur Löschung zu übermitteln.
5. Sehen Sie sich die Benachrichtigungen in der IAM-Konsole an, um den Fortschritt der Löschung der serviceverknüpften Rolle zu überwachen. Da die Löschung der serviceverknüpften IAM-Rolle asynchron erfolgt, kann die Löschung nach dem Übermitteln der Rolle für die Löschung erfolgreich sein oder fehlschlagen. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Aktualisierungen der servicegebundenen Rolle Global Accelerator (eine verwaltete AWS Richtlinie)

Zeigen Sie Details zu Aktualisierungen der dienstverknüpften Rolle für an, seit dieser Dienst mit der Verfolgung dieser Änderungen begonnen hat. Wenn Sie automatische Warnungen über Änderungen an dieser Seite erhalten, abonnieren Sie den RSS-Feed im AWS Global AcceleratorDokumentverlaufangezeigten.

Änderung	Beschreibung	Datum
AWSServiceRoleForGlobalAccelerator— Aktualisierte Richtlinie	Global Accelerator hat eine neue Berechtigung hinzugefügt, um Global Accelerator bei der Fehlerdiagnose zu unterstützen. Global Accelerator verwendet `ec2:DescribeRegion`	18. Mai 2021

Änderung	Beschreibung	Datum
	s , um die AWS Region zu ermitteln, in der sich ein Kunde befindet, wodurch Global Accelerator bei der Fehlerbehebung unterstützt werden kann.	
Global Accelerator begann mit der Verfolgung von Änderungen	Global Accelerator begann mit der Verfolgung von Änderungen für seine verwalteten AWS Richtlinien.	18. Mai 2021

Unterstützte Regionen für serviceverknüpfte Rollen von Global Accelerator

Global Accelerator unterstützt die Verwendung von serviceverknüpften Rollen in AWS Regionen, in denen Global Accelerator unterstützt wird.

Eine Liste der AWS Regionen, in denen Global Accelerator und andere Services derzeit unterstützt werden, finden Sie unter derAWS Regionentabelle.

Übersicht über den Zugriff und die Authentifizierung

Wenn neu für Sie ist, lesen Sie zum Einstieg die folgenden Themen, um mit der Autorisierung und dem Zugriff in AWS zu beginnen.

Themen

- Was ist Authentifizierung?
- Was ist Zugriffskontrolle?
- Was sind Richtlinien?
- Erste Schritte mit IAM

Was ist Authentifizierung?

Bei der Authentifizierung melden Sie sich mit Ihren Anmeldeinformationen bei AWS an.

> **Note**
>
> Wenn Sie einen schnellen Einstieg wünschen, ignorieren Sie diesen Abschnitt. Lesen Sie zunächst die einführenden Informationen zuIdentity and Access Management für AWS Global AcceleratorInformationen finden Sie unter und dann unterErste Schritte mit IAM.

Als Prinzipal müssen Sieauthentifiziert(bei AWS angemeldet) verwenden Sie eine Entität (Stammbenutzer, IAM-Benutzer oder IAM-Rolle), um eine Anforderung an AWS zu senden. Ein IAM-Benutzer kann langfristige Anmeldeinformationen wie Benutzername und Passwort oder einen Satz von Zugriffsschlüsseln haben. Wenn Sie eine IAM-Rolle annehmen, erhalten Sie temporäre Sicherheitsanmeldeinformationen.

Um sich über die AWS Management Console als Benutzer authentifizieren zu lassen, müssen Sie sich mit Ihrem Benutzernamen und Passwort anmelden. Um sich über die AWS-CLI oder AWS-API zu authentifizieren, müssen Sie Ihren Zugriffsschlüssel und den geheimen Schlüssel oder die temporären Anmeldeinformationen angeben. AWS bietet SDKs und CLI-Tools, mit denen Sie Ihre Anfrage mit Ihren Anmeldeinformationen verschlüsselt signieren können. Wenn Sie keine AWS-Tools verwenden, müssen Sie die Anforderung selbst signieren. Unabhängig von der von Ihnen verwendeten Authentifizierungsmethode müssen Sie möglicherweise auch zusätzliche Sicherheitsinformationen angeben. AWS beispielsweise empfiehlt, dass Sie die Multi-Factor Authentication (MFA) zur Erhöhung der Sicherheit Ihres Kontos nutzen.

Als Prinzipal können Sie sich bei AWS mit den folgenden Entitys (Benutzern oder Rollen) anmelden:

Stammbenutzer des AWS-Kontos

Wenn Sie ein AWS-Konto erstellen, enthält es zunächst nur eine einzelne Anmeldeidentität, die über Vollzugriff auf sämtliche AWS-Services und -Ressourcen in dem Konto verfügt. Diese Identität wird als AWS-Konto-Stammbenutzer bezeichnet. Um auf den Stammbenutzer zuzugreifen, müssen Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, die zur Erstellung des Kontos verwendet wurden. Wir raten ausdrücklich davon ab, den Stammbenutzer für Alltagsaufgaben einschließlich administrativen Aufgaben zu verwenden. Bleiben Sie stattdessen bei dem bewährten -Verfahren, den Stammbenutzer nur zu verwenden, um Ihren ersten IAM-Benutzer zu erstellen. Anschließend legen Sie die Anmeldedaten für den Stammbenutzer an einem sicheren Ort ab und verwenden sie nur, um einige Konto- und Service-Verwaltungsaufgaben durchzuführen.

IAM-Benutzer

EinIAM-BenutzerEine Entität in Ihrem AWS Konto mit spezifischen Berechtigungen. unterstützt Global Accelerator-Signaturversion 4Ein Protokoll für die Authentifizierung eingehender API-Anfragen. Weitere Informationen zur Authentifizierung von Anforderungen finden Sie unter Signature Version 4-Signaturprozess in der allgemeinen AWS-Referenz.

IAM-Rolle

EinIAM-RolleEine IAM-Identität ist eine -Identität, die Sie in Ihrem Konto mit bestimmten Berechtigungen erstellen können. Eine IAM-Rolle ist einem IAM-Benutzer ähnlich, weil es sich um eine AWS-Identität mit Berechtigungsrichtlinien handelt, die festlegen, welche Aktionen die Identität in AWS ausführen kann und welche nicht. Eine Rolle ist jedoch nicht einer einzigen Person zugeordnet, sondern kann von allen Personen angenommen werden, die diese Rolle benötigen. Einer Rolle sind außerdem keine standardmäßigen, langfristigen Anmeldeinformationen (Passwörter oder Zugriffsschlüssel) zugeordnet. Wenn Sie eine Rolle annehmen, erhalten Sie stattdessen temporäre Anmeldeinformationen für Ihre Rollensitzung. IAM-Rollen mit temporären Anmeldeinformationen sind in folgenden Situationen hilfreich:

Zugriff für verbundene Benutzer

Statt einen IAM-Benutzer zu erstellen, können Sie bereits vorhandene Identitäten von AWS Directory Service, dem Benutzerverzeichnis Ihres Unternehmens oder von einem Web-Identitätsanbieter verwenden. Diese werden als verbundene Benutzer bezeichnet. AWS weist einem verbundenen Benutzer eine Rolle zu, wenn der Zugriff über einen Identitätsanbieter angefordert wird. Weitere Informationen zu verbundenen Benutzern finden Sie unter Verbundene Benutzer und Rollen im IAM Benutzerhandbuch.

Temporäre Benutzerberechtigungen

Ein IAM-Benutzer kann eine Rolle vorübergehend annehmen, um verschiedene Berechtigungen für eine bestimmte Aufgabe zu erlangen.

Kontenübergreifender Zugriff

Sie können eine IAM-Rolle verwenden, um einem vertrauenswürdigen Prinzipal in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen sind die primäre Möglichkeit, um kontoübergreifenden Zugriff zu gewähren. In einigen AWS-Services können Sie jedoch eine Richtlinie direkt an eine Ressource anfügen (anstatt eine Rolle als Proxy zu verwenden). Global Accelerator unterstützt keine ressourcenbasierten Richtlinien. Weitere Informationen darüber, ob Sie eine Rolle oder eine ressourcenbasierte Richtlinie

verwenden, um kontoübergreifenden Zugriff zu ermöglichen, finden Sie unter Steuern des Zugriffs auf Prinzipale in einem anderen Konto.

Zugriff auf AWS-Services

Eine Servicerolle ist eineIAM-RolleAktionen, die ein Service übernimmt, um Aktionen in Ihrem Namen auszuführen. Service-Rollen bieten nur Zugriff innerhalb Ihres Kontos und können nicht genutzt werden, um Zugriff auf Services in anderen Konten zu erteilen. Ein IAM-Administrator kann eine Servicerolle in IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM Benutzerhandbuch.

Anwendungen, die auf Amazon EC2 ausgeführt werden

Sie können eine IAM-Rolle nutzen, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2-Instance ausgeführt werden und AWS CLI- oder AWS-API-Anforderungen durchführen. Das ist empfehlenswerter als Zugriffsschlüssel innerhalb der EC2-Instance zu speichern. Erstellen Sie ein Instance-Profil, das an die Instance angefügt ist, um eine AWS-Rolle einer EC2-Instance zuzuweisen und die Rolle für sämtliche Anwendungen der Instance bereitzustellen. Ein Instance-Profil enthält die Rolle und ermöglicht, dass Programme, die in der EC2-Instance ausgeführt werden, temporäre Anmeldeinformationen erhalten. Weitere Informationen finden Sie unter Verwenden einer IAM-Rolle zum Erteilen von Berechtigungen für Anwendungen, die auf Amazon EC2-Instances ausgeführt werden im IAM Benutzerhandbuch.

Was ist Zugriffskontrolle?

Nach der Anmeldung (Authentifizierung) bei AWS wird Ihr Zugriff auf AWS-Ressourcen und -Operationen durch Richtlinien geregelt. Zugriffskontrolle wird auch Autorisierung genannt.

> **Note**
>
> Wenn Sie einen schnellen Einstieg wünschen, ignorieren Sie diese Seite. Lesen Sie zunächst die einführenden Informationen zuIdentity and Access Management für AWS Global AcceleratorInformationen finden Sie unter und dann unterErste Schritte mit IAM.

Während der Autorisierung verwendet AWS Werte aus demAnforderungs-KontextÜberprüfen Sie nach gültigen Richtlinien. Anschließend wird anhand der Richtlinien festgelegt, ob die Anforderung zugelassen oder abgelehnt werden soll. Die meisten Richtlinien werden in AWS als

JSON-Dokumente gespeichert und geben die Berechtigungen an, die für Prinzipale zugelassen und verweigert werden. Weitere Informationen über die Struktur und den Inhalt von JSON-Richtliniendokumenten finden Sie unter Was sind Richtlinien?.

Mit Richtlinien kann ein Administrator festlegen, welche Benutzer auf AWS Ressourcen zugreifen können und welche Aktionen sie für diese Ressourcen ausführen dürfen. Eine IAM-Entität (Benutzer oder Rolle) besitzt zunächst keine Berechtigungen. Mit anderen Worten: Benutzer können standardmäßig nichts tun, nicht einmal ihre eigenen Zugriffsschlüssel anzeigen. Um einem Benutzer die Berechtigung für eine Aktion zu erteilen, muss ein Administrator einem Benutzer eine Berechtigungsrichtlinie zuweisen. Alternativ können sie den Benutzer zu einer Gruppe hinzufügen, die über die beabsichtigten Berechtigungen verfügt. Wenn ein Administrator dann einer Gruppe Berechtigungen erteilt, erhalten alle Benutzer dieser Gruppe diese Berechtigungen.

Möglicherweise verfügen Sie über gültige Anmeldeinformationen zur Authentifizierung Ihrer Anfragen, aber wenn Ihnen kein Administrator Berechtigungen erteilt, können Sie keine AWS Global Accelerator Ressourcen erstellen oder darauf zugreifen. Beispielsweise müssen Sie über explizite Berechtigungen verfügen, um einen AWS Global Accelerator zu erstellen.

Als Administrator können Sie eine Richtlinie schreiben, um den Zugriff auf die folgenden Elemente zu steuern:

- Prinzipale— Steuern Sie, welche Person oder Anwendung die Anfrage stellt (diePrinzipal) darf.
- IAM-Identitäten— Legen Sie fest, auf welche IAM-Identitäten (Gruppen, Benutzer und Rollen) zugegriffen werden kann und wie.
- IAM-Richtlinien— Legen Sie fest, wer kundenseitig verwaltete Richtlinien erstellen, bearbeiten und löschen und wer alle verwalteten Richtlinien anfügen und entfernen darf.
- AWS-Ressourcen— Steuern Sie, wer über eine identitätsbasierte oder ressourcenbasierte Richtlinie Zugriff auf Ressourcen hat.
- AWS Konten— Legen Sie fest, ob eine Anfrage nur für Mitglieder eines bestimmten Kontos zulässig ist.

Zugriffssteuerung für -Prinzipale

Berechtigungsrichtlinien steuern, welche Aktionen Sie als Prinzipal ausführen dürfen. Ein Administrator muss der Identität (Benutzer, Gruppe oder Rolle), die Ihre Berechtigungen bereitstellt, eine identitätsbasierte Berechtigungsrichtlinie zuweisen. Berechtigungsrichtlinien erlauben oder verweigern den Zugriff auf AWS. Administratoren können auch eine Berechtigungsgrenze für eine

IAM-Entität (Benutzer oder Rolle) festlegen, um die maximalen Berechtigungen für diese Entität zu definieren. Berechtigungsgrenzen sind eine erweiterte IAM-Funktion. Weitere Informationen über Berechtigungsgrenzen finden Sie unter Berechtigungsgrenzen für IAM-Identitäten im IAM-Benutzerhandbuch.

Weitere Informationen und ein Beispiel dafür, wie der AWS Zugriff für Prinzipale gesteuert wird, finden Sie unterSteuern des Zugriffs auf PrinzipaleimIAM-Benutzerhandbuch.

Steuern des Zugriffs auf

Administratoren steuern, welche Aktionen Sie mit einer IAM-Identität (Benutzer, Gruppe oder Rolle) ausführen können, indem sie eine Richtlinie erstellen, die einschränkt, was mit einer Identität geschehen kann oder wer darauf zugreifen kann. Dann wird diese Richtlinie der Identität zugewiesen, die Ihre Berechtigungen bereitstellt.

Ein Administrator kann Ihnen beispielsweise erlauben, das Passwort für drei bestimmte Benutzer zurückzusetzen. Dazu weisen sie Ihrem IAM-Benutzer eine Richtlinie zu, die es Ihnen ermöglicht, das Passwort nur für sich selbst und Benutzer mit dem ARN der drei angegebenen Benutzer zurückzusetzen. Dies ermöglicht es Ihnen, das Passwort Ihrer Teammitglieder, aber nicht anderer IAM-Benutzer zurückzusetzen.

Weitere Informationen und ein Beispiel für die Verwendung einer Richtlinie zur Kontrolle des AWS Zugriffs auf Identitäten finden Sie unter.Steuern des Zugriffs aufimIAM-Benutzerhandbuch.

Steuern des Zugriffs auf Richtlinien

Administratoren können steuern, wer kundenseitig verwaltete Richtlinien erstellen, bearbeiten und löschen darf und wer alle verwalteten Richtlinien zuweisen und entfernen darf. Wenn Sie eine Richtlinie überprüfen, können Sie die Richtlinienübersicht anzeigen, die eine Zusammenfassung der Zugriffsebenen für jeden Service innerhalb dieser Richtlinie enthält. AWS kategorisiert jede Service-Aktion in eine von vierZugriffsebenenbasierend auf dem, was jede Aktion tut:`List`,`Read`,`Write`, oder`Permissions management`. Sie können diese Zugriffsebenen verwenden, um zu ermitteln, welche Aktionen in Ihre Richtlinien aufgenommen werden sollen. Weitere Informationen finden Sie unterZusammenfassungen auf Zugriffsebene innerhalb von RichtlinienübersichtenimIAM-Benutzerhandbuch.

> **Warning**
>
> Sie sollten beschränken`Permissions Management`-Berechtigungen auf Zugriffsebene in Ihrem Konto. Andernfalls können Ihre Konto-Mitglieder Richtlinien mit mehr Berechtigungen

für sich selbst erstellen, als sie haben sollten. Oder sie können separate Benutzer mit vollem Zugriff auf AWS erstellen.

Weitere Informationen und ein Beispiel dafür, wie der AWS Zugriff für Richtlinien gesteuert wird, finden Sie unterSteuern des Zugriffs auf Richtlinienim IAM-Benutzerhandbuch.

Steuern des Zugriffs auf -Ressourcen

Administratoren können den Zugriff auf Ressourcen mit einer identitätsbasierten oder ressourcenbasierten Richtlinie steuern. Bei einer identitätsbasierten Richtlinie fügen Sie die Richtlinie einer Identität hinzu und geben an, auf welche Ressourcen die Identität zugreifen darf. Bei einer ressourcenbasierten Richtlinie ordnen Sie eine Richtlinie der Ressource zu, die Sie steuern möchten. Sie geben in der Richtlinie an, welche Prinzipale auf die Ressource zugreifen dürfen.

Weitere Informationen finden Sie unterSteuern des Zugriffs auf Ressourcenim IAM-Benutzerhandbuch.

Ressourcenersteller verfügen nicht automatisch über Berechtigungen

Alle Ressourcen in einem Konto gehören diesem Konto, unabhängig davon, wer diese Ressourcen erstellt hat. Der Root-Benutzer des AWS Kontos ist der Kontoeigentümer und daherDie Berechtigung hat, eine -Aktion auf allen Ressourcen innerhalb des Kontos auszuführen.

> **Important**
>
> Wir raten ausdrücklich davon ab, den Stammbenutzer für Alltagsaufgaben einschließlich administrativen Aufgaben zu verwenden. Folgen Sie stattdessen derbewährte Methode, den Stammbenutzer nur zu verwenden, um Ihren ersten IAM-Benutzer zu erstellen. Anschließend legen Sie die Anmeldedaten für den Stammbenutzer an einem sicheren Ort ab und verwenden sie nur, um einige Konto- und Service-Verwaltungsaufgaben durchzuführen. Weitere Informationen zu den Aufgaben, die Sie nur als Stammbenutzer ausführen können, finden Sie unterAWS Aufgaben, die Root-Benutzer erfordern.

Entitys (Benutzer oder Rollen) innerhalb des AWS Kontos müssen Zugriff erhalten, um eine Ressource zu erstellen. Nur weil sie eine Ressource erstellen, bedeutet das nicht, dass sie automatisch vollen Zugriff auf diese Ressource haben. Für jede Aktion müssen Administratoren

explizit Berechtigungen erteilen. Darüber hinaus können Administratoren diese Berechtigungen jederzeit widerrufen, solange sie Zugriff auf die Verwaltung von Benutzer- und Rollenberechtigungen haben.

Steuern des Zugriffs auf Prinzipale in einem anderen Konto

Administratoren können AWS Ressourcenbasierte -Richtlinien, kontoübergreifende IAM-Rollen oder den AWS Organizations service verwenden, um Prinzipalen in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen.

Bei einigen AWS -Services können Administratoren kontenübergreifenden Zugriff auf Ihre Ressourcen gewähren. Dazu fügt ein Administrator der Ressource, die er freigeben möchte, direkt eine Richtlinie an, anstatt eine Rolle als Proxy zu verwenden. Wenn der Service diesen Richtlinientyp unterstützt, dann muss die Ressource, die der Administrator freigibt, auch ressourcenbasierte Richtlinien unterstützen. Im Gegensatz zu einer benutzerbasierten Richtlinie wird bei einer ressourcenbasierten Richtlinie festgelegt, wer auf die Ressource zugreifen kann (in Form einer Liste mit ID-Nummern für das AWS Konto). Ressourcenbasierte Richtlinien werden von Global Accelerator nicht unterstützt.

Kontenübergreifender Zugriff aufgrund einer ressourcenbasierten Richtlinie verfügt gegenüber einer Rolle über einige wichtige Vorteile. Bei einer Ressource, auf die über eine ressourcenbasierte Richtlinie zugegriffen wird, arbeitet der Prinzipal (Person oder Anwendung) weiterhin im vertrauenswürdigen Konto und muss seine Benutzerberechtigungen nicht für Rollenberechtigungen aufgeben. Der Prinzipal hat also gleichzeitig Zugriff auf Ressourcen im vertrauenswürdigen Konto und im Vertrauenskonto. Dies ist nützlich für Aufgaben wie das Kopieren von Informationen von einem Konto in ein anderes. Weitere Informationen zur Verwendung kontenübergreifender Rollen finden Sie unterGewähren von Zugriff für einen IAM-Benutzer auf ein anderes AWS Konto, das Sie besitzenimIAM-Benutzerhandbuch.

AWS Organizations bieten richtlinienbasierte Verwaltung für mehrere AWS Konten, die Ihnen gehören. Organizations Sie können Gruppen von Konten erstellen, die Kontoerstellung automatisieren und Richtlinien für diese Gruppen anwenden und verwalten. Organizations ermöglichen Ihnen die zentrale Verwaltung von Richtlinien über mehrere Konten hinweg, ohne dass benutzerdefinierte Skripte und manuelle Prozesse erforderlich sind. Mithilfe von AWS Organizations können Sie Service-Kontrollrichtlinien erstellen, die eine zentrale Steuerung der AWS S-Services für mehrere AWS-Konten ermöglichen. Weitere Informationen finden Sie unterWas ist AWS Organizations?imAWS Organizations Benutzerhandbuch.

Was sind Richtlinien?

Für die Zugriffsverwaltung in AWS erstellen Sie Richtlinien und fügen sie an die IAM-Identitäten oder AWS-Ressourcen an.

> **Note**
>
> Wenn Sie einen schnellen Einstieg wünschen, ignorieren Sie diese Seite. Lesen Sie zunächst die einführenden Informationen zuIdentity and Access Management für AWS Global AcceleratorInformationen finden Sie unter und dann unterErste Schritte mit IAM.

Eine Richtlinie ist ein Objekt in AWS, das, einer Person oder Ressource zugeordnet, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal, z. B. ein Benutzer, eine Anforderung stellt. Berechtigungen in den Richtlinien bestimmen, ob die Anforderung zugelassen oder gesperrt wird. Die meisten Richtlinien werden in AWS als JSON-Dokumente gespeichert.

IAM-Richtlinien definieren Berechtigungen für eine Aktion unabhängig von der Methode, die Sie zur Ausführung der Aktion verwenden. Wenn eine Richtlinie beispielsweise dieGetUserEin Benutzer mit dieser Richtlinie kann Benutzerinformationen über die AWS-Managementkonsole, die AWS-CLI oder die AWS-API abrufen. Wenn Sie einen IAM-Benutzer erstellen, können Sie ihn so einrichten, dass Konsolen- oder Programmzugriff erlaubt sind. Der IAM-Benutzer kann sich mit einem Benutzernamen und Passwort an der Konsole anmelden. Oder sie können Zugriffsschlüssel verwenden, um mit der CLI oder API zu arbeiten.

Die folgenden Richtlinientypen sind nach der Häufigkeit ihres Auftretens gelistet und können beeinflussen, ob eine Anforderung zugelassen wird. Weitere Informationen finden Sie unter .RichtlinientypenimIAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien

IAM-Identitäten (Benutzer, Gruppen, zu denen Benutzer gehören, und Rollen) verwaltete Richtlinien anfügen.

Ressourcenbasierte Richtlinien

Sie können Inline-Richtlinien an Ressourcen in einigen AWS -Services anhängen. Die häufigsten Beispiele für ressourcenbasierte Richtlinien sind Amazon S3 Bucket-Richtlinien und Vertrauensrichtlinien für IAM-Rollen. Ressourcenbasierte Richtlinien werden von Global Accelerator nicht unterstützt.

SCPs für Organizations

AWS Organizations Sie können eine Service Control Policy (SCP) verwenden, um eine Berechtigungsgrenze auf eine AWS-Organisation oder Organisationseinheit (OU) anzuwenden. Diese Berechtigungen gelten für alle Entitäten innerhalb der Mitgliedskonten.

Zugriffskontrolllisten (ACLs)

Mit ACLs steuern Sie, welche Prinzipale auf eine Ressource zugreifen dürfen. ACLs sind ähnlich wie ressourcenbasierten Richtlinien, obwohl sie der einzige Richtlinientyp sind, der die JSON-Richtliniendokumentstruktur nicht verwendet. Global Accelerator unterstützt keine ACLs.

Diese Richtlinienarten können als Berechtigungsrichtlinien oder Berechtigungsgrenzen kategorisiert werden.

Berechtigungsrichtlinien

Sie können einer Ressource in AWS Berechtigungsrichtlinien zuweisen, um die Berechtigungen für dieses Objekt zu definieren. Innerhalb eines einzigen Kontos wertet AWS alle Berechtigungsrichtlinien gemeinsam aus. Berechtigungsrichtlinien sind die häufigsten Richtlinien. Sie können die folgenden Richtlinientypen als Berechtigungsrichtlinien verwenden:

Identitätsbasierte Richtlinien

Wenn Sie eine verwaltete oder eingebundene Richtlinie einem IAM-Benutzer, einer Gruppe oder Rolle hinzufügen, definiert die Richtlinie die Berechtigungen für diese Entität.

Ressourcenbasierte Richtlinien

Wenn Sie einer Ressource ein JSON-Richtliniendokument zuweisen, definieren Sie die Berechtigungen für diese Ressource. Der Service muss ressourcenbasierte Richtlinien unterstützen.

Zugriffskontrolllisten (ACLs)

Wenn Sie einer Ressource eine Zugriffskontrollliste anfügen, definieren Sie eine Liste von Prinzipalen mit der Berechtigung, auf diese Ressource zuzugreifen. Die Ressource muss ACLs unterstützen.

Berechtigungsgrenzen

Mithilfe von Richtlinien können Sie die Berechtigungsgrenze für eine -Entität (Benutzer oder Rolle) definieren. Eine Berechtigungsgrenze bestimmt die maximalen Berechtigungen, die eine

Entity haben kann. Berechtigungsgrenzen sind eine erweiterte AWS Funktion. Wenn mehrere Berechtigungsgrenzen für eine Anforderung gelten, wertet AWS jede Berechtigungsgrenze separat aus. Sie können eine Berechtigungsgrenzen in den folgenden Situationen anwenden:

Organisationen

AWS Organizations Sie können eine Service Control Policy (SCP) verwenden, um eine Berechtigungsgrenze auf eine AWS-Organisation oder Organisationseinheit (OU) anzuwenden.

IAM-Benutzer oder -Rollen

Sie können eine verwaltete Richtlinie für die Berechtigungsgrenze eines Benutzers oder einer Rolle verwenden. Weitere Informationen finden Sie unterBerechtigungsgrenzen für IAM-EntitätenimIAM-Benutzerhandbuch.

Themen

- Identitätsbasierte Richtlinien
- Ressourcenbasierte Richtlinien
- Klassifizierungen auf Richtlinienzugriffsebene

Identitätsbasierte Richtlinien

Richtlinien können IAM-Identitäten zugewiesen werden. Sie können z. B. Folgendes tun:

Anfügen von Berechtigungsrichtlinien zu Benutzern oder Gruppen in Ihrem Konto

Wenn Sie einem Benutzer Berechtigungen zum Erstellen einer AWS Global Accelerator Ressource, z. B. eines Beschleunigers, erteilen möchten, können Sie einem Benutzer oder einer Gruppe, zu der der Benutzer gehört, eine Berechtigungsrichtlinie anhängen.

Einer Rolle eine Berechtigungsrichtlinie zuweisen (kontoübergreifende Berechtigungen erteilen)

Sie können einer IAM-Rolle eine identitätsbasierte Berechtigungsrichtlinie zuweisen, um kontoübergreifende Berechtigungen zu erteilen. Beispielsweise kann der Administrator in Konto A eine Rolle erstellen, um einem anderen AWS-Konto (z. B. Konto B) oder einem AWS-Service kontoübergreifende Berechtigungen zu erteilen. Dazu geht er folgendermaßen vor:

1. Konto Ein Administrator erstellt eine IAM-Rolle und fügt dieser eine Berechtigungsrichtlinie an, die Berechtigungen für Ressourcen in Konto A erteilt.

2. Der Administrator von Konto A weist der Rolle eine Vertrauensrichtlinie zu, die Konto B als den Prinzipal identifiziert, der die Rolle übernehmen kann.
3. Der Administrator von Konto B kann nun Berechtigungen zur Übernahme der Rolle an alle Benutzer in Konto B delegieren. Daraufhin können die Benutzer in Konto B auf Ressourcen von Konto A zugreifen. Der Prinzipal in der Vertrauensrichtlinie kann auch ein AWS-Service-Prinzipal sein. Somit können Sie auch einem AWS-Service die Berechtigungen zur Übernahme der Rolle erteilen.

Weitere Informationen zur Delegierung von Berechtigungen mithilfe von IAM finden Sie unterZugriffsverwaltungimIAM-Benutzerhandbuch.

Weitere Informationen zu Benutzern, Gruppen, Rollen und Berechtigungen finden Sie im Thema Identitäten (Benutzer, Gruppen und Rollen) im IAM-Benutzerhandbuch.

Im Folgenden finden Sie zwei Beispiele für Richtlinien, die Sie mit Global Accelerator verwenden können. Die erste Beispielrichtlinie gewährt einem Benutzer programmgesteuerten Zugriff auf alle Aktionen zum Auflisten und Beschreiben für Beschleuniger in Ihrem AWS Konto:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "globalaccelerator:List*",
                "globalaccelerator:Describe*"
            ],
            "Resource": "*"
        }
    ]
}
```

Im folgenden Beispiel wird programmgesteuerter Zugriff auf die`ListAcceleratorsverwenden`:

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

```
                "globalaccelerator:ListAccelerators",
            ],
            "Resource": "*"
        }
    ]
}
```

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Diese Richtlinien gestatten Ihnen zu steuern, welche Aktionen ein bestimmter Prinzipal mit dieser Ressource durchführen kann und unter welchen Bedingungen dies möglich ist. Die gebräuchlichste ressourcenbasierte Richtlinie ist für einen Amazon S3 Bucket. Ressourcenbasierte Richtlinien sind eingebundene Richtlinien, die nur in der Ressource vorhanden sind. Es gibt keine verwalteten ressourcenbasierten Richtlinien.

Das Gewähren von Berechtigungen für Mitglieder von anderen AWS Konten mithilfe einer ressourcenbasierten Richtlinie hat gegenüber einer IAM-Rolle einige Vorteile. Weitere Informationen finden Sie unter Wie sich IAM-Rollen von ressourcenbasierten Richtlinien unterscheiden im IAM-Benutzerhandbuch.

Klassifizierungen auf Richtlinienzugriffsebene

In der IAM-Konsole werden Aktionen nach folgenden Zugriffsebenenklassifizierungen gruppiert:

Liste

List Berechtigung zum Auflisten von Ressourcen innerhalb des Services, um zu bestimmen, ob ein Objekt vorhanden ist. Aktionen mit dieser Zugriffsebene können Objekte auflisten, aber nicht die Inhalte einer Ressource sehen. Die meisten Aktionen der Zugriffsebene Liste können nicht in einer bestimmten Ressource ausgeführt werden. Beim Erstellen einer Richtlinienanweisung mit diesen Aktionen müssen Sie All resources (Alle Ressourcen) angeben (`"*"`).

Lesen

Bietet die Berechtigung zum Lesen, jedoch nicht zum Bearbeiten der Inhalte und Attribute der Ressourcen innerhalb des Services. Beispielsweise sind die Amazon S3 Operationen`GetObject`und`GetBucketLocation`verfügen über dieLesen-Zugriffsebene.

Write

Stellt die Berechtigung zum Erstellen, Löschen oder Ändern von Ressourcen innerhalb des Services bereit. Beispielsweise sind die Amazon S3

OperationenCreateBucket,DeleteBucket, undPutObjectverfügen über dieWrite-Zugriffsebene.

Verwaltung von Berechtigungen

Stellt die Berechtigung zum Erteilen oder Ändern von Ressourcenberechtigungen im Service bereit. Beispielsweise verfügen die meisten Richtlinienaktionen für IAM und AWS Organizations über dieVerwaltung von Berechtigungen-Zugriffsebene.

> **Tip**
>
> Zur Verbesserung der Sicherheit Ihres AWS Kontos beschränken Sie Richtlinien mit demVerwaltung von BerechtigungenKlassifizierung auf Zugriffsebene.

Markieren

Bietet die Berechtigung zum Erstellen, Löschen oder Ändern von Tags, die einer Ressource innerhalb des Services zugeordnet sind. Zum Beispiel kann der Amazon EC2CreateTagsundDeleteTags-Operationen haben dieMarkieren-Zugriffsebene.

Erste Schritte mit IAM

AWS Identity and Access Management (IAM) ist ein AWS -Service, der es Ihnen ermöglicht, den Zugriff auf Services und Ressourcen sicher zu verwalten. IAM ist eine Funktion Ihres AWS Kontos, die ohne zusätzliche Gebühren verfügbar ist.

> **Note**
>
> Lesen Sie sich die einführenden Informationen unter durch, bevor Sie mit IAM beginnen.Identity and Access Management für AWS Global Accelerator.

Wenn Sie ein AWS-Konto erstellen, enthält es zunächst nur eine einzelne Anmeldeidentität, die über Vollzugriff auf sämtliche AWS-Services und -Ressourcen in dem Konto verfügt. Diese Identität wird als AWS-Konto-Stammbenutzer bezeichnet. Um auf den Stammbenutzer zuzugreifen, müssen Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, die zur Erstellung des Kontos verwendet wurden. Wir raten ausdrücklich davon ab, den Stammbenutzer für Alltagsaufgaben einschließlich administrativen Aufgaben zu verwenden. Bleiben Sie stattdessen bei dem bewährten -Verfahren, den

Stammbenutzer nur zu verwenden, um Ihren ersten IAM-Benutzer zu erstellen. Anschließend legen Sie die Anmeldedaten für den Stammbenutzer an einem sicheren Ort ab und verwenden sie nur, um einige Konto- und Service-Verwaltungsaufgaben durchzuführen.

Erstellen Sie Ihren IAM-Admin-Benutzer

So erstellen Sie einen Administratorbenutzer für sich selbst und fügen ihn einer Administratorengruppe hinzu (Konsole)

1. Melden Sie sich bei der IAM-Konsole als Kontoinhaber an, indem Sie Root user (Stammbenutzer) auswählen und die E-Mail-Adresse Ihres AWS-Kontos eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.

   > **Note**
   >
   > Wir empfehlen nachdrücklich, die bewährten Methoden mit dem**`Administrator`**IAM-Benutzer, der die Anmeldeinformationen des Stammbenutzers an einem sicheren Ort ablegt. Melden Sie sich als Stammbenutzer an, um einige Konto- und Service-Verwaltungsaufgaben durchzuführen.

2. Wählen Sie im Navigationsbereich Users und dann Add User aus.
3. Geben Sie unter Benutzername **`Administrator`** als Benutzernamen ein.
4. Markieren Sie das Kontrollkästchen neben AWS Management Console access (Zugriff auf AWS-Managementkonsole). Wählen Sie dann Custom password (Benutzerdefiniertes Passwort) aus und geben Sie danach Ihr neues Passwort in das Textfeld ein.
5. (Optional) Standardmäßig erfordert AWS, dass der neue Benutzer bei der ersten Anmeldung ein neues Passwort erstellt. Sie können das Kontrollkästchen neben User must create a new password at next sign-in (Benutzer muss bei der nächsten Anmeldung ein neues Passwort erstellen) deaktivieren, um dem neuen Benutzer zu ermöglichen, sein Kennwort nach der Anmeldung zurückzusetzen.
6. Klicken Sie aufWeiter: Berechtigungen
7. Wählen Sie unter Set permissions (Berechtigungen festlegen) die Option Add user to group (Benutzer der Gruppe hinzufügen) aus.
8. Wählen Sie Create group (Gruppe erstellen) aus.
9. Geben Sie im Dialogfeld Create group (Gruppe erstellen) unter Group name (Gruppenname) **`Administrators`** ein.

10. Klicken Sie aufFilterrichtlinienWählen Sie und dann aus.AWS verwaltet - Auftragsfunktion, um den Tabelleninhalt zu filtern.
11. Aktivieren Sie in der Richtlinienliste das Kontrollkästchen AdministratorAccess. Wählen Sie dann Create group aus.

> **Note**
>
> Sie müssen IAM-Benutzer- und Rollenzugriff auf Billing aktivieren, bevor Sie die `AdministratorAccess`-Berechtigungen für den Zugriff auf die AWS Billing and Cost Management-Konsole verwenden können. Befolgen Sie hierzu die Anweisungen in Schritt 1 des Tutorials zum Delegieren des Zugriffs auf die Abrechnungskonsole.

12. Kehren Sie zur Gruppenliste zurück und aktivieren Sie das Kontrollkästchen der neuen Gruppe. Möglicherweise müssen Sie Refresh auswählen, damit die Gruppe in der Liste angezeigt wird.
13. Klicken Sie aufWeiter: Tags.
14. (Optional) Fügen Sie dem Benutzer Metadaten hinzu, indem Sie Tags als Schlüssel-Wert-Paare anfügen. Weitere Informationen zur Verwendung von Tags in IAM finden Sie unter Tagging von IAM-Entitäten im IAM-Benutzerhandbuch.
15. Klicken Sie aufWeiter: PrüfenUm eine Liste der Gruppenmitgliedschaften anzuzeigen, die dem neuen Benutzer hinzugefügt werden soll. Wenn Sie bereit sind, fortzufahren, wählen Sie Create user (Benutzer erstellen) aus.

Mit diesen Schritten können Sie weitere Gruppen und Benutzer erstellen und Ihren Benutzern Zugriff auf Ihre AWS-Kontoressourcen gewähren. Weitere Informationen dazu, wie Sie die Berechtigungen eines Benutzers auf bestimmte AWS-Ressourcen mithilfe von Richtlinien beschränken, finden Sie unter Zugriffsverwaltung und Beispielrichtlinien.

Erstellen Sie delegierter Benutzer für Global Accelerator

Um mehrere Benutzer in Ihrem AWS Konto zu unterstützen, müssen Sie die Berechtigung delegieren, damit andere Personen nur die Aktionen ausführen können, die Sie zulassen möchten. Dazu erstellen Sie eine IAM-Gruppe mit den Berechtigungen, die diese Menschen benötigen, und fügen Sie dann IAM-Benutzer den erforderlichen Gruppen hinzu, sobald sie erstellt werden. Sie können diesen Prozess verwenden, um die Gruppen, Benutzer und Berechtigungen für Ihr gesamtes AWS Konto einzurichten. Diese Lösung eignet sich am besten für kleine und mittlere Organisationen, in denen ein AWS Administrator die Benutzer und Gruppen manuell verwalten kann. Für große Organisationen können SieBenutzerdefinierte IAM-Rollen,Verbund, oderSingle Sign-On.

Im folgenden Verfahren erstellen Sie drei Benutzer mit dem Namen**arnav**,**carlos**, und**martha**und fügen Sie eine Richtlinie an, die die Berechtigung zum Erstellen eines Beschleunigers mit dem Namen**my-example-accelerator**, aber nur innerhalb der nächsten 30 Tage. Verwenden Sie die hier aufgeführten Maßnahmen zum Hinzufügen von Benutzern mit unterschiedlichen Berechtigungen.

So erstellen Sie einen delegierten Benutzer für eine andere Person (Konsole):

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich Users und dann Add User aus.
3. Geben Sie unter Benutzername **arnav** als Benutzernamen ein.
4. Wählen Sie Add another user (Weiteren Benutzer hinzufügen) und geben Sie **carlos** als Namen des zweiten Benutzers ein. Wählen Sie Add another user (Weiteren Benutzer hinzufügen) und geben Sie **martha** als Namen des dritten Benutzers ein.
5. Aktivieren Sie das Kontrollkästchen nebenZugriff auf AWS Management ConsoleWählen Sie und dann aus.Autogenerated password.
6. Löschen Sie das Kontrollkästchen neben User must create a new password at next sign-in (Benutzer muss bei der nächsten Anmeldung ein neues Passwort erstellen), um dem neuen Benutzer zu ermöglichen, das Kennwort nach der Anmeldung zurückzusetzen.
7. Klicken Sie aufWeiter: Berechtigungen
8. Wählen Sie Vorhandene Richtlinien direkt zuordnen. Sie erstellen eine neue verwaltete Richtlinie für die Benutzer.
9. Klicken Sie auf Create Policy.

   Auf einer neuen Registerkarte oder in einem neuen Browserfenster wird der Assistent Richtlinie erstellen geöffnet.
10. Wählen Sie auf der Registerkarte Visual editor (Visueller Editor) die Option Choose a service (Wählen Sie einen Service) aus. Wählen Sie anschließend Global Accelerator aus. Sie können das Suchfeld oben verwenden, um die Ergebnisse in der Liste der Services einzuschränken.

    Die-Servicewird geschlossen, und derAktionenwird automatisch geöffnet.
11. Wählen Sie die Aktionen des globalen Beschleunigers aus, die Sie zulassen möchten. Geben Sie beispielsweise ein, um die Berechtigung zum Erstellen eines Beschleunigers zu erteilen,**globalaccelerator:CreateAccelerator**imFilteraktionen-Textfeld verwenden. Wenn die Liste der globalen Accelerator-Aktionen gefiltert ist, aktivieren Sie das Kontrollkästchen neben**globalaccelerator:CreateAccelerator**.

Die globalen Accelerator-Aktionen sind nach Zugriffsebenenklassifizierung gruppiert. So wird es für Sie einfacher, die von jeder Aktion bereitgestellte Zugriffsebene zu bestimmen. Weitere Informationen finden Sie unter Klassifizierungen auf Richtlinienzugriffsebene.

12. Wenn die Aktionen, die Sie in den vorherigen Schritten festgelegt haben, die Auswahl bestimmter Ressourcen nicht unterstützen, dann wirdAlle Ressourcenfür Sie ausgewählt ist. In diesem Fall können Sie diesen Abschnitt nicht bearbeiten.

    Wenn Sie eine oder mehrere Aktionen auswählen, die Berechtigungen auf Ressourcenebene unterstützen, listet der visuelle Editor diese Ressourcentypen im Abschnitt Ressourcen auf. Klicken Sie aufSie haben Aktionen ausgewählt, die die-Accelerator-Ressourcentyp, um einzustellen, ob Sie einen bestimmten Accelerator für Ihre Richtlinie eingeben möchten.

13. Wenn Sie die Aktion `globalaccelerator:CreateAccelerator` für alle Ressourcen erlauben möchten, wählen Sie All resources (Alle Ressourcen) aus.

    Wenn Sie eine Ressource angeben möchten, wählen Sie Add ARN (ARN hinzufügen) aus. Geben Sie die Region und die Konto-ID (oder Konto-ID) an (oder wählen SieAlle), und geben Sie dann**`my-example-accelerator`**für die Ressource. Wählen Sie dann Add (Hinzufügen) aus.

14. Wählen Sie Specify request conditions (optional) (Anforderungsbedingungen angeben (optional)) aus.

15. Klicken Sie aufHinzufügen einer BedingungErteilt die Berechtigung zum Erstellen eines Acceleratorsinnerhalb der nächsten 7 Tage. Angenommen, heute ist der 1. Januar 2019.

16. Wählen Sie für Condition Key (Bedingungsschlüssel) aws: CurrentTime aus. Dieser Bedingungsschlüssel prüft das Datum und die Uhrzeit, zu der der Benutzer die Anfrage erstellt. Er gibt „true“ zurück (und erlaubt die Aktion **`globalaccelerator:CreateAccelerator`** somit nur, wenn das Datum und die Uhrzeit innerhalb des angegebenen Bereichs liegen.)

17. FürQualifierbehalten Sie den Standardwert bei.

18. Um den Beginn des zulässigen Datums und Zeitraums festzulegen, wählen Sie für Operator DateGreaterThan aus. Geben Sie dann unter Wert **`2019-01-01T00:00:00Z`** ein.

19. Wählen Sie Hinzufügen aus, um Ihre Bedingung zu speichern.

20. Wählen Sie Eine weitere Bedingung hinzufügen aus, um das Enddatum anzugeben.

21. Gehen Sie analog vor, um das Ende des zulässigen Datums und Zeitbereichs anzugeben. Wählen Sie für Condition Key (Bedingungsschlüssel) aws: CurrentTime aus. Wählen Sie für Operator DateLessThan aus. Geben Sie unter Wert **`2019-01-06T23:59:59Z`** (ein Datum,

das sieben Tage nach dem ersten Datum liegt) ein. Wählen Sie dann Hinzufügen aus, um Ihre Bedingung zu speichern.

22. (Optional) Um das JSON-Richtliniendokument für die Richtlinie, die Sie erstellen, anzuzeigen, wählen Sie das KontrollkästchenJSON-Registerkarte. Sie können jederzeit zwischen den Registerkarten Visual editor (Visueller Editor) und JSON wechseln. Wenn Sie jedoch Änderungen vornehmen oderÜberprüfen der RichtlinieimVisual editor (Visueller Editor)kann IAM Ihre Richtlinie umstrukturiert, um sie für den visuellen Editor zu optimieren. Weitere Informationen finden Sie unterUmstrukturierung einer RichtlinieimIAM-Benutzerhandbuch.
23. Wählen Sie, wenn Sie fertig sind, Review policy (Richtlinie überprüfen) aus.
24. Klicken Sie auf derÜberprüfen der RichtlinieSeite, fürNameGeben Sie ein,**`globalaccelerator:CreateAcceleratorPolicy`**. Geben Sie für Beschreibung den Text **`Policy to grants permission to create an accelerator`** ein. Überprüfen Sie die Richtlinienzusammenfassung, um sicherzustellen, dass Sie die beabsichtigten Berechtigungen erteilt haben, und wählen Sie dann Create policy (Richtlinie erstellen) aus, um Ihre neue Richtlinie zu speichern.
25. Kehren Sie zur ursprünglichen Registerkarte oder zum ursprünglichen Fenster zurück und aktualisieren Sie die Liste der Richtlinien.
26. Geben Sie in das Suchfeld **`globalaccelerator:CreateAcceleratorPolicy`** ein. Aktivieren Sie das Kontrollkästchen neben der neuen Richtlinie. Klicken Sie dann auf Next Step.
27. Klicken Sie aufWeiter: PrüfenWählen Sie eine Vorschau Ihrer neuen Benutzer aus. Wenn Sie bereit sind, fortzufahren, wählen Sie Create users (Benutzer erstellen) aus.
28. Laden Sie die Passwörter für Ihre neuen Benutzer herunter oder kopieren sie und übermitteln Sie sie sicher an die Benutzer. Stellen Sie Ihren Benutzern separat eineLink zu Ihrer IAM-BenutzerkonsolenseiteWählen Sie die Benutzernamen aus, die Sie soeben erstellt haben.

Berechtigen Sie Benutzern, ihre Anmeldeinformationen selbst zu verwalten

Sie müssen über physischen Zugriff auf die Hardware verfügen, die als Host für das virtuelle MFA-Gerät des Benutzers dient, um MFA konfigurieren zu können. Beispielsweise können Sie MFA für einen Benutzer konfigurieren, der ein virtuelles MFA-Gerät verwendet, das auf einem Smartphone ausgeführt wird. In diesem Fall müssen Sie das Smartphone zur Verfügung haben, um den Assistenten zu beenden. Aus diesem Grund kann es sinnvoll sein, die Konfiguration und Verwaltung der virtuellen MFA-Geräte von den Benutzern selbst vornehmen zu lassen. In diesem Fall müssen Sie den Benutzern die Berechtigungen zur Ausführung der erforderlichen IAM-Aktionen erteilen.

So erstellen Sie eine Richtlinie, um die Selbstverwaltung von Anmeldeinformationen (Konsole) zu erlauben:

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich Policies (Richtlinien) und dann Create policy (Richtlinie erstellen) aus.
3. Wählen Sie die Registerkarte JSON aus und kopieren Sie den Text aus dem folgenden JSON-Richtliniendokument. Fügen Sie den folgenden Text in das JSON-Eingabefeld ein.

> **Important**
>
> Diese Beispielrichtlinie erlaubt es Benutzern nicht, ein Passwort beim Anmelden zurückzusetzen. Neue Benutzer und Benutzer mit einem abgelaufenen Passwort könnten dies versuchen. Sie können dies erlauben, indem Sie `iam:ChangePassword` und `iam:CreateLoginProfile` der Anweisung `BlockMostAccessUnlessSignedInWithMFA` hinzufügen. Allerdings wird dies von IAM von nicht empfohlen.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowAllUsersToListAccounts",
            "Effect": "Allow",
            "Action": [
                "iam:ListAccountAliases",
                "iam:ListUsers",
                "iam:ListVirtualMFADevices",
                "iam:GetAccountPasswordPolicy",
                "iam:GetAccountSummary"
            ],
            "Resource": "*"
        },
        {
            "Sid":
 "AllowIndividualUserToSeeAndManageOnlyTheirOwnAccountInformation",
            "Effect": "Allow",
            "Action": [
```

```
                "iam:ChangePassword",
                "iam:CreateAccessKey",
                "iam:CreateLoginProfile",
                "iam:DeleteAccessKey",
                "iam:DeleteLoginProfile",
                "iam:GetLoginProfile",
                "iam:ListAccessKeys",
                "iam:UpdateAccessKey",
                "iam:UpdateLoginProfile",
                "iam:ListSigningCertificates",
                "iam:DeleteSigningCertificate",
                "iam:UpdateSigningCertificate",
                "iam:UploadSigningCertificate",
                "iam:ListSSHPublicKeys",
                "iam:GetSSHPublicKey",
                "iam:DeleteSSHPublicKey",
                "iam:UpdateSSHPublicKey",
                "iam:UploadSSHPublicKey"
            ],
            "Resource": "arn:aws:iam::*:user/${aws:username}"
        },
        {
            "Sid": "AllowIndividualUserToViewAndManageTheirOwnMFA",
            "Effect": "Allow",
            "Action": [
                "iam:CreateVirtualMFADevice",
                "iam:DeleteVirtualMFADevice",
                "iam:EnableMFADevice",
                "iam:ListMFADevices",
                "iam:ResyncMFADevice"
            ],
            "Resource": [
                "arn:aws:iam::*:mfa/${aws:username}",
                "arn:aws:iam::*:user/${aws:username}"
            ]
        },
        {
            "Sid":
 "AllowIndividualUserToDeactivateOnlyTheirOwnMFAOnlyWhenUsingMFA",
            "Effect": "Allow",
            "Action": [
                "iam:DeactivateMFADevice"
            ],
            "Resource": [
```

```
                "arn:aws:iam::*:mfa/${aws:username}",
                "arn:aws:iam::*:user/${aws:username}"
            ],
            "Condition": {
                "Bool": {
                    "aws:MultiFactorAuthPresent": "true"
                }
            }
        },
        {
            "Sid": "BlockMostAccessUnlessSignedInWithMFA",
            "Effect": "Deny",
            "NotAction": [
                "iam:CreateVirtualMFADevice",
                "iam:DeleteVirtualMFADevice",
                "iam:ListVirtualMFADevices",
                "iam:EnableMFADevice",
                "iam:ResyncMFADevice",
                "iam:ListAccountAliases",
                "iam:ListUsers",
                "iam:ListSSHPublicKeys",
                "iam:ListAccessKeys",
                "iam:ListServiceSpecificCredentials",
                "iam:ListMFADevices",
                "iam:GetAccountSummary",
                "sts:GetSessionToken"
            ],
            "Resource": "*",
            "Condition": {
                "BoolIfExists": {
                    "aws:MultiFactorAuthPresent": "false"
                }
            }
        }
    ]
}
```

Was macht diese Richtlinie?

- Die`AllowAllUsersToListAccounts`Die -Anweisung ermöglicht dem Benutzer, grundlegende Informationen zum Konto und dessen Benutzern in der IAM-Konsole anzuzeigen. Diese Berechtigungen müssen in ihrer eigenen Anweisung vorliegen, da sie keine

Ressourcen-ARN unterstützen oder eine bestimmte Ressourcen-ARN angeben müssen und stattdessen `"Resource" : "*"` angeben.

- Die`AllowIndividualUserToSeeAndManageOnlyTheirOwnAccountInformation`-Anweisung ermöglicht dem Benutzer, seine eigenen Informationen zu Benutzer, Passwort, Zugriffsschlüsseln, Signaturzertifikaten, öffentlichen SSH-Schlüsseln und MFA in der IAM-Konsole zu verwalten. Zudem können sich Benutzer zum ersten Mal anmelden, wenn ein Administrator sie auffordert, ein erstmaliges Passwort festzulegen. Der Ressourcen-ARN begrenzt die Nutzung dieser Berechtigungen auf die eigene IAM-Benutzerentität des Benutzers.
- Die `AllowIndividualUserToViewAndManageTheirOwnMFA`-Anweisung ermöglicht dem Benutzer, sein eigenes MFA-Gerät anzuzeigen oder zu verwalten. Beachten Sie, dass die Ressourcen-ARNs in dieser Anweisung nur Zugriff auf ein MFA-Gerät oder einen Benutzer gestatten, das bzw. der exakt denselben Namen wie der aktuell angemeldete Benutzer hat. Benutzer können nur ihr eigenes MFA-Gerät erstellen oder ändern.
- Die `AllowIndividualUserToDeactivateOnlyTheirOwnMFAOnlyWhenUsingMFA`-Anweisung ermöglicht dem Benutzer nur, sein eigenes MFA-Gerät zu deaktivieren. Dies jedoch nur, wenn der Benutzer sich über die MFA angemeldet hat. Dadurch wird verhindert, dass andere, die nur über die Zugriffsschlüssel (und nicht über das MFA-Gerät) verfügen, das MFA-Gerät deaktivieren und das Konto aufrufen.
- Die`BlockMostAccessUnlessSignedInWithMFA`-Anweisung verwendet eine Kombination aus`"Deny"`und`"NotAction"`, um den Zugriff auf alle bis auf einige Aktionen in IAM und anderen AWS -Services zu verweigernifder Benutzer ist nicht bei MFA angemeldet. Weitere Informationen zur Logik für diese Anweisung finden Sie unterNotAction mit DenyimIAM-Benutzerhandbuch. Wenn der Benutzer mit MFA angemeldet ist, schlägt der `"Condition"`-Test fehl. Die endgültige "deny"-Anweisung hat keine Auswirkung und andere Richtlinien oder Anweisungen für den Benutzer bestimmen die Berechtigungen des Benutzers. Diese Anweisung stellt sicher, dass ein nicht mit MFA angemeldeter Benutzer nur die aufgeführten Aktionen durchführen kann, und zwar auch nur dann, wenn eine andere Anweisung oder Richtlinie den Zugriff auf diese Aktionen erlaubt.

  Die `...IfExists`-Version des `Bool` -Operators stellt sicher, dass bei fehlendem `aws:MultiFactorAuthPresent`-Schlüssel die Bedingung den Wert "True" zurückgibt. Dies bedeutet, dass einem Benutzer, der mit langfristigen Anmeldeinformationen auf eine API zugreift, wie z. B. einem Zugriffsschlüssel, der Zugriff auf die Nicht-IAM-API-Operationen verweigert wird.

4. Wählen Sie, wenn Sie fertig sind, Review policy (Richtlinie überprüfen) aus.

5. Geben Sie auf der Seite Review (Prüfen) als Richtliniennamen **`Force_MFA`** ein. Geben Sie für die Richtlinienbeschreibung**`This policy allows users to manage their own passwords and MFA devices but nothing else unless they authenticate with MFA.`**Überprüfen der RichtlinieÜbersichtWählen Sie dann die von Ihrer Richtlinie gewährten Berechtigungen aus, und wählen SieRichtlinie erstellenverwenden, um Ihre Eingaben zu speichern.

   Die neue Richtlinie wird in der Liste der verwalteten Richtlinien angezeigt und ist bereit.

So fügen Sie die Richtlinie an einen Benutzer an (Konsole):

1. Klicken Sie im Navigationsbereich auf Users.
2. Wählen Sie den Namen des Benutzers (nicht das Kontrollkästchen) aus, den Sie bearbeiten möchten.
3. Wählen Sie auf der Registerkarte Permissions die Option Add permissions.
4. Wählen Sie Vorhandene Richtlinien direkt zuordnen.
5. Geben Sie in das Suchfeld **`Force`** ein und aktivieren Sie dann in der Liste das Kontrollkästchen neben Force_MFA. Klicken Sie dann auf Next (Weiter): Prüfen.
6. Prüfen Sie die Änderungen und wählen Sie Add permissions (Berechtigungen hinzufügen) aus.

Aktivieren von MFA für Ihren IAM-Benutzer

Aus Sicherheitsgründen empfehlen wir, Ihre Global Accelerator-Ressourcen durch Multi-Factor Authentication (MFA) zu schützen. MFA bietet zusätzliche Sicherheit, da Benutzer zusätzlich zu ihren regulären Anmeldeinformationen eine eindeutige Authentifizierung von einem von AWS unterstützten MFA Gerät bereitstellen müssen. Das sicherste AWS MFA Gerät ist der U2F-Sicherheitsschlüssel. Wenn Ihr Unternehmen bereits über U2F-Geräte verfügt, empfehlen wir, dass Sie diese Geräte für AWS aktivieren. Andernfalls müssen Sie ein Gerät für jeden Ihrer Benutzer kaufen und warten, bis die Hardware eintrifft. Weitere Informationen finden Sie unterAktivieren eines U2F-SicherheitsschlüsselsimIAM-Benutzerhandbuch.

Wenn Sie noch kein U2F-Gerät haben, können Sie schnell und kostengünstig die ersten Schritte durchführen, indem Sie ein virtuelles MFA-Gerät aktivieren. Dies erfordert die Installation einer Softwareanwendung auf einem vorhandenen Smartphone oder einem anderen Mobilgerät.
Die Vorrichtung erzeugt einen sechsstelligen numerischen Code basierend auf einem zeitsynchronisierten Einmalpasswortalgorithmus. Wenn sich der Benutzer bei AWS anmeldet, wird

er aufgefordert, auf dem Gerät einen Code einzugeben. Jedes virtuelle MFA-Gerät, das einem Benutzer zugeordnet ist, muss eindeutig sein. Ein Benutzer kann zur Authentifizierung keinen Code auf dem virtuellen MFA-Gerät eines anderen Benutzers eingeben. Eine Liste einiger unterstützter Anwendungen, die Sie als virtuelle MFA-Geräte verwenden können, finden Sie unter Multifaktor-Authentifizierung.

> **Note**
>
> Sie müssen über physischen Zugriff auf das mobile Gerät verfügen, das als Host für das virtuelle MFA Gerät des Benutzers dient, um MFA für einen IAM-Benutzer konfigurieren zu können.

So aktivieren Sie ein virtuelles MFA Gerät für einen IAM-Benutzer (Konsole)

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Klicken Sie im Navigationsbereich auf Users.
3. Wählen Sie in der Liste User Name (Benutzername) den Namen des gewünschten MFA-Benutzers aus.
4. Wechseln Sie zur Registerkarte Security credentials (Sicherheitsanmeldeinformationen). Wählen Sie neben Assigned MFA device (Zugeordnetes MFA-Gerät) die Option Manage (Verwalten).
5. Wählen Sie im Assistenten Manage MFA Device (MFA-Gerät verwalten) die Option Virtual MFA device (Virtuelles MFA-Gerät) und dann Continue (Weiter) aus.

   IAM generiert Konfigurationsinformationen für das virtuelle MFA Gerät und zeigt diese einschließlich eines QR-Codes an. Dieser Code ist eine grafische Darstellung des "geheimen Konfigurationsschlüssels", der für die manuelle Eingabe auf Geräte zur Verfügung steht, die keine QR-Codes unterstützen.
6. Öffnen Sie Ihre virtuelle MFA-App.

   Eine Liste der Anwendungen, die Sie zum Hosten von virtuellen MFA-Geräten verwenden können, finden Sie unter Multi-Factor Authentication. Wenn die virtuelle MFA-App mehrere Konten (mehrere virtuelle MFA-Geräte) unterstützt, wählen Sie die Option zum Erstellen eines neuen Kontos (eines neues virtuellen MFA-Geräts) aus.
7. Stellen Sie fest, ob die MFA-App QR-Codes unterstützt, und führen Sie dann einen der folgenden Schritte aus:

- Wählen Sie im Assistenten Show QR code (QR-Code anzeigen) und verwenden Sie dann die App, um den QR-Code zu scannen. Sie können beispielsweise das Kamerasymbol oder eine Anwendung wie z. B. Scan Code (Code scannen) auswählen und dann mit der Kamera des Geräts den Code scannen.
- Wählen Sie im Assistenten Manage MFA Device (MFA-Gerät verwalten) Show secret key (Geheimschlüssel anzeigen) aus und geben Sie dann den Geheimschlüssel in Ihrer MFA-Anwendung ein.

Wenn Sie fertig sind, beginnt das virtuelle MFA-Gerät, einmalige Passwörter zu generieren.

8. Geben Sie im Assistenten Manage MFA Device (MFA-Gerät verwalten) im Feld MFA Code 1 (MFA-Code 1) das am virtuellen MFA-Gerät angezeigte einmalige Passwort ein. Warten Sie bis zu 30 Sekunden, bis das Gerät ein neues einmaliges Passwort generiert. Geben Sie dann das zweite einmalige Passwort in das Feld MFA Code 2 (MFA-Code 2) ein. Klicken Sie auf Assign MFA (MFA zuordnen).

> **Important**
>
> Senden Sie die Anforderung direkt nach der Erzeugung der Codes. Wenn Sie die Codes generieren und zu lange mit der Anforderung warten, wird das MFA-Gerät erfolgreich mit dem Benutzer verknüpft, aber das Gerät ist nicht synchronisiert. Dies liegt daran, weil die zeitlich begrenzten einmaligen Passwörter (TOTP) nach einer kurzen Zeit ungültig werden. In diesem Fall können Sie das Gerät neu synchronisieren. Weitere Informationen finden Sie unterResynchronisieren von virtuellen und physischen MFA-GerätenimIAM-Benutzerhandbuch.

Das virtuelle MFA Gerät ist jetzt für die Verwendung mit AWS bereit.

Sichere VPC Verbindungen in AWS Global Accelerator

Wenn Sie einen internen Application Load Balancer oder einen Amazon EC2 Instance-Endpunkt in AWS Global Accelerator hinzufügen, können Sie den Internet-Datenverkehr direkt zum und vom Endpunkt in Virtual Private Clouds (VPCs) übertragen, indem Sie ihn in einem privaten Subnetz ausrichten. Die VPC, die den Load Balancer oder EC2-Instance enthält, muss über einenInternet-Gatewayangehängt, um anzuzeigen, dass die VPC Internetverkehr akzeptiert. Sie benötigen jedoch

keine öffentlichen IP-Adressen auf dem Load Balancer oder der EC2-Instanz. Sie benötigen auch keine zugeordnete Internet-Gateway-Route für das Subnetz.

Dies unterscheidet sich von dem typischen Internet-Gateway-Anwendungsfall, in dem sowohl öffentliche IP-Adressen als auch Internet-Gateway-Routen erforderlich sind, damit Internetverkehr zu Instanzen oder Lastausgleichsprogrammen in einer VPC fließen kann. Selbst wenn die elastischen Netzwerkschnittstellen Ihrer Ziele in einem öffentlichen Subnetz (d. h. einem Subnetz mit einer Internet-Gateway-Route) vorhanden sind, überschreibt Global Accelerator bei Verwendung von Global Accelerator die typische Internetroute und alle logischen Verbindungen, die über die globale Der Accelerator kehrt auch über Global Accelerator zurück und nicht über das Internet-Gateway.

> **Note**
>
> Die Verwendung öffentlicher IP-Adressen und die Verwendung eines öffentlichen Subnetzes für Ihre Amazon EC2 Instances ist nicht typisch, obwohl es möglich ist, Ihre Konfiguration mit ihnen einzurichten. Sicherheitsgruppen gelten für jeden Datenverkehr, der in Ihre Instances eintrifft, einschließlich Datenverkehr von Global Accelerator und jeder öffentlichen oder Elastic IP-Adresse, die Ihrer Instance ENI zugewiesen ist. Verwenden Sie private Subnetze, um sicherzustellen, dass Datenverkehr nur von Global Accelerator bereitgestellt wird.

Beachten Sie diese Informationen, wenn Sie Netzwerkumkreisprobleme berücksichtigen und IAM-Berechtigungen im Zusammenhang mit der Internetzugriffsverwaltung konfigurieren. Weitere Informationen über die Kontrolle des Internetzugriffs auf Ihre VPC finden Sie in diesemBeispiel für Service-Kontrollrichtlinie.

Protokollieren und überwachen in AWS Global Accelerator

Die Überwachung ist ein wichtiger Teil der Aufrechterhaltung von Verfügbarkeit und Leistung von Global Accelerator und Ihren AWS Lösungen. Sie sollten von allen Teilen Ihrer AWS-Lösung Überwachungsdaten sammeln, damit Sie Ausfälle, die sich über mehrere Punkte erstrecken, leichter debuggen können. AWS stellt mehrere Tools für die Überwachung Ihrer Global Accelerator-Ressourcen und zur Reaktion auf potenzielle Vorfälle bereit:

AWS Global Accelerator -Flow-Protokolle

Serverflussprotokolle bieten detaillierte Aufzeichnungen über den Datenverkehr, der durch einen Beschleuniger zu einem Endpunkt fließt. Server-Flow-Protokolle sind für viele

Anwendungen nützlich. Beispielsweise können Flussprotokoll-Informationen bei Sicherheits- und Zugriffsprüfungen nützlich sein. Weitere Informationen finden Sie unter Flow-Protokolle in AWS Global Accelerator.

Amazon CloudWatch Metriken und Alarme

Mit CloudWatch können Sie Ihre AWS-Ressourcen und die Anwendungen, die Sie in AWS ausführen, in Echtzeit überwachen. CloudWatch erfasst und verfolgt Metriken, bei denen es sich um Variablen handelt, die Sie im Laufe der Zeit messen. Sie können Alarme erstellen, die bestimmte -Metriken überwachen, und dann Benachrichtigungen senden oder automatisch Änderungen an den Ressourcen vornehmen, die Sie überwachen, wenn die -Metrik einen bestimmten Schwellenwert für einen bestimmten Zeitraum überschreitet. Weitere Informationen finden Sie unter Verwenden von Amazon CloudWatch mit AWS Global Accelerator.

AWS CloudTrail-Protokolle

CloudTrail bietet eine Aufzeichnung der von einem Benutzer, einer Rolle oder einem AWS -Service in Global Accelerator durchgeführten Aktionen. CloudTrail erfasst alle API-Aufrufe für Global Accelerator als Ereignisse, einschließlich Aufrufen von der Global Accelerator-Konsole und von Code-Aufrufen an die Global Accelerator API. Weitere Informationen finden Sie unter Verwenden von AWS CloudTrail zum Protokollieren von API-Aufrufen von AWS Global Accelerator.

Compliance-Validierung für AWS Global Accelerator

Externe Prüfer bewerten im Rahmen verschiedener AWS Compliance-Programme die Sicherheit und Compliance von AWS Global Accelerator. Zu diesen Programmen gehören SOC, PCI, HIPAA, DSGVO, ISO und ENS High.

Eine Liste der AWS -Services, einschließlich Global Accelerator, finden Sie unter, die in bestimmten Compliance-Programmen enthalten sind, unter.AWS -Services im Rahmen des Compliance-Programms. Allgemeine Informationen finden Sie unter AWS-Compliance-Programme.

Die Prüfberichte von externen Prüfern lassen sich mit AWS Artifact herunterladen. Weitere Informationen finden Sie unterHerunterladen von Berichten in AWS Artifact.

Ihre Compliance-Verantwortung bei Verwendung von Global Accelerator hängt von der Vertraulichkeit der Daten, den Compliance-Zielen des Unternehmens und den geltenden Gesetzen und Vorschriften ab. AWS stellt die folgenden Ressourcen bereit, um Sie bei der Compliance zu unterstützen:

- Kurzanleitungen für Sicherheit und Compliance – In diesen Bereitstellungsleitfäden finden Sie wichtige Überlegungen zur Architektur sowie die einzelnen Schritte zur Bereitstellung von sicherheits- und Compliance-orientierten Basisumgebungen in AWS.
- Whitepaper zur Erstellung einer Architektur mit HIPAA-konformer Sicherheit und Compliance – Dieses Whitepaper beschreibt, wie Unternehmen mithilfe von AWS HIPAA-konforme Anwendungen erstellen.
- AWS-Compliance-Ressourcen – Diese Arbeitsbücher und Leitfäden könnten für Ihre Branche und Ihren Standort relevant sein.
- Auswertung von Ressourcen mit Regeln im AWS Config-Entwicklerhandbuch – Der AWS Config-Service bewertet, wie gut Ihre Ressourcenkonfigurationen mit internen Praktiken, Branchenrichtlinien und Vorschriften übereinstimmen.
- AWS-Sicherheits-Hub: Dieser AWS-Service liefert einen umfassenden Überblick über den Sicherheitsstatus in AWS. So können Sie die Compliance mit den Sicherheitsstandards in der Branche und den bewährten Methoden abgleichen.

Ausfallsicherheit in AWS Global Accelerator

Im Zentrum der globalen AWS-Infrastruktur stehen die AWS-Regionen und -Availability Zones (Verfügbarkeitszonen, AZs). AWS-Regionen stellen mehrere physisch getrennte und isolierte Availability Zones bereit, die über hoch redundante Netzwerke mit niedriger Latenz und hohen Durchsätzen verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Availability Zones ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser hoch verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen über AWS-Regionen und -Availability Zones finden Sie unter Globale AWS-Infrastruktur.

Neben der Unterstützung der globalen AWS Infrastruktur bietet Global Accelerator die folgenden Funktionen, die zur Unterstützung der Datenausfallsicherheit beitragen:

- Eine Netzwerkzone bedient die statischen IP-Adressen für den Accelerator aus einem eindeutigen IP-Subnetz. Ähnlich wie bei einer AWS Availability Zone ist eine Netzwerkzone eine isolierte Einheit mit eigener physischer Infrastruktur. Wenn Sie einen Beschleuniger konfigurieren, weist Global Accelerator ihm zwei IPv4-Adressen zu. Wenn eine IP-Adresse aus einer Netzwerkzone

aufgrund der Blockierung von IP-Adressen durch bestimmte Clientnetzwerke oder aufgrund von Netzwerkunterbrechungen nicht verfügbar wird, können Clientanwendungen die fehlerfreie statische IP-Adresse aus der anderen isolierten Netzwerkzone erneut versuchen.

- Global Accelerator überwacht kontinuierlich den Zustand aller Endpunkte. Wenn festgestellt wird, dass ein aktiver Endpunkt fehlerhaft ist, beginnt Global Accelerator sofort den Datenverkehr an einen anderen verfügbaren Endpunkt zu leiten. Auf diese Weise können Sie eine Architektur mit hoher Verfügbarkeit für Ihre Anwendungen in AWS erstellen.

Sicherheit der Infrastruktur in AWS Global Accelerator

Als verwalteter Service ist AWS Global Accelerator durch die globalen Verfahren zur Gewährleistung der Netzwerksicherheit von AWS geschützt, die im AbschnittAmazon Web Services: Übersicht über Sicherheitsprozesse-Whitepaper.

Sie verwenden von AWS veröffentlichte API-Aufrufe, um über das Netzwerk auf Global Accelerator zuzugreifen. Clients müssen Transport Layer Security (TLS) 1.0 oder höher unterstützen. Wir empfehlen TLS 1.2 oder höher. Clients müssen außerdem Cipher Suites mit PFS (Perfect Forward Secrecy) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman) unterstützen. Die meisten modernen Systemen wie Java 7 und höher unterstützen diese Modi. Außerdem müssen Anforderungen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der einem IAM-Prinzipal zugeordnet ist. Alternativ können Sie mit AWS Security Token Service (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

Kontingente für AWS Global Accelerator

Ihr AWS Konto verfügt über spezifische Kontingente, die auch als Begrenzungen bezeichnet werden und sich auf beziehen.

Die Service Quotas Konsole bietet Informationen zu Global Accelerator-Kontingenten. Neben der Anzeige der Standardkontingente können Sie die Servicekontingentkonsole verwenden, umAnforderungskontingent erhöhtfür anpassbare Kontingente. Beachten Sie, dass Sie sich in den USA Ost (Nord-Virginia) befinden müssen, wenn Sie Kontingenterhöhungen für Global Accelerator anfordern.

Themen

- Allgemeine Kontingente
- Kontingente für Endpunkte pro Endpunktgruppe
- Zugehörige Kontingente

Allgemeine Kontingente

Im Folgenden werden allgemeine Kontingente für Global Accelerator aufgeführt.

Entity	Quota
Acceleratoren pro AWS Konto	20 Sie haben folgende MöglichkeitenBeantragen einer Kontingenterhöhung.
Zuhörer pro Accelerator	10 Sie haben folgende MöglichkeitenBeantragen einer Kontingenterhöhung.
Portbereiche pro Listener	10
Port-Überschreibungen pro Endpunktgruppe	10

Entity	Quota
	Sie haben folgende MöglichkeitenBeantragen einer Kontingenterhöhung.

Kontingente für Endpunkte pro Endpunktgruppe

Im Folgenden finden Sie globale Accelerator-Kontingente, die für die Anzahl der Endpunkte in Endpunktgruppen gelten.

Entity	Beschreibung	Quota
Endpunktgruppen mit mehr als einem Endpunkttyp	Anzahl der Endpunkte in einer Endpunktgruppe, die mehr als einen Endpunkttyp enthält.	10
Endpunktgruppen mit nur Application Load Balancern	Anzahl der Application Load Balancers in einer Endpunktgruppe, die nur Application Load Balancer Endpunkte enthält.	10
Endpunktgruppen mit nur Netzwerklastenausg leichsprogrammen	Anzahl der Netzwerklastenausg leichsprogramme in einer Endpunktg ruppe, die nur Network Load Balancer Endpunkte enthält.	10
Endpunktgruppen mit nur Amazon EC2 Instances	Anzahl EC2-Instances in einer Endpunktgruppe, die nur EC2-Instance-Endpunkte enthält.	10 Sie haben folgende MöglichkeitenBeantragen einer Kontingenterhöhung.
Endpunktgruppen mit nur Elastic IP-Adressen	Anzahl der Elastic IP-Adressen in einer Endpunktgruppe, die nur Elastic IP-Adressenendpunkte enthält.	10 Sie haben folgende MöglichkeitenBeantragen

Entity	Beschreibung	Quota
		einer Kontingenterhöhung .
Endpunktgruppen mit nur Amazon Virtual Private Cloud -Subnetzen	Anzahl der Amazon VPC -Subnetze in einer Endpunktgruppe, die nur Subnetz-Endpunkte enthält.	10 Sie haben folgende MöglichkeitenBeantragen einer Kontingenterhöhung .

Zugehörige Kontingente

Neben Kontingenten in Global Accelerator gibt es Kontingente, die für die Ressourcen gelten, die Sie als Endpunkte für einen Accelerator verwenden. Weitere Informationen finden Sie unter:

- Kontingente für Elastic IP-AdressenimAmazon EC2 Benutzerhandbuch.
- Amazon EC2 -ServicekontingenteimAmazon EC2 Benutzerhandbuch.
- Kontingente für Ihre Netzwerk-Load BalancerimBenutzerhandbuch für Network Load Balancer.
- Kontingente für Application Load BalancerimBenutzerhandbuch für Application Load Balancer.
- Amazon VPC-KontingenteimBenutzerhandbuch für Amazon VPC.

AWS Global Accelerator

Die hier aufgelisteten Informationen und Ressourcen können Sie dabei unterstützen, mehr über Global Accelerator zu erfahren.

Themen

- AWS Global Accelerator Dokumentation
- Supportanfragen
- Tipps aus dem Amazon Web Services-Blog

AWS Global Accelerator Dokumentation

Die folgenden verwandten Ressourcen bieten Ihnen nützliche Informationen für die Arbeit mit diesem Service.

- AWS Global Accelerator— Die API-Aktion enthält vollständige Beschreibungen der API-Aktionen, -Parameter und -Datentypen und eine Liste von Fehlern, die der Service zurückgibt.
- AWS Global Accelerator Produktinformationen— Die Hauptwebsite für Informationen zu Global Accelerator einschließlich Funktionen und Preisen.
- Nutzungsbedingungen für die -Nutzung— Detaillierte Informationen zu unseren Urheber- und Markenrechten, zu Ihrem Konto, zu Ihrer Lizenz, zu Ihrem Zugriff auf die Website und zu weiteren Themen.

Supportanfragen

Support für Global Accelerator ist in verschiedenen Formen verfügbar.

- Diskussionsforen— Ein Community-Forum, das für Entwickler eingerichtet wurde, um über technische Fragen zu Global Accelerator zu diskutieren.
- AWS Support Center – Diese Website stellt Informationen zu Ihren aktuellen Support-Vorgängen und den Ergebnissen aus AWS Trusted Advisor und Zustandsprüfungen, Links zu Diskussionsforen, technische FAQs, die Übersicht zum Servicestatus sowie Informationen zu AWS Support-Plänen bereit.

- AWS Premium Support-Informationen – Die primäre Webseite für Informationen zu AWS Premium, einem persönlichen und reaktionsschnellen Support-Kanal. Hier erhalten Sie Hilfe bei der Entwicklung und Ausführung von Anwendungen auf AWS Infrastructure Services.
- Kontakt – Links zu Informationen zu Ihrer Abrechnung. Technische Fragen stellen Sie bitte in den Diskussionsforen oder über die Support-Links.

Tipps aus dem Amazon Web Services-Blog

Das AWS -Blog enthält eine Reihe von Beiträgen, die Sie bei der Nutzung von AWS Services unterstützen können. Lesen Sie beispielsweise die folgenden Blogbeiträgen über Global Accelerator:

- AWS Global Accelerator für Verfügbarkeit und Leistung
- Management von Datenverkehr mit AWS Global Accelerator
- Analyse und Visualisierung von AWS Global Accelerator Flow Logs mit Amazon Athenaund Amazon QuickSight

Eine vollständige Liste der AWS Global Accelerator -Blogs finden Sie unterAWS Global Acceleratorin der Kategorie Netzwerk- und Inhaltsbereitstellung der AWS -Blogbeiträge.

Dokumentverlauf

Die folgenden Einträge beschreiben die wichtigsten Änderungen an der AWS Global Accelerator Dokumentation.

- API-Version: aktuelle
- Letzte Aktualisierung der Dokumentation: 9. Dezember 2020

Änderung	Beschreibung	Datum
Aktualisieren der vorhandenen serviceverknüpften Rolle Global Accelerator	Global Accelerator hat eine neue Berechtigung hinzugefügt,`ec2:DescribeRegions` , damit Global Accelerator Informationen zur AWS Region abrufen kann, um Fehler zu diagnostizieren. Weitere Informationen finden Sie unter https://docs.aws.amazon.com/global-accelerator/latest/dg/security-iam-awsmanpol-updates.html.	7. Mai 2021
Benutzerdefinierte Routing-Beschleuniger hinzugefügt	Global Accelerator führte einen neuen Typ benutzerdefinierter Beschleuniger für das Routing von Beschleunigern ein. Benutzerdefinierte Routingbeschleuniger eignen sich gut für Szenarien, in denen Sie benutzerdefinierte Anwendungslogik verwenden möchten, um einen oder mehrere Benutzer an ein bestimmtes Ziel und einen bestimmten Port unter vielen	9. Dezember 2020

Änderung	Beschreibung	Datum
	zu lenken, während sie dennoch die Leistungsvorteile von Global Accelerator nutzen. Weitere Informationen finden Sie unter https://docs.aws.amazon.com/global-accelerator/latest/dg/work-with-custom-routing-accelerators.html.	
Unterstützung für Portübers chreibungen hinzugefügt	Global Accelerator unterstüt zt jetzt das Überschreiben des Listener-Ports, der für das Routing von Datenverk ehr an Endpunkte verwendet wird, sodass Sie Datenverkehr an bestimmte Ports auf Ihren Endpunkten umleiten können. Weitere Informationen finden Sie unter https://docs.aws.amazon.com/global-accelerator/latest/dg/about-endpoint-groups-port-override.html.	21. Oktober 2020
Hinzugefügt zwei neue Regionen	Global Accelerator unterstüt zt jetzt Afrika (Kapstadt) und Europa (Mailand). Weitere Informationen finden Sie unter https://docs.aws.amazon.com/global-accelerator/latest/dg/preserve-client-ip-address.regions.html.	20. Mai 2020

Änderung	Beschreibung	Datum
Tagging und BYOIP	Diese Version bietet Unterstützung für das Hinzufügen von Tags zu Beschleunigern und das Hinzufügen Ihrer eigenen IP-Adresse in AWS Global Accelerator (BYOIP). Weitere Informationen finden Sie unter https://docs.aws.amazon.com/global-accelerator/latest/dg/tagging-in-global-accelerator.html und https://docs.aws.amazon.com/global-accelerator/latest/dg/using-byoip.html.	27. Februar 2020
Sicherheitskapitel	Inhalte für Compliance, Ausfallsicherheit und Infrastruktursicherheit hinzugefügt. Weitere Informationen finden Sie unter https://docs.aws.amazon.com/global-accelerator/latest/dg/security.html.	20. Dezember 2019

Änderung	Beschreibung	Datum
Support für EC2-Instances und Standard-DNS-Namen	AWS Global Accelerator unterstützt jetzt das Hinzufügen von EC2-Instances in unterstützten AWS Regionen. Darüber hinaus erstellt Global Accelerator einen Standard-DNS-Namen, der den statischen IP-Adressen für den Accelerator zugeordnet ist. Weitere Informationen finden Sie unter https://docs.aws.amazon.com/global-accelerator/latest/dg/introduction-how-it-works-client-ip.html und https://docs.aws.amazon.com/global-accelerator/latest/dg/about-accelerators.html#about-accelerators.dns-addressing.	29. Oktober 2019
Erhaltung der Client-IP-Adresse für Application Load Balancers	Sie können jetzt festlegen, dass AWS Global Accelerator die Client-IP-Adresse für Application Load Balancers in unterstützten AWS-Regionen beibehalten soll. Weitere Informationen finden Sie unter https://docs.aws.amazon.com/global-accelerator/latest/dg/introduction-how-it-works-client-ip.html.	28. August 2019

Änderung	Beschreibung	Datum
Freigabe des AWS Global Accelerator -Service	Das AWS Global Accelerator Developer Guide enthält Informationen zum Einrichten und Verwenden von Beschleunigern (Traffic Manager auf Netzwerkebene), die die Verfügbarkeit und Leistung Ihrer Internetanwendungen mit globaler Zielgruppe verbessern.	26. November 2018

AWS-Glossar

Die neueste AWS-Terminologie finden Sie im AWS-Glossar im AWS-Referenzhandbuch.

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.