使用者指南

AWS 轉換



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

AWS 轉換: 使用者指南

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

Amazon 的商標和商業外觀不得用於任何非 Amazon 的產品或服務，也不能以任何可能造成客戶混淆、任何貶低或使 Amazon 名譽受損的方式使用 Amazon 的商標和商業外觀。所有其他非 Amazon 擁有的商標均為其各自擁有者的財產，這些擁有者可能附屬於 Amazon，或與 Amazon 有合作關係，亦或受到 Amazon 贊助。

Table of Contents

什麼是 AWS 轉換？ 1
術語 1
開始使用 4
設定 4
開始之前 4
註冊 AWS 帳戶 4
IAM 限定存取入門 4
使用 IAM 登入資料 5
入門 AWS Organizations 6
入門 AWS IAM Identity Center 7
使用第三方身分提供者 7
上線 10
使用您自己的 S3 儲存貯體 11
啟用 AWS 轉換 19
快速入門：嘗試 AWS 轉換 21
管理使用者 21
在 IAM Identity Center 中新增使用者 21
新增使用者至 AWS 轉換 22
使用僅限 IAM 存取管理使用者 22
了解協作者許可 23
AWS 轉換環境 25
語言設定 26
啟動您的專案 27
AWS 轉換聊天 28
連接器 29
代理操作的使用者可追蹤性 29
管理連接器 30
開發人員工具 32
Kiro Power 32
代理程式外掛程式 32
IDE 外掛程式 33
MCP 伺服器 33
身分驗證 34
建置 AWS 轉換的自訂代理程式 34

Custom 36
什麼是 AWS 轉換自訂？ 36
關鍵功能 36
轉換模式 36
AWS 轉換自訂的運作方式 38
了解 的核心概念 38
轉換定義 39
轉換登錄檔 39
草稿與發佈的轉換 40
參考與課程 40
組建和驗證命令 40
持續學習 41
用戶端技能 41
開始使用 42
先決條件 42
安裝 AWS 轉換 CLI 43
設定身分驗證 43
設定 AWS 區域 45
執行您的第一個轉換 48
了解轉換結果 49
建立自訂轉換 49
AWS 轉換 Web 應用程式 （選用） 50
自訂轉換命令簡介 50
工作流程 51
執行轉換 51
持續學習 56
進階組態 57
建立自訂轉換 69
命令參考 73
互動式命令 73
轉換定義命令 73
課程命令 76
標籤命令 76
更新命令 77
MCP 命令 77
AWS受管轉換 77

概觀 77
可用 AWS受管轉換 78
自訂 AWS受管轉換 92
常用案例 92
Lambda 執行期升級 93
VPC 端點 (AWS PrivateLink) 94
AWS Transform 自訂 VPC 端點的考量事項 94
先決條件 94
為 AWS Transform 自訂建立介面 VPC 端點 95
建立 AWS Transform 自訂的 VPC 端點政策 95
使用內部部署電腦連線至 AWS Transform 自訂端點 96
疑難排解 96
日誌位置 96
常見問題 97
取得支援 99
S3 存取問題 99
CLI 版本歷史記錄 100
持續現代化 112
什麼是 AWS 轉型持續現代化？ 112
關鍵功能 112
分析類型 112
了解核心概念 113
來源 113
儲存庫 114
分析 114
調查結果 114
修復 114
轉換定義 114
AWS 轉型持續現代化的運作方式 114
運算選項 115
安全代理程式設定 117
開始使用 118
先決條件 118
快速入門 119
使用持續現代化 120
來源管理 120

儲存庫探索和管理 121
執行分析 121
管理調查結果 122
建立修復 123
遠端執行 123
排程週期性分析 127
標記和存取控制 128
AWS 轉換 Web 應用程式 129
開發人員工具 131
代理技能 131
CLI 參考 132
疑難排解 135
遷移評估 137
先決條件 137
遷移評估的運作方式 137
上傳庫存資料 138
檢閱探索結果 138
管理庫存範圍 139
設定評估案例 139
評估功能 140
Amazon EC2 大小適中 140
Amazon EBS 儲存體 140
Amazon FSx 140
Amazon RDS for SQL Server 140
Amazon EC2 SQL Server 141
內部部署定價 141
永續性 141
商業價值評估 141
網路成本 142
支援成本 142
最終使用者運算 142
使用聊天式評估 142
資料有限的粗略估算 142
透過聊天新增庫存 142
修改成本和新增服務 143
比較案例 143

建立案例 143
執行比較 143
假設分析 144
產生交付項目 144
相關主題 144
探索工具 145
工作流程 145
設定 探索工具 146
先決條件 146
在 VMware 上部署 148
在 Hyper-V 上部署 149
在 Linux 上部署 149
設定 探索工具 152
所需的許可 163
VMware vCenter 163
Hyper-V 主機 (Windows) 164
Linux 伺服器 (SSH) 164
Windows 伺服器 (WinRM) — 作業系統指標 166
Windows 伺服器 (WinRM) — SQL Server 集合 167
Oracle 資料庫 (SQL) 167
網路集合 168
快速參考：使用案例的最低許可 169
資料收集 170
收集排程 170
探索的庫存 171
作業系統相關資料 174
安全考量 189
保護探索工具 VM 189
保護登入資料 189
登入資料儲存 191
謹慎使用自動連線功能 191
CSV Import Security 192
撤銷存取考量 192
探索工具故障診斷 193
驗證探索工具與 vCenter 的連線 193
WinRM 故障診斷 195

Kerberos 疑難排解 195
Oracle 資料庫疑難排解 198
SNMP 故障診斷 200
網路集合錯誤 201
作業系統指標集合錯誤 202
已探索庫存中的存取問題 202
SSH 金鑰身分驗證疑難排解 202
Linux 安裝程式疑難排解 203
常見錯誤訊息 203
版本備註 204
遷移 (包括 VMware) 209
功能和主要功能 209
Architecture 209
遷移任務 210
取得工作區 210
任務類型 211
建立和啟動任務 212
下載工作區摘要報告 212
使用專家模式 213
限制 214
探索來源資料 214
建置遷移計劃 215
遷移規劃術語 216
工作流程 216
7Rs 建議 218
圖表和報告 219
連接目標 AWS 帳戶和區域 220
步驟 1：遷移類型選擇 220
步驟 2：MAP 協議 220
步驟 3：連接器組態 220
建置登陸區域 226
連接器設定 226
基礎設定 227
工作負載帳戶設計 230
IaC 格式 231
部署核准程序 232

標記登陸區域資源 232
反轉變更 233
相關資源 233
將您的網路遷移至 AWS 234
步驟 1：來源網路映射 234
步驟 2：其他組態檔案 236
步驟 3：網路拓撲 236
步驟 4：安全群組映射 238
步驟 5：檢閱和最佳化您的網路 241
步驟 6：網路圖表 244
步驟 7：設定資源標記 244
步驟 8：部署您的網路 245
刪除部署的網路資源 246
組態檔案擷取 247
遷移伺服器 248
先決條件和設定遷移預設值 249
版本備註 266
2026 年 8 月 266
2026 年 7 月 266
2026 年 6 月 267
2026 年 5 月 267
2026 年 4 月 267
2026 年 3 月 268
2026 年 2 月 268
2026 年 1 月 268
2025 年 12 月 268
2025 年 10 月 268
2025 年 9 月 268
2025 年 8 月 269
2025 年 5 月 269
原始程式碼容器化 270
功能和主要功能 270
容器化的運作方式 270
先決條件 271
容器化工作流程 271
啟動容器化任務 272

許可 272
基本政策 272
網路政策 273
儲存政策 273
AWS KMS 政策 273
Amazon ECS 政策 273
Amazon EKS 政策 274
步驟 1：安全免責聲明 274
免責聲明涵蓋的內容 274
您需要執行的事項 275
步驟 2：複製原始程式碼 275
選項 1：Git 儲存庫 275
選項 2：Zip 檔案上傳 276
選用：設定私有相依性 276
確認容器化偏好設定 277
步驟 3：容器化 277
容器化期間會發生什麼情況 277
支援的應用程式類型 278
您需要執行的事項 278
步驟 4：檢閱成品 278
檢閱 Git 儲存庫的變更 278
檢閱 zip 上傳的變更 279
請求變更 279
步驟 5：發佈映像 279
發佈期間會發生什麼情況 279
您需要執行的事項 279
步驟 6：產生 IaC 280
Amazon Elastic Kubernetes Service (Kubernetes) 280
Amazon Elastic Container Service (Terraform) 281
自動化驗證和安全性掃描 281
在沒有發佈映像的情況下產生 IaC 281
您需要執行的事項 281
步驟 7：部署測試基礎設施 282
測試部署期間會發生什麼情況 282
您需要執行的事項 282
在基礎設施上反覆運算 282

工作階段復原 283
步驟 8：清除測試基礎設施 283
您需要執行的事項 283
步驟 9：部署切換基礎設施 283
您需要執行的事項 283
工作階段復原 284
大型主機現代化 285
功能和主要功能 285
高階演練 286
循環中的人類 (HITL) 286
大型主機應用程式轉換支援的檔案類型 286
適用於 AWS Transform 主機的支援區域和配額 287
現代化旅程 287
階段 1：評估 288
階段 2：調動 289
階段 3：遷移和現代化 289
階段 4：操作、最佳化和創新 291
大型主機應用程式工作流程的轉換 291
先決條件：在 S3 中準備專案輸入 292
大型主機來源成品集合 293
登入並建立任務 301
追蹤轉換進度 302
設定連接器 302
評估和重新構想任務計畫 306
重新構想任務計畫 310
自訂任務計畫 310
建置和部署現代化應用程式 336
先決條件 336
步驟 1：擷取現代化程式碼 337
步驟 2：建置現代化應用程式 337
步驟 3：設定測試環境 338
步驟 4：部署現代化應用程式 339
步驟 5：測試現代化應用程式 339
其他範例 339
全堆疊 Windows 現代化 340
.NET 340

體驗 340
功能和主要功能 341
支援的版本和專案類型 341
限制 342
人工介入 342
其他資訊 342
.NET Web 應用程式 343
.NET IDE 357
移植 UI layer 程式碼 363
轉換報告 365
最佳實務 367
SQL Server 現代化 371
支援的 區域 372
功能和主要功能 372
支援的版本和專案類型 373
現代化任務入門 377
連線至資料庫 （線上工作流程） 377
上傳 DDL 檔案 （離線工作流程） 426
最佳實務和疑難排解 429
安全 435
資料保護 435
跨區域處理 437
資料加密 445
服務改進 454
身分與存取管理 454
目標對象 455
使用身分驗證 455
使用政策管理存取權 456
AWS 轉換如何與 IAM 搭配使用 457
身分型政策範例 462
疑難排解 471
使用服務連結角色 473
AWS 受管政策 478
AWS 轉換許可參考 490
法規遵循驗證 492
恢復能力 493

VPC 端點 (AWS PrivateLink) 493
AWS Transform VPC 端點的考量事項 493
先決條件 493
建立 的介面 VPC 端點 AWS Transform 494
使用內部部署電腦連線至 AWS Transform 端點 495
Web 應用程式 VPC 存取 495
運作方式 495
Architecture 496
先決條件 496
設定 VPC 端點政策 497
設定受控網際網路輸出 497
驗證 504
疑難排解 505
成本考量 506
清除 506
監控 508
CloudTrail 日誌 508
AWS 轉換 CloudTrail 中的資訊 509
了解 AWS 轉換日誌檔案項目 509
通知 509
電子郵件通知 510
配額 512
支援的區域 515
Supported AWS 區域 （預設為啟用） 515
支援 517
先決條件 517
啟用支援案例管理 517
建立支援案例 517
檢視支援案例 518
將通訊新增至案例 519
解決案例 519
停用支援案例管理 519
用量遙測 520
操作資料 521
變更日誌 522
文件歷史紀錄 538

..... dxlv

什麼是 AWS 轉換？

AWS 轉換是一項服務，可協助您透過代理式 AI 體驗加速和簡化基礎設施、應用程式和程式碼的轉換。它提供專門的工具，以簡化各種工作負載的現代化和遷移工作。

透過 AWS 轉換，您可以：

- 將 IBM z/OS 和 Fujitsu GS21 現代化並遷移至 AWS
- 將虛擬和裸機伺服器環境遷移至 Amazon EC2，包括 VMware、Hyper-V 和其他平台：
  - 探索。從多個來源收集和分析現場部署伺服器庫存，以便在規劃之前了解您的環境。
  - 遷移規劃。將應用程式分組，識別相依性，並建置優先遷移波。
  - 建立登陸區域。設計和部署具有組織結構、控管控制和帳戶設定的多帳戶 AWS 基礎。
  - 網路遷移。將您的來源網路組態轉換為生產就緒的 AWS VPC 架構，並將其部署。
  - 伺服器重新託管。使用引導式複寫、測試和切換工作流程，重新託管伺服器以在 Amazon EC2 上原生執行。
  - 原始程式碼容器化。從原始程式碼容器化應用程式，並部署到 Amazon Elastic Container Service 或 Amazon Elastic Kubernetes Service。
- 將 .NET 應用程式現代化為 Linux 就緒的跨平台 .NET
- 評估工作負載的遷移準備程度

AWS 轉換可協助您將整個探索、規劃和執行階段的人力密集、複雜轉換任務卸載給具備語言、架構和基礎設施專業知識的 AI 代理器。這種方法可讓您的團隊專注於創新，同時透過統一的 Web 體驗有效率地轉換複雜的大規模專案。

使用 AWS Transform 無需額外費用。

術語

在本節中，斜體表示不同詞彙定義的正式詞彙。

帳戶連線

> 此內容中的帳戶是 或遠端服務中資源的客戶擁有容器 AWS 或安全界限的一般參考，例如 AWS 帳戶 或 GitHub 帳戶。

成品

AWS Transform 產生的輸出可交付項目。

管理員

管理員可以讀取和變更工作區中的所有內容。他們可以使用 AWS 轉換開始聊天、開始和停止任務，以及上傳/下載成品。管理員可以針對human-in-the-loop(HITL) 動作與執行中的任務互動，也可以核准重要的 HITL 動作，例如合併至主要、執行圖形分解，或將程式碼部署至生產環境。管理員可以變更工作區、連接器和使用者。

代理程式

執行特定轉換類型的任務特定服務。例如，VMware 遷移。

核准者

核准者具有與管理員類似的許可，但他們沒有變更工作區、連接器或使用者的許可。核准者無法變更工作區、連接器或使用者。

資產

轉換任務的輸入。例如，客戶的原始碼、伺服器、資料庫、網路。透過連接器存取資產。

協作器請求

AWS 轉換正在要求人類執行任務的任務。

連接器

連接器是資產提供者，允許存取 AWS Transform 外部系統中的客戶擁有資源。

當您設定連接器時，您要連線的帳戶管理員必須接受連線。若要接受連線，他們必須擁有連接器接受者政策中授予的許可。

下列兩個帳戶必須相同，或在相同的 AWS Organizations 組織中：

- AWS 轉換管理員從中啟用服務的 帳戶。
- 將在轉換接收端的帳戶。此帳戶必須獲指派 IAM 角色，允許其使用連接器。

貢獻者

貢獻者可以讀取工作區中的所有內容。他們可以使用轉換開始聊天 AWS 、開始和停止任務、上傳或下載成品，以及與 HITL 動作的執行中任務互動。不過，他們無法執行重要的 HITL 動作，例如合併至主要、執行圖形分解，或將程式碼部署至生產環境。貢獻者也無法變更工作區、連接器或使用者。

目標

AWS 轉換可達到的使用者定義結束狀態。使用者撰寫此項目，然後 AWS 轉換會將目標轉換為一系列任務，並在需要時與使用者協同執行。

任務

AWS 轉換正在進行的長期執行程序（週/月+），以滿足使用者定義的目標。由多個任務和協作者請求組成。

計劃

Transform 為追求目標所 AWS 進行（在人類使用者的協助下）的任務清單。

讀取器

讀者可以檢視 AWS 轉換任務的狀態和結果，但無法進行任何變更。他們可以讀取工作區中的所有內容、下載成品、檢視任務，以及檢視human-in-the-loop(HITL) 動作。不過，讀者無法在 AWS 轉換中執行變動動作。

任務

屬於任務一部分的個別工作單位。

Worklog

AWS 轉換和使用者在任務中執行哪些動作的日誌。

工作區

包含連接器和任務等其他資源的 AWS 轉換資源。工作區做為許可界限。

AWS 轉換入門

主題

- 設定 AWS 轉換
- 啟用 AWS 轉換
- 快速入門：嘗試 AWS 轉換
- 管理使用者
- AWS 轉換環境
- AWS 轉換連接器

設定 AWS 轉換

開始之前

設定 AWS 轉換之前，請確定您擁有具有管理員存取權 AWS 的帳戶

> **Note**
>
> 如果您想要嘗試 AWS 轉換作為proof-of-concept或測試環境，請參閱快速入門：嘗試 AWS 轉換。

註冊 AWS 帳戶

若要開始使用 AWS，您需要 AWS 帳戶。如需建立 的相關資訊 AWS 帳戶，請參閱《 AWS 帳戶管理參考指南》中的 入門 AWS 帳戶。

IAM 限定存取入門

透過僅限 IAM 的存取，使用者會使用其現有的 AWS 登入資料進行身分驗證。

若要設定僅限 IAM 存取：

1. 在 AWS 主控台中，導覽至 AWS 轉換，然後選擇開始使用。
2. 完成帳戶設定組態。

3. 在使用者存取下，選取僅限 IAM 存取。
4. 選擇啟用以建立您的設定檔。

使用者透過 AWS Sign-In 登入 AWS Transform Web 應用程式。Web 應用程式中的使用者識別符是以其 IAM 主體為基礎。

> **Important**
>
> 設定完成後，您就無法新增身分提供者。若要使用 IAM Identity Center 或現有的身分提供者管理使用者，請在初始設定期間選擇其中一個選項。

透過僅限 IAM 存取，任何在設定檔資源上具有 `transform:AccessTransformProfile`許可的 IAM 主體都可以存取 AWS Transform。您可以透過 IAM 政策管理使用者存取權，而不是透過身分提供者使用者指派。

`transform:AccessTransformProfile` 動作只會授予 AWS 對 Transform 的存取權。進入 AWS 轉換後，工作區角色會控制使用者可以執行的動作。這些角色包括管理員、貢獻者、核准者和唯讀。無論使用者如何驗證，工作區角色都適用。

使用 IAM 登入資料

使用者資訊處理

當 IAM 主體存取 AWS Transform 時，服務處理使用者身分的方式與使用身分提供者型存取的方式不同。

使用者身分

IAM 使用者由其 IAM 主體識別。

雙重身分

同時具有身分提供者身分 （ 例如 IAM Identity Center) 和 IAM 工作階段的使用者會在 AWS 轉換中顯示為兩個不同的使用者。它們的工作不會在兩個身分之間連結。

電子郵件通知

只有 SSO 使用者才能啟用電子郵件通知。IAM 主體仍可新增至工作區，但不會收到電子郵件通知。

稽核

IAM API 呼叫會使用 AWS CloudTrail 呼叫者的 IAM 身分登入。任務中 IAM 使用者執行的動作也可以在 AWS 轉換工作日誌中追蹤。

與身分提供者一起啟用 IAM 存取

如果您使用 IAM Identity Center 或第三方身分提供者設定 AWS 轉換，您也可以啟用 IAM 存取作為驗證的額外方式。這可讓 IAM 主體與您現有的身分提供者使用者一起存取 AWS Transform。

當您使用 IAM Identity Center 或第三方身分提供者建立設定檔時，預設會啟用 IAM 存取。若要隨時啟用或停用 IAM 存取：

1. 在 AWS 轉換主控台中，導覽至設定。
2. 在使用 IAM 登入資料進行存取 AWS 轉換下，開啟或關閉啟用 IAM 存取。

啟用 IAM 存取時，身分提供者使用者和 IAM 主體都可以使用 AWS 轉換。IAM 使用者和身分提供者使用者可以在同一個工作區中進行協作。

入門 AWS Organizations

請依照下列步驟設定 AWS 轉換：

1. 登入您的 AWS Organizations 管理帳戶。
2. 導覽至 AWS 轉換服務。
3. 選擇為您的組織啟用服務以使用 AWS 轉換。
4. 設定組織成員帳戶的必要許可。
5. 從成員帳戶存取 AWS 轉換 Web 體驗。

> **Note**
>
> 若要在 AWS 解決方案上使用登陸區域加速器 (LZA) 來建置您的登陸區域以及遷移功能的 AWS 轉換，您的 AWS 轉換帳戶和 LZA 安裝必須位於相同的 AWS 組織。不支援使用 LZA 和 AWS Transform 部署的個別 Organizations IDs，因為這可能會導致組織管理和資源部署不一致。若要了解如何使用 Organizations 設定 LZA 安裝，請參閱《實作指南》中的部署雲端基礎來支援高度管制的工作負載和複雜的合規要求。 AWS

入門 AWS IAM Identity Center

請依照下列步驟使用 IAM Identity Center 進行 AWS 轉換，並新增使用者和群組。

根據預設，當您第一次啟用 AWS 轉換時，沒有任何使用者可以存取轉換。

> **Note**
>
> IAM Identity Center 不限於其設定所在的區域。如果您已在 AWS Transform 不支援的區域設定 IAM Identity Center，則可以將其用於 AWS Transform。

1. 按照 中的指示設定 IAM Identity Center 以啟用 IAM Identity Center 的執行個體。

   設定 IAM Identity Center 使用外部企業身分提供者，並將其使用者和群組資訊複寫至 IAM Identity Center。
2. 在 AWS 主控台中，選取 AWS 轉換，然後選擇開始使用。
3. 選擇為您的組織啟用服務以使用 AWS 轉換。
4. 選取加密金鑰。預設選擇是 AWS 受管金鑰。若要使用自訂金鑰：

   a. 在加密金鑰下，選擇自訂加密設定。
   b. 選取使用 AWS KMS 金鑰。
   c. 選擇現有的金鑰或建立新的金鑰。
   d. 選擇提交以套用您的變更，然後選擇啟用 AWS 轉換。

   選擇檢視設定檔以檢視組態。您的使用者會使用 Web 應用程式 URL 來存取 AWS 轉換統一的 Web 體驗。
5. 在導覽窗格中選取使用者，然後選取指派使用者或群組。
6. 搜尋您要授權使用 AWS Transform 的使用者或群組名稱。搜尋會參考從您的身分提供者傳播的使用者和群組。
7. 選取群組或使用者，選取完成，然後選取指派。這些使用者有權使用 AWS 轉換統一 Web 界面。

使用第三方身分提供者

AWS Transform 支援與第三方身分提供者 (IdPs整合，例如 Azure Active Directory (Entra ID) 和 Okta Workforce Identity。這可讓您使用現有的身分管理系統進行使用者身分驗證。

先決條件

在設定第三方身分提供者整合之前，請確定身分提供者中的使用者已設定名稱、電子郵件和使用者名稱屬性

儲存的資訊

當您搭配 IdPs 使用 AWS Transform 時， 會 AWS 存放加密且安全的最少使用者資訊：

儲存的使用者資訊

AWS 轉換會在第一次登入時存放基本使用者設定檔資訊，包括顯示名稱、電子郵件地址、使用者名稱 (preferred_username) 和唯一的使用者識別符。此資訊會使用客戶擁有的 KMS 金鑰或服務擁有的金鑰進行加密，取決於客戶的 AWS 轉換設定檔組態。資料會存放在 AWS 轉換的身分驗證資料庫中，而且只會在初始登入工作階段期間收集。這會在邀請其他使用者加入工作區時填入搜尋結果。

資料生命週期

使用者資訊只會儲存給已登入 AWS Transform Web 應用程式至少一次的使用者，如果使用者在身分提供者中更新其資訊而不重新登入 AWS Transform，可能會變得過時。刪除 AWS 轉換設定檔時，會刪除所有儲存的使用者資訊。

用戶端秘密儲存

設定期間提供的用戶端秘密 AWS Secrets Manager 會透過您帳戶中的服務連結秘密 (SLS) 使用 儲存。

使用者識別符處理

Entra

使用「oid」（物件識別符）宣告做為唯一的使用者識別符，該識別符是不可變且唯一識別 Microsoft 租用戶中的使用者。客戶可以在 Entra 主控台中看到此值，並顯示在 CloudTrail 日誌中。

Okta 人力資源身分

根據權杖類型，使用不同的宣告進行使用者識別 - ID 權杖中的「sub」宣告和存取權杖中的「uid」宣告。 AWS Transform 會在身分驗證期間驗證這兩個宣告是否包含相同的值。客戶可以在 Okta 主控台中看到此值，並顯示在 CloudTrail 日誌中。

設定 Azure Active Directory (Entra ID)

若要設定 Azure Active Directory 與 AWS Transform 的整合：

1. 導覽至 Azure 入口網站，然後選取 Azure Active Directory。
2. 在左側導覽窗格中，選擇管理 > 應用程式註冊。
3. 選擇 + 新註冊。
4. 輸入應用程式名稱、選擇支援的帳戶類型、將重新導向 URI 保留空白，然後選擇註冊。
5. 在左側導覽中，選擇管理 > 資訊清單。
6. `requestedAccessTokenVersion` 從 更新`null`為 `2` ，然後選擇儲存。
7. 選擇管理 > 公開 API，然後選擇新增範圍。
8. 使用預設結構 建立應用程式 ID URI`api://<client-id>`。
9. 新增範圍 `transform:read_write`。
10. 選擇新增憑證或秘密，並建立新的用戶端秘密。視需要儲存此值以建立設定檔。
11. 選擇端點並選取 OpenID Connect 中繼資料文件，以尋找發行者 URL。中繼資料中的「發行者」欄位是您的發行者 URL。
12. 使用用戶端 ID、用戶端秘密和發行者 URL 在 AWS 轉換主控台中建立設定檔。
13. 建立設定檔後，選擇新增平台、選取 Web 並輸入 來新增重新導向 URI`<web-application-url>/login/callback`。

設定 Okta 人力資源身分

若要設定 Okta Workforce Identity 與 AWS Transform 整合：

1. 導覽至 Okta Workforce Identity 主控台。
2. 選擇應用程式 > 應用程式，然後選擇建立應用程式整合。
3. 選取 OIDC - OpenID Connect 和 Web 應用程式，然後選擇下一步。
4. 為您的應用程式命名、將授予類型保留為授權碼、將重新導向 URIs保留空白、設定使用者指派，然後選擇儲存。
5. 導覽至登入索引標籤，並將發行者設定為 Okta URL，而非動態。
6. 複製用戶端 ID，並前往安全 > API 並新增授權伺服器，將其設定為授權伺服器的對象。
7. 在授權伺服器中，在範圍索引標籤`transform:read_write`下新增範圍。
8. 新增存取政策，允許 OIDC 應用程式使用此授權伺服器並設定政策的規則。

9. 在授權伺服器設定頁面上，記下在 AWS 轉換中建立設定檔的發行者 URL。
10. 使用應用程式設定中的發行者 URL、用戶端 ID 和用戶端秘密，在 AWS 轉換中建立設定檔。
11. 建立設定檔後，在應用程式的一般索引標籤中將 新增`<web-application-url>/login/callback`為重新導向 URL。

> **Note**
>
> 如果您想要在登出後重新導向回 AWS 轉換 Web 應用程式，則需要在安全 > API 下將 Web 應用程式 URL 設定為信任的原始伺服器。

使用者加入

本節說明已獲授予 AWS Transform 存取權的使用者體驗。

接受邀請

當使用者新增至 AWS 轉換時，他們會收到電子郵件邀請，其中包含：

- 邀請的問候語和資訊
- AWS 轉換 Web 應用程式 URL
- 他們的使用者名稱
- 接受邀請並設定其密碼的連結

若要設定其帳戶：

1. 使用者按一下電子郵件中的「接受邀請」連結。
2. 在「新使用者註冊」頁面上，他們輸入並確認密碼。
3. 密碼必須符合安全要求，包括：
    - 至少 8 個字元
    - 至少一個大寫字母
    - 至少一個小寫字母
    - 至少有一個數字
    - 至少一個特殊字元
4. 建立密碼後，他們會看到其帳戶已成功建立的確認。

登入以進行 AWS 轉換

若要登入以進行 AWS 轉換：

1. 導覽至邀請電子郵件中提供的 AWS 轉換 Web 應用程式 URL。
2. 輸入使用者名稱。
3. 選擇下一步。
4. 輸入密碼。
5. 選擇登入。

歡迎體驗

第一次登入時，使用者會看到 AWS Transform 歡迎頁面，其中包含：

- 個人化問候語
- 可用的轉換功能
- 建立工作區的選項

歡迎頁面提供有關 AWS Transform 中可用轉換功能的資訊，包括：

- 現代化 IBM z/OS 遷移至 AWS
- 將 VMware 工作負載遷移至 Amazon EC2
- 將 .NET 應用程式現代化為 Linux 就緒的跨平台 .NET
- 評估工作負載的遷移準備程度

使用者可以從建立工作區開始，或要求團隊將他們新增至現有的工作區。

使用您自己的 Amazon S3 儲存貯體

根據預設， AWS Transform 會使用服務管理的 Amazon S3 儲存貯體來存放轉換成品。您可以選擇使用自己的 Amazon S3 儲存貯體，以更好地控制資料儲存、加密和存取政策。

> **Note**
>
> 如果您有用於大型主機轉換的 Amazon S3 儲存貯體，您可以繼續使用該 S3 連接器，而且不需要使用此功能。

> **Note**
>
> Amazon S3 儲存貯體只會儲存您互動的上傳和轉換成品。系統產生的內部成品不會存放在您的儲存貯體中。此外，AWS Transform 會為儲存貯體中的成品編製索引。它將索引資料存放在服務管理的知識庫中，用於為您提供豐富的聊天體驗。

先決條件

在您設定自己的 Amazon S3 儲存貯體之前，請確定符合下列要求：

- 儲存貯體必須位於啟用 AWS 轉換的相同 AWS 區域中。
- 必要的儲存貯體政策必須套用至您的儲存貯體。如需詳細資訊，請參閱the section called “必要的儲存貯體政策”。
- 如果您使用 AWS Transform Web 應用程式，則必須在儲存貯體上設定 CORS。如需詳細資訊，請參閱the section called “必要的 CORS 組態”。
- 如果您使用自訂 AWS KMS 金鑰，則必須套用必要的金鑰政策。如需詳細資訊，請參閱the section called “KMS 金鑰政策 （選用）”。

支援的加密組態

您的儲存貯體必須使用下列其中一個加密組態：

- SSE-S3 (AES256) — 將 KMS 金鑰欄位保留空白。 AWS 轉換會寫入物件而不指定加密標頭，而 Amazon S3 會使用 S3-managed金鑰套用儲存貯體的預設加密。如需詳細資訊，請參閱《Amazon S3 使用者指南》中的搭配 Amazon S3 受管金鑰 (SSE-S3) 使用伺服器端加密。
- SSE-KMS 搭配客戶管理的 KMS 金鑰 — 提供 KMS 金鑰 ARN。 AWS Transform `x-amz-server-side-encryption: aws:kms`使用提供的金鑰搭配 寫入物件。遵循the section called “KMS 金鑰政策 （選用）”。

不支援下列項目：

- 具有 受管 KMS 金鑰 AWS的 SSE-KMS （例如 `aws/s3`)
- SSE-C
- DSSE-KMS
- 非對稱 KMS 金鑰或具有 SYMMETRIC_DEFAULT 以外金鑰規格的 KMS 金鑰

> **Warning**
>
> AWS不支援 受管 KMS 金鑰。如果您的儲存貯體使用 加密aws/s3，請先遷移至客戶受管金鑰或 SSE-S3，再將儲存貯體與 AWS Transform 搭配使用。

設定 Amazon S3 儲存貯體

您可以從 AWS 轉換主控台將 AWS 轉換設定為使用您自己的 Amazon S3 儲存貯體。

使用您自己的 Amazon S3 儲存貯體

1. 在 AWS 轉換主控台中，選擇設定。
2. 在成品儲存體下，選擇使用我自己的 S3 儲存貯體。您可以在目前 AWS 帳戶 或其他帳戶中使用儲存貯體。
3. 針對儲存貯體，輸入 Amazon S3 URI。
4. （選用）對於 KMS 金鑰，輸入 AWS KMS 金鑰 ARN 來加密儲存貯體中的物件。如果您將此欄位保留空白， AWS Transform 會在沒有加密標頭的情況下寫入物件，而 Amazon S3 會套用儲存貯體的預設加密設定。如需詳細資訊，請參閱《Amazon S3 使用者指南》中的設定 Amazon S3 儲存貯體的預設伺服器端加密行為。 Amazon S3

   如果您儲存貯體的預設加密是 SSE-KMS，請在此欄位中輸入客戶管理的 KMS 金鑰 ARN，並更新您的金鑰政策。如需詳細資訊，請參閱the section called “KMS 金鑰政策（選用）”。
5. 選擇 Save. AWS Transform 會在套用組態之前驗證儲存貯體組態和許可。

儲存組態之後， AWS Transform 會使用儲存貯體來存放轉換成品。

> **Note**
>
> AWS 轉換只會在您儲存時驗證您的組態。如果您稍後變更儲存貯體政策、CORS 組態或 KMS 金鑰政策，請重新儲存設定檔設定以重新驗證。

必要的儲存貯體政策

您必須設定儲存貯體政策來授予 AWS 轉換存取權。將下列儲存貯體政策新增至 Amazon S3 儲存貯體，以允許 AWS 轉換服務主體讀取、寫入、刪除和列出轉換成品。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "transform.amazonaws.com"
                ]
            },
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:AbortMultipartUpload",
                "s3:ListMultipartUploadParts",
                "s3:PutObjectTagging"
            ],
            "Resource": "arn:aws:s3:::bucket-name/AWSTransform/*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "profile-account-id",
                    "aws:SourceArn": "profile-arn"
                }
            }
        },
        {
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "transform.amazonaws.com"
                ]
            },
            "Action": "s3:ListBucket",
            "Resource": "arn:aws:s3:::bucket-name",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "profile-account-id",
                    "aws:SourceArn": "profile-arn"
                }
            }
        }
    ]
```

```
}
```

取代以下的值：

- *bucket-name* – Amazon S3 儲存貯體的名稱。
- *profile-account-id* – 與您的 AWS 轉換設定檔相關聯的 AWS 帳戶 ID。
- *profile-arn* – AWS 轉換設定檔的 ARN。

必要的 CORS 組態

如果您使用 AWS Transform Web 應用程式，則必須在 Amazon S3 儲存貯體上設定跨來源資源共用 (CORS)。您可以在啟用 AWS 轉換後找到 Web 應用程式網域。如需詳細資訊，請參閱開始使用。

```
[
    {
        "AllowedHeaders": [
            "host",
            "content-type",
            "if-none-match",
            "x-amz-checksum-sha256",
            "x-amz-expected-bucket-owner",
            "x-amz-server-side-encryption",
            "x-amz-server-side-encryption-aws-kms-key-id",
            "x-amz-server-side-encryption-context",
            "x-amz-source-account",
            "x-amz-source-arn"
        ],
        "AllowedMethods": [
            "GET",
            "PUT",
            "HEAD"
        ],
        "AllowedOrigins": [
            "webapp-domain"
        ],
        "ExposeHeaders": [
            "ETag",
            "x-amz-checksum-sha256",
            "x-amz-request-id",
            "x-amz-id-2"
        ],
```

```
        "MaxAgeSeconds": 3600
    }
]
```

取代以下的值：

- *webapp-domain* – 您的 Web 應用程式原始伺服器 URL（例如 https://1a2b3c4d5e6f7a8b9.transform.us-east-1.on.aws），可在 AWS 轉換設定頁面上找到。請勿包含結尾斜線。

KMS 金鑰政策（選用）

本節僅適用於使用客戶受管 KMS 金鑰加密儲存貯體的情況。如果您的儲存貯體使用 SSE-S3，請略過本節。

如果您為儲存貯體加密指定自己的 AWS KMS 金鑰，請將下列陳述式新增至您的金鑰政策。 AWS Transform 依賴轉送存取工作階段 (FAS) 為其服務主體建立授權。這些授權用於驗證 Amazon S3 儲存貯體中的金鑰和存取成品。

```
{
    "Sid": "AllowAWSTransformServiceAccess",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::key-owner-account-id:root"
    },
    "Action": [
        "kms:CreateGrant",
        "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:ViaService": "transform.region.amazonaws.com"
        }
    }
}
```

取代以下的值：

- *key-owner-account-id* – 擁有 KMS 金鑰的 AWS 帳戶 ID。
- *region* – 啟用 AWS 轉換 AWS 的區域（例如 us-east-1）。

切換回預設儲存貯體

您可以隨時切換回服務受管儲存貯體。

切換到 AWS 轉換受管儲存

1. 在 AWS 轉換主控台中，選擇設定。
2. 在成品儲存體下，選擇編輯。
3. 選擇AWS 轉換受管儲存。
4. 選擇儲存。

> **Warning**
>
> 如果您在轉換任務進行時切換儲存組態，這些任務會失敗。也無法存取那些進行中任務已產生的任何成品。

> **Important**
>
> 當您切換回服務受管儲存貯體時：
>
> - 儲存貯體中的成品不會自動遷移。若要保留任何成品，請從 Amazon S3 儲存貯體下載它們，並透過 AWS 轉換 Web 應用程式將它們重新上傳到對應工作區和任務的成品存放區。
> - AWS 轉換會淘汰其對 KMS 金鑰的授予。寫入儲存貯體的物件會保留在您的儲存貯體中；如果不再需要，請手動將其刪除。

將檔案直接上傳至您的儲存貯體

您可以直接將檔案上傳至 Amazon S3 儲存貯體，而無需使用 AWS Transform Web 應用程式。若要讓轉換客服人員可以使用上傳的檔案，請將它們上傳到任務的 `User Uploads` 資料夾。此資料夾的目錄路徑使用下列格式：

```
AWSTransform/Workspaces/workspace-id/Jobs/job-id/User Uploads/
```

取代以下的值：

- *`workspace-id`* – AWS 轉換工作區的 ID。

- *job-id* – 轉換任務的 ID。

AWS Transform 中的每個任務都有自己的`User Uploads`資料夾。您上傳至此路徑的檔案會顯示在 Web 應用程式中，並在轉換代理程式完成任務時可供他們使用。

檔案路徑不得包含 `..`、 `//`或前置或結尾空格，客服人員看不到違反這些限制的檔案。

刪除儲存貯體內容可能會導致任務失敗

刪除`job_objective`會導致作用中任務或工作階段還原時的任務失敗。對於所有其他檔案，刪除它們可能會導致意外的客服人員行為或任務失敗。

Important

如果您的儲存貯體使用 SSE-KMS，請在每次直接上傳時包含下列標頭：

```
x-amz-server-side-encryption: aws:kms
x-amz-server-side-encryption-aws-kms-key-id: your-kms-key-arn
```

物件必須使用在 AWS 轉換設定檔中註冊的 KMS 金鑰進行加密。使用任何其他金鑰加密的物件無法存取 AWS Transform。

相容性矩陣

下表摘要說明 AWS Transform 與常見 Amazon S3 儲存貯體功能的相容性。

功能	相容性	備註
儲存貯體版本控制	支援	使用生命週期規則管理非最新版本。
物件擁有權	必要：儲存貯體擁有者強制執行	不支援偏好的儲存貯體擁有者和物件寫入器。
ACL	不支援	必須在儲存貯體上停用 ACLs。
物件鎖定（管理模式）	部分支援	保留設定可能會封鎖刪除。

功能	相容性	備註
物件鎖定（合規模式）	不支援	—
封鎖公有存取權限	支援	—
請求者付款	不支援	—
S3 存取點	不支援	使用儲存貯體名稱。
S3 Object Lambda 存取點	不支援	使用儲存貯體名稱。
S3 on Outposts	不支援	—
S3 Express One Zone（目錄儲存貯體）	不支援	—
跨區域儲存貯體	不支援	—
跨帳戶儲存貯體	支援	—
跨帳戶 KMS 金鑰	不支援	—
生命週期規則	支援	—
CloudTrail 資料事件	支援	—

啟用 AWS 轉換

若要啟用 AWS 轉換：

1. 登入 AWS 管理主控台。

2. 在主控台頂端的搜尋列中，搜尋AWS 轉換。
3. 從搜尋結果中選取AWS 轉換。
4. 選擇開始使用，在您目前的區域中啟用 服務。
5. 選用：設定 IAM Identity Center。您也可以在後續步驟中選擇使用第三方身分提供者 (IdP)。

6. 選取加密金鑰：預設 AWS 受管金鑰或自訂加密設定。
7. 選用：使用您自己的 Amazon S3 儲存貯體。根據預設，AWS Transform 會使用服務管理的 Amazon S3 儲存貯體來存放轉換成品。您可以選擇改用自己的儲存貯體。如需詳細資訊，請參閱使用您自己的 Amazon S3 儲存貯體。
8. 選擇您要啟用的 AWS 轉換功能：
   - 建立和執行自訂轉換所需的命令列界面 (CLI)。若要啟用 CLI，請檢視並遵循下載指示。
   - Web 應用程式，用於現代化的代理程式使用者介面。選擇啟用 Web 應用程式以使用它。
9. 選擇啟用 AWS 轉換。
10. 選用：選擇啟用檢視設定檔以存取 AWS 轉換使用者、設定和連接器索引標籤，或管理使用者以管理使用者。

    您可以隨時存取使用者、設定和連接器索引標籤，方法是選擇主控台左上角的功能表圖示。
11. 選擇下列其中一個選項來設定使用者存取：
    - IAM Identity Center
    - 第三方身分提供者 (IdP)
    - 僅限 IAM 存取

    > **Note**
    >
    > 此選項已完成，且在啟用 AWS 轉換時無法變更。
12. 選擇啟用 Web 應用程式。
13. 系統會在建立必要的資源時顯示「啟用 AWS 轉換」。

啟用 AWS 轉換後，設定索引標籤會顯示下列資訊：

- Web 應用程式 URL - 用於存取 AWS Transform Web 應用程式的 URL
- IDE 的啟動 URL - 用於在整合開發環境中存取 AWS Transform 的 URL
- 區域 - 啟用 AWS 轉換 AWS 的區域

快速入門：嘗試 AWS 轉換

嘗試 AWS 轉換的最簡單方法是使用獨立 AWS 帳戶。您可能想要將其作為proof-of-concept或用於測試環境。使用此程序：

1. 登入 AWS 管理主控台。
2. 導覽至 AWS 轉換服務。
3. 選擇開始使用以啟用服務。
4. 選取並設定您的身分提供者。
5. 將使用者指派給 AWS 轉換服務。
6. 啟用服務後，您會看到 AWS 轉換 Web 應用程式 URL。
7. 在新的瀏覽器視窗中開啟該 URL，以存取 AWS 轉換 Web 體驗。

現在您已準備好設定您的工作區。

管理使用者

如何管理使用者對 AWS Transform 的存取，取決於您在設定期間選擇的存取模型。如果您已設定 IAM Identity Center，您可以透過 IAM Identity Center 新增使用者。如果您已設定第三方身分提供者，您可以管理該提供者中的使用者。如果您選擇僅 IAM 存取，使用者存取會透過 IAM 政策進行管理。

在 IAM Identity Center 中新增使用者

若要在 IAM Identity Center 中新增使用者：

1. 導覽至 IAM Identity Center 主控台。
2. 在導覽窗格中，選擇 Users (使用者)。
3. 選擇新增使用者。
4. 輸入必要資訊：
    - 使用者名稱 - 使用者的唯一識別符 （稍後無法變更）
    - 電子郵件地址 - 使用者的電子郵件地址
    - 名字和姓氏 - 使用者名稱
    - 顯示名稱 - 出現在使用者清單中的名稱

5. 針對密碼，選擇使用者接收密碼的方式：
   - 傳送電子郵件 - 透過電子郵件傳送設定指示
   - 產生一次性密碼 - 建立密碼以手動共用
6. 選擇下一步以檢閱使用者資訊。
7. 檢閱詳細資訊，然後選擇新增使用者。

新增使用者後，他們將收到一封電子郵件邀請，以設定其 IAM Identity Center 帳戶。邀請連結的有效期為 7 天。

您也可以在此影片中了解如何使用 IAM Identity Center 和 AWS Transform：

VideoTitle

新增使用者至 AWS 轉換

將使用者新增至 IAM Identity Center 之後，您可以授予他們 AWS 轉換的存取權：

1. 返回 AWS 轉換主控台。
2. 在導覽窗格中，選擇使用者和群組。
3. 選取使用者索引標籤或群組索引標籤。
4. 搜尋並選取您要從 IAM Identity Center 新增的使用者或群組。
5. 選擇指派使用者和群組，以授予所選使用者或群組對 AWS 轉換的存取權。

新增使用者後，他們會出現在使用者清單中，狀態為「待定」，直到他們接受邀請並登入為止。

使用僅限 IAM 存取管理使用者

如果您設定僅限 IAM 存取的 AWS 轉換，使用者存取會透過 IAM 政策管理。在設定檔資源上具有 `transform:AccessTransformProfile`許可的任何 IAM 主體都可以存取 AWS Transform。

若要授予使用者或角色對 AWS Transform 的存取權：

1. 導覽至 IAM 主控台。
2. 將包含 `transform:AccessTransformProfile`動作的政策連接至 IAM 使用者或角色。如需範例政策，請參閱允許使用者使用 IAM 登入資料存取 AWS 轉換。

若要撤銷存取權，請從 IAM 使用者或角色移除政策。

了解協作者許可

AWS 轉換使用工作區型許可模型來控制對資源和動作的存取。每個使用者都會在工作區中獲指派特定角色，以決定他們可以執行哪些動作。使用者可以在不同的工作區中具有不同的角色。

使用者角色

AWS 轉換支援每個工作區中的五個使用者角色。這些角色適用於工作區的內容，使用者會在其所屬的每個工作區中指派角色。為每個角色定義的存取許可與工作區無關，因此在工作區 A 中具有管理員角色的使用者 A 具有與在工作區 B 中具有管理員角色的使用者 B 相同的許可。

角色許可

每個角色的詳細許可：

Action	ResourceType	管理員	核准者	作者群	ReadOnly
建立	工作區	✓	✓	✓	✓
清單	工作區	✓	✓	✓	✓
取得	工作區	✓	✓	✓	✓
更新	工作區	✓	✗	✗	✗
刪除	工作區	✓	✗	✗	✗
建立	ChatMessage	✓	✓	✓	✗
讀取	ChatMessage	✓	✓	✓	✓
建立	RoleAssociation	✓	✗	✗	✗
讀取	RoleAssociation	✓	✓	✓	✓
更新	RoleAssociation	✓	✗	✗	✗
刪除	RoleAssociation	✓	✗	✗	✗
讀取	CriticalHITLTask	✓	✓	✓	✓

Action	ResourceType	管理員	核准者	作者群	ReadOnly
更新	CriticalHITLTask	✓	✓	✗	✗
刪除	CriticalHITLTask	✓	✓	✗	✗
讀取	HITLTask	✓	✓	✓	✓
更新	HITLTask	✓	✓	✓	✗
刪除	HITLTask	✓	✓	✓	✗
建立	任務	✓	✓	✓	✗
讀取	任務	✓	✓	✓	✓
更新	任務	✓	✓	✓	✗
刪除	任務	✓	✓	✓	✗
讀取	工作日誌	✓	✓	✓	✓
建立	Artifact	✓	✓	✓	✗
讀取	Artifact	✓	✓	✓	✓
更新	Artifact	✓	✓	✓	✗
刪除	Artifact	✓	✓	✓	✗
建立	連接器	✓	✓	✓	✗
讀取	連接器	✓	✓	✓	✓
更新	連接器	✓	✓	✓	✗
刪除	連接器	✓	✓	✓	✗

Human-in-the-loop(HITL) 動作

AWS 轉換提供兩種類型的 HITL 動作 - 標準和關鍵：

標準 HITL 動作

這些是可由具有貢獻者、核准者或管理員角色的使用者執行的例行動作。

關鍵 HITL 動作

這些是具有重大影響的動作，因此需要更高的許可層級。範例包括：

- 將程式碼合併至主要分支
- 執行圖形分解
- 將程式碼部署至生產環境

關鍵 HITL 動作只能由具有核准者或管理員角色的使用者執行。

為了確保 AuthZ 政策中的標準 HITL 和關鍵 HITL 動作之間存在差異， AWS Transform 提供兩個單獨的 HITL APIs，一個用於完成標準 HITL 動作，另一個用於完成關鍵 HITL 動作。

AWS 轉換環境

AWS 轉換是一種代理服務，使用自然語言處理來協助您規劃和執行工作負載轉換。您主要透過對話界面與 AWS Transform 互動，服務會根據您的討論內容進行調整和回應。例如，您可以從使用日常語言描述目前的架構和轉型目標開始，例如「我需要將我的現場部署 VMs遷移到 EC2」。

當您與 AWS Transform 對話時，服務會建置符合您特定需求的自訂任務計畫。對話流程是動態的，由您驅動，可讓您反覆精簡轉換計畫。您可以在對話期間修改任務計畫，方法是提出「在生產切換之前新增測試階段」或「移除備份步驟，因為我們已有解決方案。」 您也可以返回先前的任務並再次執行。AWS Transform 會根據您的輸入持續更新計畫，確保最終轉型策略符合您的技術與業務需求。

以下是您在開啟 AWS 轉換時看到的內容。

- 檢視控制窗格：這是 AWS 轉換左側的窄窗格。您可以選擇其中一個圖示，以選擇檢視控制窗格右側的檢視。將滑鼠游標移至每個圖示上，以取得說明檢視的工具提示。從上到下提供標準檢視如下：
  - 任務計畫
  - 儀表板
  - 核准
  - 成品
  - Worklog

  有些工作流程提供額外的檢視。

當您在任務計畫中工作時，檢視如下：

- 聊天
- 核准
- 成品存放區
- Worklog

當您在工作區時，檢視位於頂端：

- 任務
- 成品
- 協作者（使用者）
- 連接器
- 設定

- 檢視窗格位於檢視控制項旁。
- 聊天窗格位於中央。這是您與 AWS Transform 進行對話的地方。

> **Note**
>
> 具有唯讀許可的使用者無法在聊天中傳送訊息。

- 右側是協同合作窗格。這會在執行循環中的人工 (HITL) 活動時出現，例如：
  - 上傳資料檔案
  - 檢閱 AWS Transform 提供的資訊和計劃

語言設定

AWS 轉換支援特定工作流程的當地語系化。您可以選擇右上角的設定圖示，然後從語言功能表中選取您偏好的語言，以變更 Web 應用程式的顯示語言。

支援下列語言：

- 英文 (美國)
- 英文 (英國)
- Deutsch（德文）
- 西班牙文（西班牙文）

- Français （法文）
- 日本語 （日文）
- 印尼文 （印尼文）
- 義大利文 （義大利文）
- 葡萄牙文 （葡萄牙文）
- 井字遊戲 （韓文）
- 中文 （简体）（簡體中文）
- 中文 （繁體）（繁體中文）
- Türkçe （土耳其文）

下列工作流程支援當地語系化：

- 遷移 （包括 VMware)

> **Note**
>
> 其他 AWS 轉換工作流程目前僅提供英文版本。未來更新可能會新增其他工作流程的當地語系化支援。

啟動您的專案

AWS 轉換會引導您完成現代化和遷移專案。開始使用：

1. 建立工作區以託管您的專案。在工作區頁面上，選擇建立工作區。依照指示操作，然後開啟工作區。
2. 在聊天窗格中，輸入「建立任務」
3. 選擇任務，並遵循 AWS Transform 提供的指示。如果需要輸入，則會顯示協同合作窗格並說明必要項目。

工作流程彈性

AWS 轉換工作流程環境可在現代化專案的進展過程中提供彈性。在聊天窗格中使用自然語言，您可以：

- 重試 AWS 轉換已完成的任務，在整個過程中提供不同的human-in-the-loop輸入。
- 例如，如果您的現代化來源有所變更，請重新執行任務。

與 AWS 轉換聊天

AWS 轉換聊天功能可在專案的每個階段使用。若要開啟聊天，請按一下 Web 主控台右下角的紫色六邊形圖示。

此聊天可供您詢問任何問題。例如，您可以要求聊天解釋概念、引導您完成程序、解釋 AWS 轉換請求或回應，或解釋 AWS 轉換報告。

> **Note**
>
> 具有唯讀許可的使用者無法在聊天中傳送訊息。

AWS 轉換聊天整合

AWS 轉換聊天已與 整合：

以經驗為基礎的加速

以體驗為基礎的加速 (EBA) 是透過 AWS 轉換聊天提供。它可讓您針對 Windows 工作負載執行 EBA 評估，並產生計劃。您可以從 CAST 匯入評估結果開始。它可協助您探索應用程式產品組合，之後您可以使用 AWS 轉換聊天來選取符合您業務需求的應用程式（例如，根據複雜性或程式碼行篩選應用程式）。然後，您可以對選取的應用程式執行更深入的評估，並產生現代化計劃。

AWS Countdown Premium

整合到 AWS Transform 中的 AWS Countdown Premium (CDP) 提供持續的專家指導，並提供指定的 AWS 工程支援。您指定的 CDP 工程師深入探索您的技術堆疊，在發生問題時提供個人化的內容感知支援。使用者可以利用 AWS Transform 直接從其聊天介面記錄支援票證。支援票證內嵌工作日誌和工作計畫詳細資訊，以協助支援了解客戶的內容。如果客戶或合作夥伴是 CDP 計畫的一部分，支援票證會自動路由至指定的 CDP 工程師，該工程師可協助偵錯問題、解譯轉換輸出，並推動快速解決問題的進度。例如：

- 對於 .NET 工作負載，CDP 可協助處理儲存庫連接器問題、相依性解析和轉換後部署。
- 在大型主機案例中，CDP 可協助疑難排解重構的 Java 程式碼、設定資料庫遷移工具，以及建置 CI/CD 管道。

- 在 VMware 遷移中，CDP 可以加速網路組態、GN 設定和代理程式安裝。

AWS 技能建置器

AWS Skill Builder 透過聊天提供相關的學習模組。您可以詢問 AWS 轉換聊天，了解您的學習需求，並提供相關的課程目錄。Skill Builder 會在您進行轉型階段時提供情境式微型學習體驗。

AWS 轉換連接器

AWS 轉換連接器可讓您安全地跨帳戶邊界存取資源，以進行遷移和現代化工作流程。這可讓您跨帳戶邊界存取和管理資源，同時維護安全控制和許可。連接器代表已啟用 AWS 轉換的來源帳戶與 AWS 目標帳戶或第三方系統中的外部資源之間的連線。

連接器需要來自來源連接器的存取請求，以及來自目標帳戶擁有者的核准。您在設定來源連接器時提出此請求。同樣地，您可能會收到核准目的地連接器的請求，以允許其他帳戶存取您的帳戶。

- 連接器建立：在您的已啟用 AWS 轉換的來源帳戶中建立連接器，指定目標帳戶和必要的許可
- 許可設定： AWS Transform 需要目的地帳戶中的特定 IAM 角色和許可，才能執行遷移動作，包括：
  - 使用 管理遷移資料 AWS KMS
  - 進行跨區域 API 呼叫
  - 在 VMware 伺服器上安裝複寫代理程式
  - 建立網路基礎設施 VPCs、子網路、路由）
  - 啟動 Amazon EC2 執行個體和部署 CloudFormation 堆疊
  - 透過 Migration Hub 執行遷移工作流程
- 核准程序：您必須先核准目的地連接器請求， AWS 轉換才能存取您的資源。
- 作用中連線：核准連接器後，它可讓 AWS Transform 任務安全地存取和管理目標帳戶中的資源。

代理操作的使用者可追蹤性

根據預設， 會在 AWS 轉換服務身分下的 AWS 資源上 AWS CloudTrail 記錄代理程式動作。使用者可追蹤性將這些動作歸納到啟動任務或與任務互動的特定 AWS IAM Identity Center 使用者，以便在個別使用者層級進行安全稽核和事件調查。

> **Note**
>
> 僅 IAM Identity Center (IDC) 使用者支援使用者可追蹤性。

若要啟用使用者可追蹤性，請在 AWS 轉換設定檔設定中啟用背景工作階段。啟用時， AWS Transform 會在您與任務互動時自動建立 IAM Identity Center 背景工作階段，並使用它來產生連接器操作的身分增強 IAM 角色工作階段。這些工作階段會將您的使用者身分嵌入下游 AWS 服務呼叫和 AWS CloudTrail 事件。停用背景工作階段時， AWS Transform 會回到沒有使用者身分內容的標準擔任角色工作階段。

新連接器會自動設定為支援使用者可追蹤性。對於現有的連接器，您必須手動將 `sts:SetContext`新增至連接器角色的信任政策：

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

您可以從任務頁面上的背景工作階段索引標籤檢視和撤銷作用中的背景工作階段。撤銷工作階段會立即使工作階段及其衍生的任何連接器工作階段失效。

如需詳細資訊，請參閱《AWS IAM Identity Center 使用者指南》中的受信任身分傳播概觀。

管理連接器

在連接器頁面上，您可以看到：

- Source Connectors 標籤：列出您為連接到其他帳戶而建立的所有連接器，顯示目標帳戶和連接器狀態
- 目的地連接器索引標籤：顯示來自想要存取資源之其他帳戶的傳入連接器請求，並需要您的核准或拒絕

AWS 轉換需要確認關鍵動作，例如核准、拒絕或刪除連接器，以避免可能中斷作用中遷移工作流程的意外變更。

建立連接器

1. 導覽至來源連接器索引標籤。
2. 指定目標帳戶和資源類型。
3. 設定必要的許可和存取範圍。

若要設定 許可

1. 選擇建立具有必要許可的新 IAM 角色，或
2. 選取您先前為連接器建立的現有角色。
3. 確保角色具有 AWS 轉換操作的所有必要許可。

管理傳入請求

1. 在目的地連接器索引標籤中檢閱連接器請求。
2. 核准合法請求以啟用跨帳戶存取。
3. 拒絕未經授權或不必要的連線嘗試。

管理您的連接器

1. 監控作用中連接器的安全性和合規性。
2. 當您不再需要連接器時，請刪除連接器。請注意，這會導致使用連接器執行中的任務失敗。
3. 在您的需求變更時更新許可。

開發人員工具

您可以從代理程式 IDEs、代理程式外掛程式和 MCP 伺服器存取 AWS Transform 代理程式。選擇適合您工作流程的表面。

> **Note**
>
> Kiro Power 和代理程式外掛程式會自動安裝 MCP 伺服器。只有在您想要在沒有 Kiro Power 或代理程式外掛程式的情況下使用 MCP 伺服器時，才需要手動安裝。

Kiro Power

AWS Transform Kiro Power 提供從 Kiro IDE AWS 轉換代理程式的完整存取權。

安裝 AWS Transform Kiro Power

1. 開啟 Kiro IDE 並導覽至 Powers 面板。
2. 在清單中尋找AWS 轉換並安裝它。
3. 開啟 Kiro Chat，按一下電源，然後選取嘗試電源。

或者，在 Powers 面板中，選擇新增自訂電源 > 從 GitHub 匯入電源並貼上： `https://github.com/kirodotdev/powers/tree/main/aws-transform`

代理程式外掛程式

AWS 轉換代理程式外掛程式可在 GitHub 的 `plugins/aws-transform`目錄中的 awslabs/agent-plugins 取得。外掛程式支援 Claude Code、Codex 和 Cursor。

外掛程式包含 `.claude-plugin`、 `.codex-plugin`和 `.mcp.json`組態。它可讓您存取所有 AWS 轉換代理程式，例如 .NET、大型主機、VMware、SQL Server 和自訂轉換。

在 Claude Code 中安裝

執行下列命令：

```
/plugin marketplace add awslabs/agent-plugins
```

```
/plugin install aws-transform@agent-plugins-for-aws
```

在 Codex 或 Cursor 中安裝

遵循代理程式外掛程式儲存庫 README 中的指示。

IDE 外掛程式

AWS 轉換 IDE 外掛程式可在 VS 程式碼和 Open VSX 相容編輯器上使用。它公開 AWS 了轉換自訂功能，包括建立和執行轉換定義。它還公開了大型主機功能，包括現代化要求、業務規則和原始程式碼之間的可追蹤性，以及隨需產生技術文件的能力。若要開始使用，請使用下列其中一種方法安裝 ：

- VS 程式碼：從 VS Code Marketplace 安裝 。
- Open VSX：從 Open VSX 登錄檔安裝 。

MCP 伺服器

使用 MCP 伺服器以程式設計方式將 AWS 轉換與任何 MCP 相容用戶端整合。您可以從 PyPI 安裝 MCP 伺服器做為 `awslabs.aws-transform-mcp-server`。它提供 19 個工具，用於工作區管理、任務管理、human-in-the-loop(HITL) 任務、成品處理、連接器管理、聊天和資源瀏覽。

先決條件

- Python 3.10 或更新版本

安裝

Claude 程式碼

```
claude mcp add awslabs.aws-transform-mcp-server -- uvx awslabs.aws-transform-mcp-
server@latest
```

開羅

新增至 `~/.kiro/settings/mcp.json`：

```
{
```

```
  "mcpServers": {
    "awslabs.aws-transform-mcp-server": {
      "command": "uvx",
      "args": ["awslabs.aws-transform-mcp-server@latest"]
    }
  }
}
```

如需特定 MCP 用戶端的組態詳細資訊，請參閱 GitHub 上的 aws-transform-mcp-server README。

身分驗證

AWS 轉換支援 SSO (AWS Identity and Access Management 身分中心） 和 IAM 角色型身分驗證。

SSO (IAM Identity Center)

請您的 AI 助理「使用 SSO 設定 AWS 轉換」。助理會提供開始 URL，並開啟瀏覽器以進行登入。

IAM 角色

您的環境會自動提供 AWS 登入資料。在 MCP 用戶端組態env區塊AWS_PROFILE中設定 ，以選取特定設定檔。

如需設定 AWS 轉換身分驗證的資訊，請參閱 AWS 轉換入門。

建置 AWS 轉換的自訂代理程式

客服人員建置器工具組可讓 AWS 合作夥伴和客戶針對其在 AWS Transform 中運作的特定現代化需求，建置量身打造的客服人員。

安裝代理程式建置器工具組

1. 開啟 Kiro IDE 並導覽至 Powers 面板。
2. 在清單中尋找 AWS Transform Agent Toolkit 並安裝它。

或者，在 Powers 面板中，選擇新增自訂電源 > 從 GitHub 匯入電源並貼上： `https://github.com/kirodotdev/powers/tree/main/aws-transform-agent-toolkit`

代理程式建置器工具組可讓遷移和現代化能力合作夥伴、ISVs或客戶針對特定使用案例建立轉換解決方案。您可以將專門的代理程式、工具、知識庫和工作流程與 AWS Transform agentic AI 功能整合。

客服人員生命週期

建置

使用 Kiro Power 結合基本代理程式和 SDK 來撰寫您自己的自訂代理程式。

Share (分享)

將客服人員與團隊或跨合作夥伴網路分發。

登錄

向 AWS Transform 註冊代理程式以供其他使用者探索。

Custom

什麼是 AWS 轉換自訂？

AWS 轉換自訂使用代理式 AI 對軟體、程式碼、程式庫和架構執行大規模現代化，以減少技術負債。它處理各種案例，包括語言版本升級、API 和服務遷移、架構升級和遷移、程式碼重構，以及組織特定的轉換。

透過持續學習，代理程式會從每個執行和開發人員意見回饋中改進，提供高品質、可重複的轉換，而無需專業自動化專業知識。

關鍵功能

AWS 轉換自訂提供下列功能：

- 自然語言驅動的轉換定義 - 使用自然語言、文件和程式碼範例建立自訂轉換
- 轉換執行 - 在多個程式碼庫中一致且可靠地套用轉換
- 持續學習 - 自動改善每次執行的轉換品質
- AWS受管轉換 - 針對常見案例使用ready-to-use AWS、經過審核的轉換

轉換模式

AWS 轉換自訂支援各種轉換模式，以滿足您的現代化需求。根據所需變更的範圍和性質，每個模式都有不同的複雜性特性。

模式	說明	複雜性	範例
API 和服務遷移	在 API 版本或同等服務之間遷移，同時維護功能	中	AWS SDK v1→v2 (Java、Python、JavaScript)、Boto2→Boto3、JUnit 4→5、javax→jakarta
語言版本升級	升級到相同程式設計語言的較新版本，採	中低	Java 8→17、Python 3.9→3.13、Node.js

模式	說明	複雜性	範例
	用新功能並取代已取代的功能		12→22、TypeScript 版本升級
架構升級	升級到相同架構的較新版本，解決重大變更	中	Spring Boot 2.x→3.x、React 17→18、角度升級、Django 升級
架構遷移	遷移至具有類似目的的完全不同架構	高	Angular→React、Redux→Zustand、Vue.js→React
程式庫和相依性升級	將第三方程式庫升級至較新版本，同時維護相同的語言和架構	中低	Pandas 1.x→2.x、NumPy 升級、Hadoop/HBase/Hive 程式庫升級、Lodash 升級
程式碼重構和模式現代化	現代化程式碼模式並採用最佳實務，而不變更外部功能	中低	Print→Logging 架構、字串串連→f-strings、類型提示採用、可觀測性檢測
指令碼和File-by-File轉譯	翻譯獨立指令碼或組態檔案，其中檔案大部分是獨立的	中低	AWS CDK→Terraform、Terraform→CloudFormation、Excel→Python 筆記本、Bash→PowerShell
架構遷移	以最少的程式碼變更在硬體架構或執行期環境之間遷移	中高	x86→AWS Graviton (ARM)、內部部署→Lambda、傳統伺服器→容器

模式	說明	複雜性	範例
Language-to-Language遷移	將程式碼庫從一種程式設計語言轉譯為另一種程式設計語言	非常高	Java→Python、JavaScript→TypeScript、C→Rust、Python→Go
自訂和組織特定轉換	獨特的組織需求和專業現代化需求	各有不同	自訂內部程式庫遷移、組織特定的編碼標準、專屬架構遷移

> **Note**
>
> 對於 COBOL/大型主機語言，請使用適用於大型主機的 AWS Transform。對於升級至 .NET Core 的 .NET Framework，請考慮 AWS Transform for Windows。對於 VMware 遷移到 AWS，請考慮 AWS Transform for VMware。

AWS 轉換自訂的運作方式

AWS 轉換自訂通常用於轉換多個程式碼庫或模組的大規模專案。團隊通常會遵循四階段工作流程：

定義轉換 - 提供自然語言提示、文件和程式碼範例給代理程式，以產生初始轉換定義。此定義可以透過聊天或直接編輯反覆改進。使用 AWS受管轉換時，可以略過此階段。

試行或Proof-of-Concept- 在範例程式碼庫上測試轉換，並根據結果進行精簡。此驗證階段有助於預估完整轉換的成本和工作量。在此階段中，持續學習可改善品質。

擴展執行 - 使用 CLI 設定自動大量執行，讓開發人員檢閱和驗證結果。使用 Web 應用程式監控進度，並追蹤跨多個儲存庫的轉換。

監控和檢閱 - 持續學習會自動改善轉換品質。檢閱從先前執行中擷取的教訓，以確保它們符合品質標準，並封存任何沒有用的內容。

了解 的核心概念

本節說明使用 AWS 轉換自訂的重要概念。

轉換定義

轉換定義包含執行特定程式碼轉換所需的指示和知識。它以技能表示，並由以下項目組成：

- `SKILL.md`（必要）- Markdown 中包含核心轉換邏輯和執行指示的 YAML 前綴 (`name` 和 `description` 欄位）的指示
- `references/` 資料夾（選用）- 在轉換執行期間視需要載入的文件
- `scripts/` 資料夾（選用）- 轉換在執行期間下載和執行的指令碼

AWS 轉換 CLI 會在執行、檢查或修改需要時，自動將轉換定義下載到目前的目錄。

> **Important**
>
> 發佈轉換時，目錄必須僅包含 `SKILL.md`，也可以包含 `references/` 資料夾、 `scripts/` 資料夾或兩者。不允許其他檔案或子目錄。

> **Note**
>
> CLI 2.0 版和更新版本使用技能格式。CLI 會自動處理現有的轉換定義。

轉換登錄檔

轉換登錄檔是您 AWS 帳戶的集中式儲存庫，用於儲存和管理轉換定義。登錄檔中的轉換可以是：

- 使用 列出 `atx custom def list`
- 在多個程式碼庫中執行
- 與您 AWS 帳戶中的其他使用者共用
- 版本控制

> **Important**
>
> 轉換定義是帳戶特定的。如果您想要在不同帳戶中使用轉換 AWS ，則必須在該帳戶中單獨發佈轉換。

草稿與發佈的轉換

AWS 轉換自訂支援在登錄檔中轉換的兩種狀態：

草案轉換是進行中或未測試的轉換定義。它們會儲存為特定版本，並由參考該特定版本的使用者擷取、更新和執行。在準備與您的團隊共用轉換之前，草稿對於反覆開發、測試和改進很有用。草稿也會與特定對話相關聯。如果您重新啟動 CLI，您可以使用 `atx --conversation-id {id}`還原先前的 CLI。

已發佈的轉換可在您帳戶的轉換登錄檔中使用，以供具有所需 IAM 許可的其他使用者執行。您可以使用 探索已發佈的轉換`atx custom def list`。

典型的工作流程是：

1. 在本機建立轉換
2. 儲存為草稿以供測試 (`atx custom def save-draft`)
3. 精簡和驗證
4. 發佈以與您的團隊共用 (`atx custom def publish`)

您也可以直接發佈轉換，而無需將其儲存為草稿。

參考與課程

AWS 轉換自訂使用兩種類型的知識來改善轉換品質：

參考是使用者提供的文件，存放在轉換定義的 `references/` 資料夾中。參考僅支援文字檔案 （所有檔案總計最多 10MB)，通常包含文件、API 規格、遷移指南和程式碼範例。轉換執行期間會視需要載入參考。在互動式模式下建立或更新轉換定義時，您可以新增參考。

課程會自動從先前的轉換執行中擷取。持續學習系統會從轉換期間遇到的執行軌跡、開發人員意見回饋和程式碼修正產生它們。它會將相關課程分組為類別，以便您可以一起檢閱。與預先提供的參考不同，當您跨不同程式碼庫執行轉換時，課程會隨著時間累積，而系統會自動套用它們來改善未來的執行。您可以使用 以互動方式檢閱和管理課程`atx custom def learnings`。

組建和驗證命令

組建或驗證命令是選用參數，指定如何在轉換過程中驗證您的程式碼。此命令會在轉換期間的不同時間點執行，以確保程式碼完整性。

提供命令來驗證結果，並在驗證失敗時傳回問題，對於透過持續學習改善轉型品質非常重要。如果不需要建置或驗證，請從輸入中省略 。

如需範例和詳細指引，請參閱工作流程區段中的建置和驗證命令。

持續學習

持續學習是一種系統，可自動擷取每個轉換執行的意見回饋，並隨著時間改善轉換品質。系統會透過下列方式收集資訊：

- 明確意見回饋 - 互動式模式中提供的評論和程式碼修正
- 隱含觀察 - 代理程式在轉換和偵錯程式碼時遇到的問題

持續學習系統會處理此資訊，以建立新增至轉換定義的課程，以改善未來的轉換。系統會在轉換完成後自動執行學習程序，不需要您提供其他輸入。

> **Important**
>
> 課程是轉換特定的，不會在不同轉換或不同的客戶帳戶之間共用。

管理課程

系統會自動產生課程，但您可以控制哪些課程會套用至未來的執行。`atx custom def learnings` 命令會開啟互動式終端機工作階段，以檢閱和策劃轉換累積的教訓。

在此工作階段中，您可以：

- 瀏覽分組為類別的課程，並查看每個類別包含多少個作用中課程。
- 開啟一個課程來閱讀其完整詳細資訊，包括課程內文、其影響，以及之前所參考的執行次數。
- 封存課程，以防止系統將其套用至未來的執行，並視需要稍後還原。
- 永久刪除不再有用的封存課程。

如需逐步說明，請參閱 the section called “持續學習”。

用戶端技能

用戶端技能是在轉換執行期間擴展代理程式的額外功能。與定義要執行哪些轉換的轉換定義不同，用戶端技能提供代理程式可在任何轉換期間與其內建功能搭配使用的補充工具、指令碼和指示。

從專案層級和使用者層級目錄探索用戶端技能。將技能放在專案層級，當它們強制執行特定於儲存庫的標準時，將技能放在使用者層級，當它們套用於您的所有專案時。只有在提供程式碼儲存庫路徑時，才能使用專案層級技能。如需詳細的組態和用量，請參閱 the section called “用戶端技能”。

開始使用

本節說明如何設定 AWS 轉換自訂並執行您的第一個轉換。

先決條件

安裝 AWS 轉換自訂之前，請確定您有下列項目：

支援的平台

AWS 轉換自訂支援下列作業系統：

- Linux - 全面支援所有 Linux 發行版本
- macOS - macOS 系統的完整支援
- Windows - 使用 Windows Terminal 和 PowerShell 完整支援原生 Windows (Windows 尚未支援這些`atx ct`命令)
- 適用於 Linux 的 Windows 子系統 (WSL) - 在 WSL 下執行時支援

必要軟體

- Node.js 22 或更新版本 - 從 https：//https://nodejs.org/en/download 下載
- Git - 必須安裝，且工作目錄必須是有效的 Git 儲存庫才能執行轉換。執行 `git init; git add .; git commit -m "Initial commit"`以在工作目錄中初始化 Git 儲存庫。

網路要求

需要可存取下列端點的網際網路連線：

- `transform-cli.awsstatic.com`
- `transform-custom.<region>.api.aws`
- `*.s3.amazonaws.com`

如果您在網際網路受限的環境中工作，請更新防火牆規則以允許列出這些 URLs。

安裝 AWS 轉換 CLI

建議的安裝方法使用 安裝指令碼。選擇作業系統的索引標籤。

安裝 AWS 轉換 CLI

1. 執行安裝指令碼：

   Linux and macOS

   ```
   curl -fsSL https://transform-cli.awsstatic.com/install.sh | bash
   ```

   Windows (PowerShell)

   在原生 Windows 上，使用 PowerShell 從 Windows 終端機執行安裝指令碼。

   ```
   irm https://transform-cli.awsstatic.com/install.ps1 | iex
   ```

2. 驗證安裝：

   ```
   atx --version
   ```

   命令應會顯示 AWS Transform CLI 的安裝版本。

設定身分驗證

AWS 轉換自訂需要 AWS 登入資料，才能使用 服務進行驗證。使用下列其中一種方法設定身分驗證。

環境變數

設定下列環境變數。

Linux and macOS

```
export AWS_ACCESS_KEY_ID=your_access_key
export AWS_SECRET_ACCESS_KEY=your_secret_key
export AWS_SESSION_TOKEN=your_session_token
```

Windows (PowerShell)

```
$env:AWS_ACCESS_KEY_ID="your_access_key"
```

```
$env:AWS_SECRET_ACCESS_KEY="your_secret_key"
$env:AWS_SESSION_TOKEN="your_session_token"
```

您也可以使用 AWS_PROFILE環境變數指定設定檔。

Linux and macOS

```
export AWS_PROFILE=your_profile_name
```

Windows (PowerShell)

```
$env:AWS_PROFILE="your_profile_name"
```

> **Note**
>
> 在 PowerShell $env:中使用 設定的環境變數僅適用於目前的工作階段。
> 若要跨工作階段保留它們，請透過系統屬性 > 環境變數進行設定，或使用
> [System.Environment]::SetEnvironmentVariable()。

AWS 登入資料檔案

在登入資料檔案中設定 AWS 登入資料，位於 Linux 和 macOS ~/.aws/credentials 上的 或 Windows %USERPROFILE%\.aws\credentials上的 ：

```
[default]
aws_access_key_id = your_access_key
aws_secret_access_key = your_secret_key
```

IAM 許可

您的 AWS 登入資料必須具有呼叫 AWS 轉換自訂服務的許可。建議您將 AWSTransformCustomFullAccess AWS 受管政策連接至 IAM 使用者或角色。此政策提供 AWS 轉換自訂的完整存取權，包括建立 CloudWatch 指標傳送至您的帳戶所需的服務連結角色的許可。

如需更精細的控制， AWS Transform 自訂也提供下列 AWS 受管政策：

- AWSTransformCustomExecuteTransformations – 提供執行轉換的存取權。

- AWSTransformCustomManageTransformations – 提供建立、更新、讀取和刪除轉換資源的存取權，以及執行轉換。

如需這些政策的詳細資訊，請參閱 AWSAWS Transform 的 受管政策。如需具有資源層級許可的自訂 IAM 政策，請參閱 AWS 轉換自訂 IAM 服務授權參考指南。

> **Note**
>
> - 轉換定義是具有 ARNs(Amazon Resource Name) AWS 的資源。您可以使用 IAM 政策，在 IAM 政策資源陳述式中指定轉換 ARN，以控制對特定轉換或轉換群組的存取。標籤可用於分組存取控制。
> - AWS 存取 AWS 轉換需要 IAM Identity Center，但使用 CLI 不需要。

設定 AWS 區域

AWS 轉換自訂可在特定 AWS 區域使用，並使用標準 CLI AWS 優先順序自動偵測您的區域組態。

支援的區域

AWS 轉換自訂可在下列 AWS 區域使用：

- us-east-1（美國東部 - 維吉尼亞北部）
- eu-central-1（歐洲 - 法蘭克福）
- eu-west-2（歐洲 - 倫敦）
- ca-central-1（加拿大 - 中部）
- ap-northeast-1（亞太區域 - 東京）
- ap-northeast-2（亞太區域 - 首爾）
- ap-southeast-2（亞太區域 - 雪梨）
- ap-south-1（亞太區域 - 孟買）

區域如何決定

CLI 會依優先順序檢查這些來源，以決定要使用的區域：

1. AWS_REGION 環境變數（最高優先順序）
2. AWS_DEFAULT_REGION 環境變數
3. 組態檔案中選取的設定檔 AWS （透過AWS_PROFILE環境變數）
4. AWS 組態檔案中的預設設定檔
5. us-east-1 如果找不到組態，預設回復至

> **Note**
>
> 組態檔案位於 Linux AWS 和 macOS ~/.aws/config 上的 ，或 Windows %USERPROFILE%\.aws\config上的 。

> **Note**
>
> 如果ATX_CUSTOM_ENDPOINT已設定 ，則會從端點 URL 擷取區域，並覆寫所有其他設定。

設定您的區域

選擇下列其中一種方法來設定您的區域：

選項 1：環境變數（建議暫時使用）：

Linux and macOS

```
export AWS_REGION=<your-region>
```

Windows (PowerShell)

```
$env:AWS_REGION="<your-region>"
```

選項 2： AWS CLI 組態（建議永久設定）：

```
aws configure set region <your-region>
```

選項 3：設定檔特定的組態：

Linux and macOS

```
aws configure set region <your-region> --profile your_profile_name
export AWS_PROFILE=your_profile_name
```

Windows (PowerShell)

```
aws configure set region <your-region> --profile your_profile_name
$env:AWS_PROFILE="your_profile_name"
```

選項 4：直接檔案編輯：

直接編輯組態檔案 AWS (`~/.aws/config`在 Linux 和 macOS 上，或在 Windows `%USERPROFILE%\.aws\config`上）：

```
[default]
region = <your-region>

[profile your_profile_name]
region = <your-region>
```

驗證您的區域組態

若要檢查 AWS 轉換自訂將使用的區域：

檢查目前的區域設定：

```
aws configure get region
```

檢查環境變數：

Linux and macOS

```
echo "AWS_REGION: $AWS_REGION"
echo "AWS_DEFAULT_REGION: $AWS_DEFAULT_REGION"
echo "AWS_PROFILE: $AWS_PROFILE"
```

Windows (PowerShell)

```
echo "AWS_REGION: $env:AWS_REGION"
```

```
echo "AWS_DEFAULT_REGION: $env:AWS_DEFAULT_REGION"
echo "AWS_PROFILE: $env:AWS_PROFILE"
```

在偵錯日誌中檢視詳細的區域解析：

Linux and macOS

```
tail -f ~/.aws/atx/logs/debug.log
```

Windows (PowerShell)

```
Get-Content "$env:USERPROFILE\.aws\atx\logs\debug.log" -Wait -Tail 10
```

顯示區域來源的日誌輸出範例：

```
2026-01-07 22:34:28 [DEBUG]: Initializing FrontendServiceClient with config:
{
  "endpoint": "https://transform-custom.us-east-1.api.aws",
  "region": "us-east-1",
  "regionSource": "AWS_REGION"
}
```

`regionSource` 欄位顯示區域衍生自何處（例如 "aws-config (profile：default)"、"AWS_REGION"、"default")。

> **Important**
>
> 如果您的區域組態指向不支援的區域，CLI 會顯示明確的錯誤訊息，其中包含將組態更新為支援區域的指示。

執行您的第一個轉換

開始使用的最快方法是使用 AWS受管轉換。 AWS受管轉換是預先建置、經過 AWS審核的轉換，無需任何設定即可使用。

若要以互動方式執行受 AWS管轉換：

```
atx
```

然後要求代理程式執行轉換：

```
Execute the AWS/java-aws-sdk-v1-to-v2 transformation on the codebase at ./my-java-
project
```

若要以非互動方式執行轉換：

```
atx custom def exec -n AWS/java-aws-sdk-v1-to-v2 -p ./my-java-project -c "mvn clean
 install" -x -t
```

如需執行模式、組態選項和命令旗標的詳細資訊，請參閱 the section called “命令參考”。

了解轉換結果

當轉換完成時， AWS Transform 自訂會提供描述結果的報告。如果轉換未經過驗證 （例如，Java 應用程式的成功建置），則報告會提供進一步動作的建議。

大多數轉換都會以多個步驟執行，使用 Git 遞交中繼轉換。您可以使用標準 Git 命令檢閱轉換所做的變更：

```
git status
git log
git diff <original commit-id>
```

建立自訂轉換

當 AWS受管轉換不符合您的需求時，您可以根據特定需求建立自訂轉換。

建立自訂轉換

1. 在互動式模式下啟動 AWS 轉換 CLI：

   ```
   atx
   ```

2. 告訴客服人員您要建立新的轉換，並描述您的需求。
3. 提供參考資料，例如文件和程式碼範例，以改善品質。

4. 反覆測試和精簡轉換。
5. 將其發佈到組織的轉換登錄檔。

如需建立自訂轉換的詳細說明，請參閱 the section called “工作流程”。

AWS 轉換 Web 應用程式 （選用）

AWS 轉換 Web 應用程式是選擇性的界面，用於監控跨多個儲存庫的大規模轉換行銷活動。在使用 AWS 轉換 Web 應用程式之前，您需要啟用使用者身分才能存取組織中的 AWS 轉換。如需啟用 AWS 轉換的相關資訊，請參閱設定 AWS 轉換。

若要使用 AWS 轉換 Web 應用程式：

1. 請造訪 https://aws.amazon.com/transform/：// 並使用 AWS IAM Identity Center 登入資料登入。
2. 在 AWS 轉換 Web 應用程式中選取「自訂/程式碼」任務類型。
3. 告訴客服人員您要使用的轉換定義名稱。
4. Web 應用程式提供 AWS Transform CLI 命令，可與您的團隊共用。此命令會叫用轉換定義，並將執行結果記錄到 Web 應用程式。
5. 擷取轉換結果後，請在儀表板中檢視統計資料、節省時間測量，並詢問任務進度的問題。

Web 應用程式專為企業規模操作而設計，您需要集中監控跨多個程式碼庫的轉換。

> **Note**
>
> AWS 存取 AWS Transform Web 應用程式需要 IAM Identity Center。CLI 不需要 IAM Identity Center - 只需要標準 AWS 登入資料。

自訂轉換命令簡介

以下是您可以搭配自訂轉換使用的幾個命令。命令的完整清單位於AWS 轉換自訂轉換命令參考中。

- `atx custom`
  - 執行自訂轉換互動式體驗，允許建立、探索、執行和改善轉換。
  - 這是 的預設命令`atx`。

  - `--trust-all-tools (-t)` 是選用的，並隱含地允許代理程式提出所有請求的工具請求。請謹慎使用，尤其是在生產環境中。您可以使用信任設定檔案，為特定工具和命令設定工具信任。
- `atx custom --help | atx custom -h`
  - 顯示說明選單。
  - 每個命令也包含說明功能表，例如 `atx custom def exec --help`。
- `atx --version | atx -v`
  - 顯示版本。
  - 版本編號會隨每個版本而變更。
- `atx custom def list`
  - 列印轉換登錄檔中可用的轉換清單。
- `atx custom def exec`
  - 執行轉換
- `atx custom def learnings`
  - 開啟互動式工作階段，以檢視和管理轉換從先前執行中學到的經驗教訓
- `atx mcp`
  - 用來管理 MCP 伺服器組態

工作流程

執行轉換

本節說明執行轉換的不同方式，以及控制執行行為的選項。

執行模式

AWS 轉換自訂支援三種執行模式，以適應不同的工作流程。

互動式對話模式

使用 啟動 CLI，`atx`並要求代理程式透過自然語言執行轉換。此模式可讓您與客服人員進行完整對話、隨時中斷執行，並在轉換過程中提供意見回饋。

當您想要獲得最大控制，以及能夠引導客服人員完成複雜案例時，請使用此模式。

直接互動式執行

使用 atx custom def exec -n <transformation-name> -p <path> 以互動方式啟動特定轉換。此模式可讓您在執行開始時、期間或結束時，檢閱代理程式並與之互動。客服人員將在關鍵決策點暫停，並詢問您的輸入。

這非常適合在自動執行轉換之前進行測試和精簡轉換。

您可以在非互動式模式或無周邊模式下執行轉換。非互動式模式會在具名轉換期間隱藏提示。無頭模式可讓您使用純文字提示執行代理程式，完全略過互動式界面。

非互動式模式

使用 atx custom def exec -n <transformation-name> -p <path> -x -t 進行完整自動化。新增 -t -x以在非互動式模式下執行，並在不提示的情況下自動信任所有工具。

此模式專為 CI/CD 管道整合和大量執行而設計，其中沒有可用的人工介入或不需要人工介入。

無周邊模式

若要在不與代理程式互動的情況下完成任務，請以純文字執行atx -x "<prompt>" -t並提供您的指示。

無周邊轉換執行

使用此模式將現有的轉換定義套用至您的程式碼庫。轉換會自動執行每個步驟，而不需要您的核准。

```
atx -x "apply transformation definition <transformation_definition_name> to
 <codebase_path>" -t
```

無周邊轉型開發

建立或修改轉換定義。

若要將舊版轉換定義轉換為新的技能格式 (SKILL.md：// + references/)，請執行下列命令：

```
atx -x "convert <legacy_transformation_definition_name> transformation definition to
 skill and save as draft" -t
```

若要建立新的轉換定義，請執行下列命令：

```
atx -x "create a transformation definition to <description> with references docs
 <reference_docs_path>" -t
```

常見命令旗標

使用 執行轉換時`atx custom def exec`，通常會使用下列旗標：

- `-n` 或 `--transformation-name` - 指定要執行的轉換名稱
- `-p` 或 `--code-repository-path` - 指定程式碼庫的路徑 （目前目錄使用 "."）
- `-c` 或 `--build-command` - 指定要執行的建置或驗證命令
- `-x` 或 `--non-interactive` - 啟用非互動式模式 （無使用者提示）
- `-t` 或 `--trust-all-tools` - 自動信任所有工具而不提示
- `-d` 或 `--do-not-learn` - 防止從此執行中擷取經驗教訓
- `--tv` 或 `--transformation-version` - 指定轉換的特定版本
- `-g` 或 `--configuration` - 提供組態檔案或內嵌組態

> **Important**
>
> `-t` 或 `--trust-all-tools`旗標會自動核准所有工具執行，而不會提示並略過大多數的安全防護機制 （除非 覆寫，否則符合您`alwaysPromptCommands`清單的命令仍需要明確許可`trustedShellCommands`)。完全自主的體驗需要傳入 `--trust-all-tools --non-interactive`和 ，但執行轉換不需要。在生產環境中謹慎使用 。

使用組態檔案

AWS 轉換自訂支援 YAML 或 JSON 格式的選用組態檔案。組態檔案可讓您指定執行參數，並提供其他內容給代理程式。

若要使用組態檔案：

```
atx custom def exec --configuration file://config.yaml
```

您也可以將組態提供為內嵌索引鍵/值對：

```
atx custom def exec --configuration "key=value,key2=value2"
```

範例組態檔案 (config.yaml)：

```
codeRepositoryPath: ./my-project
transformationName: my-transformation
buildCommand: mvn clean install
additionalPlanContext: |
  The target Java version to upgrade to is Java 17.
  Ensure compatibility with our internal logging framework version 2.3.
validationCommands: |
  mvn test
  mvn verify
```

additionalPlanContext 參數為代理程式的執行計畫提供額外的內容。這對於 AWS受管轉換特別有用，可根據您的特定需求自訂其行為。

組建和驗證命令

建置或驗證命令是選用參數，指定如何在轉換過程中驗證您的程式碼。如果未指定， AWS 轉換自訂會嘗試根據轉換推斷最佳建置命令，但建議針對品質指定。

建置和驗證命令的範例：

- Java： `mvn clean install` 或 `gradle build`
- Python： `pytest` 或 `python -m py_compile`
- Node.js： `npm run build`或 `npm test`
- Linters： `eslint .` 或 `pylint .`

即使對於不需要建置的語言或轉換，提供驗證結果的命令，並在驗證失敗時傳回問題，對於改善轉換品質非常重要。

如果不需要建置或驗證，請從輸入中省略 。

控制學習行為

根據預設， AWS Transform 自訂會從每個轉換執行中擷取課程。您可以防止學習特定執行。

若要防止從執行中學習：

```
atx custom def exec -n my-transformation -p ./my-project -d
```

-d 或 --do-not-learn標記選擇退出允許從目前執行中擷取課程。

繼續對話

AWS 轉換自訂可讓您在建立後的 30 天內繼續先前的對話。

若要繼續最近的對話：

```
atx --resume
```

若要繼續特定對話：

```
atx --conversation-id <conversation-id>
```

> **Important**
>
> 對話只能在建立後的 30 天內恢復。30 天後，就無法再繼續對話。

追蹤代理程式分鐘

AWS 轉換自訂會追蹤轉換工作階段期間使用的客服人員分鐘數。客服人員分鐘會累積到整個對話生命週期，並在對話結束時顯示：

```
Agent minutes used: 12.50
```

客服人員分鐘會在中斷期間持續存在。如果您使用 Ctrl+C 中斷工作階段並稍後繼續，則先前累積的分鐘會繼續累積在繼續的工作階段中。

若要在互動式工作階段期間檢查客服人員分鐘數：

`/usage` 在輸入提示中輸入 ，以顯示目前累積的客服人員分鐘，而不結束對話。

若要設定客服人員分鐘預算限制：

```
atx custom def exec -n my-transformation -p ./my-project --limit 30
```

`--limit` 選項會設定工作階段的客服人員分鐘預算上限。客服人員分鐘反映作用中的客服人員工作時間，而不是牆上時鐘時間。達到限制時，CLI 會顯示訊息並結束，其中包含繼續的指示：

```
## Budget limit reached: 30.00 / 30.00 Agent Minutes. Exiting.
```

您可以稍後以更高的限制繼續對話：

```
atx --conversation-id <conversation_id> -t --limit <increased_limit>
```

持續學習

本節說明如何檢閱和管理持續學習所建立的課程。

了解 課程

持續學習系統會自動從先前的轉換執行中擷取經驗教訓。系統會根據下列項目以非同步方式建立它們：

- 在互動式模式中提供的開發人員意見回饋
- 轉換期間遇到的程式碼問題

當您跨不同的程式碼庫執行轉換時，課程會隨著時間累積。系統會自動套用它們來改善未來的執行。每個課程都屬於一個類別，其中包含類似網域的所有課程，因此您可以一起檢閱相關課程。對於您不想使用的課程，您可以完全封存或刪除該課程。

檢視和管理課程

使用 `learnings`命令開啟互動式工作階段，以瀏覽和管理轉換定義的課程。

若要開啟課程檢視器：

```
atx custom def learnings -n my-transformation
```

檢視器會在課程類別清單上開啟，每個類別都會顯示其中包含多少個作用中課程。選取類別以查看其教訓，然後選取一個教訓以檢視其完整詳細資訊，包括課程內文、其影響，以及之前所參考的執行次數。

封存和還原課程

系統會自動套用課程。如果您不希望系統套用課程，您可以將其封存。系統會保留封存的課程，但不會將其套用至未來的執行。所有封存的課程都會分組在一起，因此您可以檢閱它們，並將任何 還原為作用中使用。

刪除課程

永久移除沒有幫助的課程。刪除無法復原，系統可能會從未來的執行中重新學習已刪除的課程。

必須先封存課程，才能將其刪除。

進階組態

本節說明 AWS 轉換自訂的進階功能和組態選項。

環境變數

您可以使用環境變數自訂 CLI 行為。

> **Note**
>
> 下列範例顯示 Linux 和 macOS 語法 (`export`)。在 Windows 上，使用 在 PowerShell 中設定環境變數`$env:NAME="value"`。如需同等命令，請參閱 Windows (PowerShell) 索引標籤。

ATX_SHELL_TIMEOUT

覆寫 Shell 命令的預設逾時 (900 秒/15 分鐘）。

Linux and macOS

```
export ATX_SHELL_TIMEOUT=1800  # 30 minutes
```

Windows (PowerShell)

```
$env:ATX_SHELL_TIMEOUT=1800  # 30 minutes
```

這適用於大型程式碼庫或長時間執行的建置程序。

ATX_DISABLE_UPDATE_CHECK

在命令執行期間停用自動版本檢查和更新通知。

Linux and macOS

```
export ATX_DISABLE_UPDATE_CHECK=true
```

Windows (PowerShell)

```
$env:ATX_DISABLE_UPDATE_CHECK="true"
```

ATX_GIT_COMMITTER_NAME 和 ATX_GIT_COMMITTER_EMAIL

設定轉換自訂在 AWS 轉換期間套用變更時，在儲存庫中建立的檢查點遞交所使用的作者身分。未設定這些變數時，檢查點遞交會歸因於預設身分 (ATX Bot <checkpoint@atx.bot>)。將兩個變數設定為將檢查點屬性設為特定作者。

Linux and macOS

```
export ATX_GIT_COMMITTER_NAME="Jane Developer"
export ATX_GIT_COMMITTER_EMAIL="jane@example.com"
```

Windows (PowerShell)

```
$env:ATX_GIT_COMMITTER_NAME="Jane Developer"
$env:ATX_GIT_COMMITTER_EMAIL="jane@example.com"
```

信任設定

信任設定可讓您預先核准特定工具和命令，無需提示即可執行。您也可以要求特定 shell 命令的明確許可，無論信任層級為何。這些設定是在 `~/.aws/atx/trust-settings.yaml` 檔案中設定。

檔案包含三個清單：

- `trustedTools` - 可在不提示的情況下執行的工具
- `trustedShellCommands` - 可在不提示的情況下執行的 Shell 命令
- `alwaysPromptCommands` - 需要明確許可的 Shell 命令模式`trustedShellCommands`，除非 覆寫，無論`-t`旗標或工作階段信任為何。這些模式不會在非互動式模式中強制執行 (`-x`)。

預設信任的工具：

- `file_read`
- `get_transformation_from_registry`

- `list_available_transformations_from_registry`

編輯信任設定：

您可以手動編輯 trust-settings.yaml 檔案，以新增或移除信任的工具和命令。`trustedShellCommands` 和 都`alwaysPromptCommands`支援使用 的 glob 萬用字元模式*。

> **Note**
>
> 如果命令符合這兩個清單，`trustedShellCommands`會優先處理。

以下說明每個命令清單並提供範例：

- `trustedShellCommands` - 符合這些模式的命令會在沒有提示的情況下執行，繞過所有其他護欄。模式會比對完整的命令字串。

  範例：

  - `cd *` - 符合以 cd 開頭的複合命令
  - `*&&*` - 信任所有具有 && 運算子的命令
- `alwaysPromptCommands` - 符合這些模式的命令需要明確許可，除非由 覆寫`trustedShellCommands`，無論`-t`旗標或工作階段信任為何。這些模式不會在非互動式模式中強制執行 (`-x`)。模式會與複合表達式 (&&、||、命令替換） 中的每個子命令進行比對。

  範例：

  - `rm -rf *` - 一律提示遞迴強制刪除命令
  - `sudo *` - 一律提示使用 sudo 執行的命令
  - `find * -exec *` - 一律使用 -exec 提示尋找命令

工作階段層級信任：

在互動式提示期間，您可以選擇：

- `(y)es` - 執行一次
- `(n)o` - 拒絕
- `(t)rust` - 僅限目前工作階段的信任

工作階段層級信任設定是暫時的，並在 CLI 重新啟動時重設，提供暫時核准，而不會永久修改 trust-settings.yaml。

> **Note**
>
> 工作階段信任不適用於符合您`alwaysPromptCommands`清單的命令。

模型內容通訊協定 (MCP) 伺服器

AWS 轉換 CLI 支援模型內容通訊協定 (MCP) 伺服器，可使用其他工具擴展其功能。

組態：

在 `~/.aws/atx/mcp.json` 檔案中設定 MCP 伺服器。 AWS 轉換 CLI 支援兩種類型的 MCP 伺服器：本機命令型伺服器和遠端 HTTP 伺服器。

本機命令型伺服器：

本機伺服器會在您的機器上做為子程序執行。使用 `command` 屬性設定它們：

```
{
  "mcpServers": {
    "my-local-server": {
      "command": "npx",
      "args": ["-y", "@example/mcp-server"]
    }
  }
}
```

遠端 HTTP 伺服器：

遠端伺服器會連線至 HTTP 或 HTTPS URL 託管的 MCP 伺服器。使用 `url` 屬性設定它們：

```
{
  "mcpServers": {
    "my-remote-server": {
      "url": "https://api.example.com/mcp",
      "headers": {
        "Authorization": "Bearer ${MCP_API_TOKEN}"
      }
    }
```

```
  }
}
```

headers 屬性是選用的，並支援使用${VAR_NAME}語法進行環境變數擴展。這可讓您將 API 字符等敏感值存放在環境變數中，而不是儲存在組態檔案中。

組態屬性：

本機命令型伺服器支援下列屬性：

- command （必要） - 執行伺服器的命令
- args （選用） - 命令列引數陣列
- env （選用） - 要傳遞至伺服器程序的環境變數

遠端 HTTP 伺服器支援下列屬性：

- url （必要） - 遠端 MCP 伺服器的 HTTP 或 HTTPS URL
- headers （選用） - 包含在請求中的 HTTP 標頭，支援${VAR_NAME}環境變數擴展

管理 MCP 伺服器：

檢視設定的 MCP 伺服器清單：

```
atx mcp tools
```

列出特定 MCP 伺服器提供的可用工具：

```
atx mcp tools --server <server-name>
```

用量追蹤：

CLI 會在轉換執行期間自動追蹤 MCP 工具用量。用量統計資料會與 一起保留mcp_usage.json為對話目錄中的 metadata.json。每個執行的檔案會記錄每個工具的指標，包括：

- 每個工具的叫用次數
- 每個工具的錯誤數量
- 每個工具的總執行時間
- 上次錯誤詳細資訊 （如果有的話）

用戶端技能

用戶端技能是在轉換執行期間擴展代理程式的額外功能。它們可讓您提供自訂工具、指令碼和指示，讓代理程式與其內建功能搭配使用。

技能探索目錄：

技能會依優先順序從四個目錄探索。如果具有相同名稱的技能存在於多個目錄中，清單中的第一個目錄會優先：

1. `<project>/.aws/atx/skills/` - 專案層級， AWS Transform CLI 特定
2. `<project>/.agents/skills/` - 專案層級、跨用戶端（適用於任何相容的代理程式工具）
3. `~/.aws/atx/skills/` - 使用者層級， AWS Transform CLI 特定
4. `~/.agents/skills/` - 使用者層級、跨用戶端（適用於任何相容的代理程式工具）

`.aws/atx/skills/` 目錄專屬於 AWS 轉換 CLI。`.agents/skills/` 目錄是跨用戶端的，這表示放置的技能可供 AWS Transform CLI 以外的任何相容代理程式工具使用。

技能目錄結構：

每個技能都是一個目錄，其中包含具有 YAML 前綴`SKILL.md`的檔案：

```
~/.aws/atx/skills/
### my-skill/
    ### SKILL.md          # Required: frontmatter + instructions
    ### references/       # Optional: reference docs the agent can read
    #   ### guide.md
    ### scripts/          # Optional: scripts the agent can execute
        ### validate.py
```

SKILL.md 格式：

```
---
name: my-skill
description: When to use this skill
---
# Skill Title

Instructions for the agent...
```

name 欄位必須符合父目錄名稱。

停用技能：

若要避免在不移除其檔案的情況下載入技能，請將 disable-model-invocation: true新增至前端：

```
---
name: my-skill
description: When to use this skill
disable-model-invocation: true
---
```

設定此屬性時，CLI 會在探索期間略過技能。除非轉換定義明確指示客服人員讀取技能檔案，否則客服人員無法查看或使用技能。使用此選項可暫時停用技能、將其標記為work-in-progress，或保留僅供人類讀者使用的參考資料。

> **Note**
>
> 停用的技能檔案會保留在磁碟上。如果轉換定義指示代理程式讀取特定檔案路徑，代理程式仍然可以存取內容。disable-model-invocation 屬性可防止自動探索和內容注入，而不是檔案系統存取。

依執行模式區分的技能可用性：

- Exec 模式 (atx custom def exec 搭配 --code-repository-path) - 從使用者層級和專案層級目錄探索技能。
- 互動式模式 (atx) - 一開始只會探索使用者層級的技能。當您在工作階段期間提供程式碼儲存庫路徑時，也會載入專案層級的技能。

驗證技能探索：

在執行後檢查 CLI 的偵錯日誌，以確認發現了哪些技能：

Linux and macOS

```
grep -i "skill" ~/.aws/atx/logs/debug.log | tail -20
```

Windows (PowerShell)

```
Select-String -Pattern "skill" "$env:USERPROFILE\.aws\atx\logs\debug.log" | Select-Object -Last 20
```

驗證失敗的技能會略過，並在偵錯日誌中出現警告。

> **Note**
>
> 用戶端技能需要 CLI 2.0 版或更新版本。

在專案層級和使用者層級技能之間進行選擇

您放置技能的位置會決定誰從中受益，以及啟用的時間。

專案層級技能 (`<project>/.aws/atx/skills/`)：

將這些遞交至版本控制，讓每個針對儲存庫執行轉換的團隊成員自動探索。將專案層級技能用於：

- 儲存庫特定的合規檢查 (Dockerfile 規則、Terraform 政策、遷移安全驗證程式）
- 適用於此程式碼庫的組織編碼標準（可觀測性模式、錯誤處理、命名慣例）
- 建置或測試專案特有的指令碼（自訂文字、架構健身函數）
- 此儲存庫中使用的內部程式庫 API 遷移指南

使用者層級技能 (`~/.aws/atx/skills/`)：

這些會保留在您的機器上，並在所有轉換期間啟用，無論您以哪個儲存庫為目標。將使用者層級技能用於：

- 個人工作流程工具 (changelog 產生器、遞交訊息格式器）
- 跨專案偏好設定（偏好的測試模式、文件樣式提醒）
- 您的組織在所有儲存庫中所需的授權合規檢查
- 您使用的每個程式碼庫強制執行的涵蓋閾值或品質閘道

有效技能的秘訣：

- 在您的SKILL.md前端編寫清晰description的欄位。客服人員使用此欄位來決定技能的相關性。
- 在成功時以代碼 0 結束驗證指令碼，在失敗時以非零結束驗證指令碼。代理程式會解譯結束代碼以判斷合規性。
- 在指令碼中列印清晰、可行的錯誤訊息。代理程式會讀取輸出以了解要修正的項目。
- 將技能放在任一層級的跨用戶端目錄 (.agents/skills/) 中，以與 AWS Transform CLI 以外的其他 AI 開發工具共用。

用戶端技能範例

這些範例顯示兩種常見模式：以指令碼為基礎的驗證技能和僅限參考技能。

範例：Dockerfile 合規檢查程式 （ 以指令碼為基礎 ）

此技能會根據安全性和操作最佳實務驗證 Dockerfile。它使用代理程式在進行變更前後執行的驗證指令碼。

目錄結構：

```
.aws/atx/skills/
### dockerfile-compliance/
    ### SKILL.md
    ### scripts/
    #   ### lint_dockerfile.sh
    ### references/
        ### dockerfile-best-practices.md
```

https：//SKILL.md：

```
---
name: dockerfile-compliance
description: Validates Dockerfiles against security and operational best practices
---
# Dockerfile Compliance Checker

When a transformation creates or modifies Dockerfiles, run the compliance checker.

## When to use

- After creating a new Dockerfile
- After modifying FROM, RUN, USER, or EXPOSE directives
```

```
- When containerizing an application as part of a transformation

## How to use

Run: `bash scripts/lint_dockerfile.sh <path-to-Dockerfile>`

If violations are found, consult `references/dockerfile-best-practices.md`
for compliant patterns.
```

驗證指令碼會檢查未固定的基礎映像標籤、做為根目錄執行、ENV指令中的硬式編碼秘密，以及缺少HEALTHCHECK定義。代理程式會執行指令碼、使用參考檔案中的模式修正違規，並重新執行指令碼以確認合規。

範例：API 棄用協助程式（僅限參考）

此技能會引導客服人員在升級轉換期間取代已取代的 API 呼叫。它只使用沒有指令碼的參考檔案。

目錄結構：

```
.aws/atx/skills/
### api-deprecation-helper/
    ### SKILL.md
    ### references/
        ### aws-sdk-v2-to-v3.md
        ### react-class-to-hooks.md
```

https：//SKILL.md：

```
---
name: api-deprecation-helper
description: Guides the agent through replacing deprecated API calls with modern
 equivalents
---
# API Deprecation Helper

When performing upgrade transformations, use this skill to identify and replace
deprecated API calls with their modern equivalents.

## When to use

- During any version upgrade transformation
- When build warnings mention deprecated APIs
```

```
- When transforming code that uses legacy patterns

## Process

1. Identify deprecated API calls in the codebase
2. For each deprecated call, find the replacement in `references/`
3. Apply the replacement, preserving the original behavior
4. Verify the replacement compiles and tests pass
```

參考檔案包含before-and-after程式碼範例。例如，使用 S3Client和 將 等量的模式aws-sdk-v2-to-v3.md映射s3.putObject(params).promise()至模組化 v3PutObjectCommand。

標籤和組織

您可以使用標籤來組織轉換，以進行存取控制和分類。

> **Note**
> 其中一些命令需要指定轉換定義的 Amazon Resource Name (ARN)。ARN 結構為：`arn:aws:transform-custom:<region>:<account-id>:package/<td-name>`

若要列出轉換的標籤：

```
atx custom def list-tags --arn <transformation-arn>
```

若要將標籤新增至轉換：

```
atx custom def tag --arn <transformation-arn> --tags '{"env":"prod","team":"backend"}'
```

若要從轉換中移除標籤：

```
atx custom def untag --arn <transformation-arn> --tag-keys "env,team"
```

標籤可用於 IAM 政策中的分組存取控制。您可以建立政策，將許可授予具有特定標籤的所有轉換（例如，所有以 team:frontend或 標記的轉換environment:production)。

日誌

AWS Transform CLI 會維護三種類型的日誌，以進行疑難排解和偵錯。

對話日誌：

Linux and macOS

```
~/.aws/atx/custom/<conversation_id>/logs/<timestamp>-conversation.log
```

Windows

```
%USERPROFILE%\.aws\atx\custom\<conversation_id>\logs\<timestamp>-conversation.log
```

這些日誌包含特定工作階段的完整對話歷史記錄。

子代理程式日誌：

Linux and macOS

```
~/.aws/atx/custom/<conversation_id>/logs/subagents/<name>.log
```

Windows

```
%USERPROFILE%\.aws\atx\custom\<conversation_id>\logs\subagents\<name>.log
```

這些日誌包含來自子代理程式的輸出，主要代理程式會在轉換期間產生這些輸出。您不需要直接管理子代理程式。

開發人員偵錯日誌：

Linux and macOS

```
~/.aws/atx/logs/debug*.log
~/.aws/atx/logs/error.log
```

Windows

```
%USERPROFILE%\.aws\atx\logs\debug*.log
%USERPROFILE%\.aws\atx\logs\error.log
```

這些日誌提供 CLI 本身的進階疑難排解資訊。

> **Note**
>
> 日誌目錄中可能有多個偵錯日誌檔案（即 debug1.log、debug2.log)。開啟支援票證以加快解決速度時，請檢閱並提供所有相關日誌，例如 ~/.aws/atx/custom/<conversation-id>/* 和 ~/.aws/atx/logs/*。

CLI 更新

將您的 CLI 保持在最新狀態，以存取新功能和改善項目。

若要檢查更新：

```
atx update --check
```

若要更新至最新版本：

```
atx update
```

若要更新至特定版本：

```
atx update --target-version <version>
```

建立自訂轉換

本節說明如何建立、修改和管理自訂轉換定義。

建立新的轉換

使用互動式 CLI 建立新的轉換定義。

建立轉換定義

1. 啟動 AWS 轉換 CLI：

   ```
   atx
   ```

2. 告訴客服人員您要建立新的轉換。
3. 提供清楚、詳細的轉換目標說明。包括：

- 來源和目標狀態（例如「從 X 版升級至 Y 版」）
- 所需的特定變更（例如「更新匯入陳述式、取代已棄用的方法」）
- 任何特殊考量或限制

4. 當客服人員要求釐清或其他資訊時，請提供特定範例和參考資料。
5. 檢閱客服人員建立的初始轉換定義。
6. 在範例程式碼庫上測試轉換。
7. 透過提供意見回饋、程式碼修正或其他範例來反覆運算。
8. 在本機儲存轉換，或將其發佈至登錄檔。

建立轉換的最佳實務：

- 先從簡單、定義明確的轉換開始，然後再嘗試複雜的轉換
- 提供完整的參考資料，包括遷移指南和程式碼範例
- 發佈前在多個範例程式碼庫上測試
- 使用確定性建置或驗證命令來啟用持續學習
- 考慮將複雜的轉換分成多個較小的步驟
- 在您的轉換定義中，使用「關鍵：」或「重要：」標記重要資訊，以確保客服人員優先考慮這些要求
- 當您需要遵循確切的要求時（例如使用特定命令或字串值），請在轉換定義中明確指定完整字串。您可以用 bash 引號括住這些引號，以清楚指出它們是終端機命令或常值字串，這可減少變異性並確保一致的執行

提供參考資料

您可以在對話期間指定檔案路徑，為 AWS 轉換自訂提供參考檔案。這些檔案會存放在轉換定義的 `references/`資料夾中。

建議的參考檔案類型：

- 之前/之後的範例程式碼
- 涉及APIs、程式庫或功能的文件
- 人類可讀遷移指南

若要提供參考檔案：

```
Take a look at the documentation here: /path/to/migration-guide.md
```

您也可以提供包含多個參考檔案的目錄：

```
Take a look at the docs we have here: /path/to/docs/
```

> **Note**
>
> 僅支援文字型檔案 (.md、.html、.txt、程式碼檔案）。目前不支援二進位檔案、映像和富文字檔案（例如 .pdf、.png、.docx)。通常可以擷取文字內容並將其用作參考。如果您有許多小型文字檔案，請考慮將它們串連成幾個描述性命名的檔案。所有檔案的總計限制為 10MB。

修改現有的轉換

您可以在將自訂轉換儲存為草稿或發佈之前和之後修改自訂轉換。您無法修改受 AWS管轉換。如果您需要自訂它們，您可以使用 組態檔案提供額外的內容。

修改現有的轉換

1. 啟動 AWS 轉換 CLI：

   ```
   atx
   ```

2. 告訴客服人員您要修改現有的轉換。
3. 選擇是否：

   - 提供本機儲存轉換的檔案路徑（即不是已儲存的草稿或已發佈）
   - 從登錄檔請求轉換清單

4. 如果從登錄檔中選擇，請選取您要修改的轉換。
5. 與客服人員合作，描述您要進行的變更。
6. 在範例程式碼庫上測試更新的轉換。
7. 視需要將您的更新發佈至登錄檔。

發佈和管理轉換

您可以使用互動式體驗或下列命令來發佈和管理轉換。

若要將轉換儲存為草稿：

```
atx custom def save-draft -n my-transformation --description "Description of the
 transformation" --sd ./transformation-directory
```

若要發佈轉換：

```
atx custom def publish -n my-transformation --description "Description of the
 transformation" --sd ./transformation-directory
```

若要列出可用的轉換：

```
atx custom def list
```

若要下載轉換定義：

```
atx custom def get -n my-transformation
```

這會將轉換定義下載到您目前的工作目錄。您可以使用 `--td`旗標指定目標目錄，並使用 `--tv`旗標指定版本。

若要刪除轉換定義：

```
atx custom def delete -n my-transformation
```

> **Important**
>
> 這會從您的帳戶永久刪除指定的轉換定義。

管理轉換版本

AWS 轉換自訂會維護轉換定義的版本。您可以在執行或下載轉換時指定版本。

若要執行特定版本：

```
atx custom def exec -n my-transformation --tv v1 -p ./my-project
```

若要下載特定版本：

```
atx custom def get -n my-transformation --tv v1
```

如果未指定版本，則會使用最新版本。

命令參考

本節提供所有 AWS 轉換自訂 CLI 命令的完整參考。

互動式命令

atx

使用 AWS 轉換 CLI 開始互動式對話。

```
atx                          # Start new conversation
atx --resume                 # Resume most recent conversation
atx --conversation-id <id>   # Resume specific conversation
atx -t                       # Start with all tools trusted
```

互動式工作階段命令

在互動式工作階段期間，可以在輸入提示中輸入下列命令：

- `/usage` - 顯示目前工作階段的累積客服人員分鐘數

轉換定義命令

atx 自訂 def exec

在程式碼儲存庫上執行轉換定義。

選項	長表單	參數	說明
`-p`	`--code-repository-path`	`<path>`	要轉換的程式碼儲存庫路徑。對於目前的目錄，請使用 "."
`-c`	`--build-command`	`<command>`	建置儲存庫時要執行的命令

選項	長表單	參數	說明
-n	--transformation-name	<name>	登錄檔中轉換定義的名稱
-x	--non-interactive	-	在沒有使用者協助的情況下執行轉換
-t	--trust-all-tools	-	信任所有工具 （沒有工具提示）
-d	--do-not-learn	-	選擇不允許從此執行中擷取課程
-g	--configuration	<config>	組態檔案 (JSON 或 YAML) 或 key=value 對的路徑
--tv	--transformation-version	<version>	要使用的轉換定義版本
--limit	--limit	<limit>	設定客服人員分鐘預算限制。當達到限制時，轉換會結束，並且可以提高限制繼續
-h	--help	-	顯示命令的說明

atx 自訂定義清單

列出可用的轉換定義。

```
atx custom def list
atx custom def list --json    # Output in JSON format
```

atx 自訂 def get

取得特定轉換定義的詳細資訊。

選項	長表單	參數	說明
-n	--transformation-name	<name>	要擷取的轉換定義名稱
--tv	--transformation-version	<version>	要擷取的轉換定義版本
--td	--target-directory	<directory>	要儲存轉換定義的目標目錄（預設值："."）
--json	--json	-	JSON 格式的輸出回應
-h	--help	-	顯示命令的說明

atx 自訂定義刪除

永久刪除轉換定義。

```
atx custom def delete -n <transformation-name>
```

atx 自訂定義發佈

將轉換定義發佈至登錄檔。

選項	長表單	參數	說明
-n	--transformation-name	<name>	要發佈的轉換定義名稱
--tv	--transformation-version	<version>	要使用的轉換定義版本（不適用於 --description 或 --source-directory）
--sd	--source-directory	<directory>	讀取本機轉換定義檔案的來源目錄（不適

選項	長表單	參數	說明
			用於 --transformation-version)
--description	--description	<description>	轉換定義的描述（不適用於 --transformation-version)
--json	--json	-	JSON 格式的輸出回應
-h	--help	-	顯示命令的說明

atx 自訂 def save-draft

在登錄檔中將轉換定義儲存為草稿。草稿會在 30 天後過期，且不會顯示在登錄檔中。此命令會傳回草稿的版本編號。您必須使用轉換名稱和版本編號明確執行和擷取草稿。

```
atx custom def save-draft -n <transformation-name> --description "Description" --sd
 <directory>
```

課程命令

atx 自訂定義學習

開啟互動式工作階段，以檢視和管理轉換定義從先前執行中學到的經驗教訓。依類別瀏覽課程、檢視課程詳細資訊，以及封存、還原或刪除課程。

```
atx custom def learnings -n <transformation-name>
```

標籤命令

atx 自訂 def list-tags

列出轉換定義的標籤。

```
atx custom def list-tags --arn <transformation-arn>
```

atx 自訂定義標籤

將標籤新增至轉換定義。

```
atx custom def tag --arn <arn> --tags '{"env":"prod","team":"backend"}'
```

atx 自訂定義取消標籤

從轉換定義中移除標籤。

```
atx custom def untag --arn <arn> --tag-keys "env,team"
```

更新命令

atx 更新

更新 AWS 轉換 CLI。

```
atx update                    # Update to latest version
atx update --check            # Check for updates only
atx update --target-version <version>  # Update to specific version
```

MCP 命令

atx mcp 工具

允許用戶端檢視/確認其 MCP 工具組態。組態的更新必須透過檔案 ~/.aws/atx/mcp.json 直接管理

```

atx mcp tools     # View list of MCP servers
atx mcp tools -s    # List tools for the specified server
```

AWS受管轉換

AWS受管轉換是針對常見使用案例預先建置 AWS、經過審核的轉換，無須額外設定即可使用。

概觀

AWS受管轉換具有下列特性：

- 驗證者 AWS - 這些轉換由 審核 AWS 為高品質

- 準備使用 - 不需要其他設定
- 持續成長 - 持續新增其他轉換
- 可自訂 - 預先建置的轉換可以透過使用`additionalPlanContext`組態參數提供組織需求的其他指引或需求來自訂
- 早期存取支援 - 某些轉換可能會在進一步測試和改進時標記為早期存取

可用 AWS受管轉換

下列目錄列出目前可用的 AWS受管轉換，依使用案例分組。每個資料表會顯示轉換名稱、其套用的語言或堆疊及其狀態。若要快速尋找轉換，請使用此頁面頂端的搜尋方塊，依名稱、語言或使用案例進行搜尋。

此目錄是 AWS受管轉換的正式清單。Kiro Power、代理程式外掛程式、VS Code 外掛程式和 CLI 都會執行相同的轉換。若要列出登錄檔中可用的轉換，請執行 `atx custom def list`。

> **Note**
>
> 標記為早期存取的轉換可正常運作，但可能會根據客戶意見回饋頻繁更新。

執行期升級

將語言或執行時間升級至較新的版本，或變更執行時間分佈。

轉換	語言/堆疊	狀態	說明
`AWS/java-version-upgrade`	Java	全面推出	使用任何建置系統，將 Java 應用程式從任何來源 JDK 版本升級到任何目標 JDK 版本，包括雅加達 EE 遷移、資料庫驅動程式、ORM 架構和 Spring 生態系統更新。在聊天中或使用 `additionalPlanContext` 參

轉換	語言/堆疊	狀態	說明
			數指定目標 JDK 版本。
AWS/python-version-upgrade	Python	全面推出	將 Python 專案從 Python 3.8 或 3.9 遷移至 Python 3.11、3.12 或 3.13，同時維護功能和效能。在聊天中或使用 additionalPlanContext 參數指定目標 Python 版本。
AWS/nodejs-version-upgrade	Node.js	全面推出	將 Node.js 應用程式從任何來源 Node.js 版本升級至任何目標 Node.js 版本。在聊天中或使用 additionalPlanContext 參數指定目標版本。
AWS/lambda-nodejs-runtime-upgrade	Node.js (Lambda)	早期存取	將 AWS Lambda 函數從舊版 Node.js 執行期 (nodejs4.3 到 nodejs22.x) 升級至 nodejs24.x，解決 Lambda 執行期界面用戶端 (RIC) 和 Node.js 24 語言執行期中的重大變更。

轉換	語言/堆疊	狀態	說明
AWS/oracle-java-to-corretto	Java (JDK 分佈)	早期存取	將 Java 專案從 Oracle JDK 遷移至 Amazon Corretto。以標準 Java 對等項目取代 Oracle 特定的內部 APIs、更新建置組態 (Maven 和 Gradle) 和容器基礎映像、移除商業 JVM 旗標，以及產生授權報告。
AWS/ruby-upgrade	Ruby	早期存取	將 Ruby 應用程式從 Ruby 2.x 升級至 Ruby 4.0，及其架構升級至 Rails 8.0 或 Sinatra 4.1。您可以搭配 Rails 和 ActiveRecord 應用程式、Sinatra 應用程式和獨立 Gem 套件使用此轉換。轉換會將每個 Ruby 版本凹凸與相符的架構升級配對，並執行測試套件。然後，它會在進入下一個版本之前隔離失敗。

轉換	語言/堆疊	狀態	說明
AWS/dotnet-version-upgrade	.NET	全面推出	透過受控制的 使用者互動，將 .NET Framework 解決方案遷移至現代 .NET（預設net10.0；支援 net8.0 或更新版本）。評估複雜性和相依性、提供遷移計劃、使用驗證轉換專案，以及產生包含後續步驟的摘要。

SDK 遷移

在 AWS SDK 的主要版本之間遷移。

轉換	語言/堆疊	狀態	說明
AWS/java-aws-sdk-v1-to-v2	Java	全面推出	使用 Maven 或 Gradle 將適用於 Java 專案的 AWS SDK 從 v1 升級到 v2。
AWS/python-boto2-to-boto3	Python	全面推出	根據官方遷移文件，將 Python 應用程式從 boto2 AWS 遷移至 boto3。
AWS/nodejs-aws-sdk-v2-to-v3	Node.js	全面推出	將 Node.js 應用程式從適用於 JavaScript 的 AWS SDK v2 升級至適用於模組化架構的 v3、一級 TypeScript 支援和改善效能，而

轉換	語言/堆疊	狀態	說明
			無需變更 Node.js 版本。

架構升級和遷移

將架構升級至較新的版本，或遷移至不同的架構。

轉換	語言/堆疊	狀態	說明
`AWS/spring-boot-version-upgrade`	Java/Sring 開機	全面推出	將 Spring Boot 3.x 專案遷移至 Spring Boot 4.x（以 4.1.0 GA 為目標）。涵蓋版本升級、入門重新命名、Jackson 3 遷移、Spring Security 7 DSL、@MockBean 移除、屬性重新命名、套件重新定位、可觀測性整合、Spring AI 2.0、Spring Cloud 2025.1、Spring Batch、Kafka、AMQP、gRPC、Native/AOT、JJersey、JSpecify、內嵌伺服器變更、第三方相容性和驗證。
`AWS/JBoss-to-Spring-Boot`	Java (JBoss 或 WildFly to Spring Boot)	早期存取	將 JBoss EAP 或 WildFly 上執行的 Java EE 或 Jakarta EE 企業應用程式遷移至 Spring Boot，消除雲端原生、容器化部署

轉換	語言/堆疊	狀態	說明
			模型的應用程式伺服器相依性。
AWS/early-access-angular-to-react-migration	要反應的角度	早期存取	將 Angular 應用程式轉換為 React。
AWS/angular-version-upgrade	角度	早期存取	將較舊的 Angular 應用程式升級至目標 Angular 版本，包括元件、服務、範本和路由。
AWS/vue.js-version-upgrade	Vue.js	早期存取	執行從 Vue.js 2 到 Vue.js 3 的主要版本升級，現代化元件、狀態管理、路由和全域 APIs。次要和修補程式更新超出範圍。

GenAI 和模型遷移

將生成式 AI 工作負載遷移至 。

轉換	語言/堆疊	狀態	說明
AWS/GenAI-to-Bedrock-Migration-Assessment	生成式 AI 工作負載	早期存取	評估從第三方供應商 (OpenAI、Google Gemini、Anthropic Direct 和開放原始碼模型） 遷移到 的生成式 AI 工作負載。探索 SDK 用量和模型、釐清需求、設計模

轉換	語言/堆疊	狀態	說明
			型映射、預估成本和風險，以及產生評估成品。僅限評估；不會修改原始程式碼。也涵蓋代理式架構，例如CrewAI、Lang Graph 和 Strands。

Language-to-language遷移

將程式碼庫從一種程式設計語言轉換為另一種程式設計語言。

轉換	語言/堆疊	狀態	說明
`AWS/vba-to-python-migration`	VBA 到 Python	早期存取	使用 Openpyxl、Pandas、tkinter 或 PyQt6 和標準程式庫，將 Excel VBA 巨集、模組、UserForms 和內嵌邏輯遷移至同等 Python 指令碼和模組。目標語言為 Python 3.8 或更新版本。轉換 .bas、.cls、.frm 或 .xlsm 內嵌 VBA 程式碼時使用 。

資料庫遷移

目前沒有可用的資料庫特定受 AWS管轉換。若要將 Microsoft SQL Server 資料庫及其相關聯的 .NET 應用程式現代化為 Amazon Aurora PostgreSQL，請參閱 the section called “SQL Server 現代化”。

可觀測性

將記錄和監控現代化為 AWS原生 服務。

轉換	語言/堆疊	狀態	說明
AWS/early-access-log4j-to-slf4j-migration	Java （記錄）	早期存取	使用 Logback 後端將 Java 應用程式從 Log4j (1.x 或 2.x) 遷移至 SLF4J。處理原始碼、相依性管理 (Maven 和 Gradle) 和記錄組態檔案，並透過編譯、測試和剩餘匯入掃描進行驗證。
AWS/datadog-monitors-to-cloudwatch-alarms	基礎設施即程式碼/監控	早期存取	將追蹤 AWS 服務指標和自訂指標的 DataDog 指標監控遷移至原生 CloudWatch 警示做為基礎設施做為程式碼。產生 CloudFormation YAML、CDK TypeScript 和 Terraform HCL。

Architecture

重新架構、重新格式化或最佳化應用程式 AWS。

轉換	語言/堆疊	狀態	說明
AWS/java-performance-optimization	Java （效能）	全面推出	透過分析 JFR 分析資料來偵測 CPU 和記憶體熱點和反模式，然後套用目標程式碼修正，以最佳化 Java 應用程式效能。如需收集 JFR 資料的指示，

轉換	語言/堆疊	狀態	說明
			請參閱 JFR 執行時間指南。
AWS/early-access-java-x86-to-graviton	Java (Arm64 / Graviton)	早期存取	驗證 Java 應用程式與 Graviton 處理器 Arm64 AWS 架構的相容性，並在來源碼可用時更新相依性、偵測架構特定的程式碼模式，以及重新編譯原生程式庫，以解決不相容的問題。許多現代 Java 應用程式已經Arm64-compatible。
AWS/oracle-service-bus-to-aws	Java/整合到無伺服器	早期存取	將 Oracle Service Bus (OSB) 和 BPEL 程序組態遷移至 AWS 原生無伺服器架構，使用 Amazon API Gateway、 AWS Lambda 和 AWS Step Functions 產生可部署的 CDK TypeScript 專案。

轉換	語言/堆疊	狀態	說明
AWS/mulesoft-to-aws-native-java	Java / MuleSoft 至無伺服器	早期存取	使用 SnapStart 將 MuleSoft Mule 3.x 和 4.x 應用程式轉換為無 AWS 伺服器架構 (Amazon API Gateway、 AWS Lambda 和 AWS Step Functions)，以 AWS Lambda 上的 Java 17 為目標。將流程觸發映射至 AWS 事件來源、將 DataWeave 和 MEL 轉換為分層 AWS 對等項目 (VTL、Step Functions、Lambda)、將連接器取代為適用於 Java v2 呼叫的 AWS SDK，並將流程協調為 Step Functions。產生 SAM 範本、Java Lambda 處理常式程式碼、Maven pom.xml、架構文件和 JUnit 5 測試。

轉換	語言/堆疊	狀態	說明
AWS/payshield-hsm-to-aws-payment-cryptography	Java (HSM 到 AWS 付款密碼編譯)	全面推出	將 Java 應用程式從 Thales PayShield HSM 通訊端型命令通訊協定遷移至 AWS Payment Cryptography Service (APC) SDK v2。涵蓋命令映射、金鑰遷移 (TR-31 和 TR-34 匯入、KCV 驗證)、SDK 相依性設定 (Maven、Gradle 和 Ant)、基礎設施移除 (通訊集區、回應剖析器)、測試基礎設施更新和同位測試。

轉換	語言/堆疊	狀態	說明
`AWS/websphere-jaxrs-to-bedrock-agentcore`	Java (WebSphere 到 AgentCore)	早期存取	從 WebSphere 或 Liberty 應用程式中的 REST 端點產生 AgentCore 工具定義，因此 AI 代理器可以呼叫現有的商業邏輯。轉換會讀取您的原始程式碼，並將新檔案寫入輸出目錄，而不會變更任何內容。它會尋找在 javax.ws.rs 和 jakarta.ws.rs 命名空間中使用 JAX-RS 的端點，包括透過 JAX-RS 外觀公開的 EJB。對於每個端點，它將 Java 參數和類型映射到 JSON 結構描述，會解析 HTTP 方法，並評定其可信度，以便您知道要檢閱的內容。輸出包括探索報告、每個端點的 JSON 結構描述、Python 中的工具實作，以及向 AgentCore 閘道註冊它們的資訊清單。

Codebase 分析

分析程式碼庫和產品組合以規劃現代化。這些轉換會產生報告，而且不會修改您的程式碼。

轉換	語言/堆疊	狀態	說明
AWS/comprehensive-codebase-analysis	多種語言	全面推出	對程式碼庫執行深度靜態分析，以產生階層式、交叉參考的文件，結合行為分析、架構文件和商業智慧，並強調技術債務洞察。
AWS/agentic-readiness-analysis	多種語言	早期存取	評估 AI 代理器是否已準備好安全地呼叫系統，涵蓋 APIs、身分、狀態管理、human-in-the-loop和可觀測性。
AWS/modernization-readiness-analysis	多種語言	早期存取	掃描產品組合的雲端原生成熟度差距，並將調查結果映射到 AWS 現代化途徑。
AWS/portfolio-agentic-readiness-analysis	產品組合	早期存取	彙總應用程式產品組合中的個別代理程式整備度分析報告，以識別交叉切割封鎖程式、共用修復模式和優先建議。
AWS/portfolio-modernization-readiness-analysis	產品組合	早期存取	將產品組合中的個別現代化分析報告彙總為合併藍圖，其中包含優先遷移波紋和建議的現代化途徑。
AWS/business-rules-extraction	多種語言	早期存取	此轉換會靜態分析單體程式碼庫，以產生可重寫的文件，而不

轉換	語言/堆疊	狀態	說明
			需要建置、執行或原始程式碼修改。它會將系統分解為邊界網域，並擷取每個網域的業務規則、工作流程、交叉切入考量和資料庫結構。輸出包含機器可讀取的資訊清單、互動式儀表板，以及每個網域的語言中立實作規格，以引導現代化或完整重寫。

安全

根據掃描器調查結果修正原始碼中的安全漏洞。

轉換	語言/堆疊	狀態	說明
`AWS/security-issue-fixer`	多種語言	全面推出	根據第三方掃描器結果（具有 CWE IDs、檔案路徑和行號的 SARIF、JSON、CSV 或純文字問題清單）修正原始碼中的安全漏洞。不執行掃描或探索；它只會在保留功能行為時修復提供的調查結果。涵蓋注入、中斷的身分驗證、密碼編譯失敗、授權、CSRF、不安全的還原序列化、SSRF、路徑周遊、XXE 等。

轉換	語言/堆疊	狀態	說明
			支援 Python、JavaScript、TypeScript、Java、Go、C#、.NET、C、C++ 和 Ruby。

自訂 AWS受管轉換

您可以透過 `additionalPlanContext`組態參數提供額外的內容，自訂 AWS受管轉換以滿足組織的特定需求。

範例：自訂 Java 版本升級

```
codeRepositoryPath: ./my-project
transformationName: AWS/java-version-upgrade
buildCommand: mvn clean install
additionalPlanContext: |
  The target Java version to upgrade to is Java 17.
  Update all internal library dependencies to versions compatible with Java 17.
  Ensure compatibility with our custom authentication framework.
```

範例：自訂 AWS SDK 遷移

```
codeRepositoryPath: ./my-project
transformationName: AWS/java-aws-sdk-v1-to-v2
buildCommand: gradle build
additionalPlanContext: |
  Maintain our existing error handling patterns.
  Use our organization's standard credential provider chain.
  Update logging to use our internal logging framework.
```

常用案例

本節提供使用 轉換 CLI 之常見 AWS 轉換案例的step-by-step指引。

Lambda 執行期升級

Lambda 會定期棄用較舊的語言執行期，要求團隊將其 Lambda 函數升級至支援的版本。 AWS 轉換自訂可以使用 AWS受管語言版本升級轉換來自動化這些升級。例如，若要將以 Python 3.9 寫入的 Lambda 函數升級至 Python 3.13，您可以使用 `AWS/python-version-upgrade`轉換。Java (`AWS/java-version-upgrade`) 和 Node.js (`AWS/nodejs-version-upgrade`) 也提供類似的轉換，涵蓋最常見的 Lambda 執行時間語言。

若要以互動方式升級單一 Lambda 函數，請導覽至函數來源儲存庫的根目錄，然後使用 啟動 AWS 轉換 CLI`atx`。在互動式工作階段中，描述您需要的升級，例如「將此 Python 3.9 Lambda 函數升級至 Python 3.13」。代理程式會選取適當的 AWS受管轉換、分析程式碼、更新語言語法、調整相依性，以及現代化已棄用 API 呼叫。您可以提供組建或驗證命令，例如 `pytest`或 ，`python -m py_compile *.py`以便代理程式可以驗證轉換的程式碼編譯並通過測試。在整個互動式工作階段中，您可以在接受最終結果之前檢閱客服人員提議的變更、提供意見回饋和請求調整。

當您需要升級多個儲存庫的 Lambda 執行時間時，請使用非互動式模式大規模執行轉換。對於每個儲存庫，使用適當的旗標叫用 CLI，以便在沒有使用者輸入的情況下執行。例如，若要將 Node.js 16 Lambda 函數升級至 Node.js 22：

```
atx custom def exec \
  -n AWS/nodejs-version-upgrade \
  -p ./my-lambda-repo \
  -c "npm test" \
  -g "additionalPlanContext='Upgrade from Node.js 16 to Node.js 22'" \
  -x -t
```

`-x` 旗標會以非互動方式執行轉換，並`-t`信任所有工具執行，因此不需要提示。您可以使用簡單的 shell 迴圈，將此命令編寫到數十個或數百個儲存庫。每次轉換完成後，請檢閱 Git diff 以驗證變更，並執行測試套件以確認升級的函數正常運作。您也可以將 AWS 轉換自訂整合到您的 CI/CD 管道中，以持續識別已淘汰的 Lambda 函數。此方法不僅解決已棄用執行時間的立即問題，還建立持續程序，在函數達到end-of-support狀態之前對其進行偵測和升級。

中央平台團隊可以透過 AWS Transform Web 應用程式建立行銷活動，以定義轉換、指定目標 Lambda 儲存庫，以及追蹤整個組織的進度。如需使用 AWS Batch 建置生產級擴展部署解決方案的詳細演練，請參閱使用 AWS 轉換自訂建置可擴展的程式碼現代化解決方案。

AWS Transform 自訂和界面端點 (AWS PrivateLink)

您可以建立介面 VPC 端點，在 VPC 與 AWS Transform 自訂之間建立私有連線。介面端點採用 AWS PrivateLink技術，可讓您在沒有網際網路閘道、NAT 裝置、VPN 連線或 Direct Connect 連線的情況下私密存取 AWS Transform 自訂服務。VPC 與 AWS Transform 自訂之間的流量不會離開 Amazon 網路。

每個介面端點都是由您子網路中的一或多個彈性網路介面表示。

如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的介面 VPC 端點 (AWS PrivateLink)。

> **Note**
>
> - 您必須啟用 Amazon S3 的 AWS PrivateLink 整合，因為 AWS Transform 自訂會進行 S3 API 呼叫。如需詳細說明，請參閱AWS PrivateLink 適用於 Amazon S3 的 文件。如果您在使用 AWS Transform 自訂時遇到 S3 存取問題，請參閱我們的故障診斷指南。
> - 如果您未使用 AWS PrivateLink 私有 DNS 功能 （請參閱私有 DNS)，您必須：
>   - 設定路由至 VPC 介面端點 （請參閱路由至 VPC 介面端點文件 ）
>   - 設定ATX_CUSTOM_ENDPOINT環境變數以指定您的自訂網域，例如：
>
>     ```
>     ATX_CUSTOM_ENDPOINT=https://transform-custom.<region>.api.aws atx
>     ```

AWS Transform 自訂 VPC 端點的考量事項

為 AWS Transform 自訂設定介面 VPC 端點之前，請務必檢閱《Amazon VPC 使用者指南》中的介面端點屬性和限制。

AWS Transform 自訂支援透過介面端點呼叫其所有 API 動作。

先決條件

開始進行下方任何程序之前，務必先備妥下列各項：

- 具有適當許可來建立和設定資源 AWS 的帳戶。
- 已在 AWS 您的帳戶中建立 VPC。
- 熟悉 AWS 服務，特別是 Amazon VPC 和 AWS Transform 自訂。

為 AWS Transform 自訂建立介面 VPC 端點

您可以使用 Amazon VPC 主控台或 AWS Command Line Interface () 為 AWS Transform 自訂服務建立 VPC 端點AWS CLI。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的建立介面端點。

使用此服務名稱為 AWS Transform 自訂建立下列 VPC 端點：

- com.amazonaws.*region*.transform-custom

將##取代為您想要使用 AWS Transform 自訂 CLI AWS 的區域，例如 com.amazonaws.us-east-1.transform-custom。

如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的透過介面端點存取服務。

建立 AWS Transform 自訂的 VPC 端點政策

您可以將端點政策連接至控制 AWS Transform 自訂存取的 VPC 端點。此政策會指定下列資訊：

- 可執行動作的主體。
- 可執行的動作。
- 可供執行動作的資源。

如需詳細資訊，請參閱 Amazon VPC 使用者指南中的使用 VPC 端點控制對服務的存取。

範例： AWS Transform 自訂動作的 VPC 端點政策

以下是 AWS Transform 自訂端點政策的範例。連接到端點時，此政策會授予所有資源上所有主體所列出的 AWS Transform 自訂動作的存取權。

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "transform-custom:*"
         ],
         "Resource":"*"
      }
   ]
```

```
}
```

使用內部部署電腦連線至 AWS Transform 自訂端點

本節說明使用內部部署電腦，透過 AWS VPC 中的 AWS PrivateLink 端點連線至 AWS Transform 自訂的程序。

1. 在內部部署裝置與 VPC 之間建立 VPN 連線。
2. 為 AWS Transform 自訂建立介面 VPC 端點。
3. 設定傳入 Amazon Route 53 端點。這可讓您從內部部署裝置使用 AWS Transform 自訂端點的 DNS 名稱。

疑難排解

本節提供使用 AWS 轉換自訂疑難排解常見問題的指引。

日誌位置

AWS 轉換 CLI 會在下列位置維護日誌：

對話日誌：

Linux and macOS

```
~/.aws/atx/custom/<conversation_id>/logs/<timestamp>-conversation.log
```

Windows

```
%USERPROFILE%\.aws\atx\custom\<conversation_id>\logs\<timestamp>-conversation.log
```

這些日誌包含用於偵錯特定轉換執行的完整對話歷史記錄。

子代理程式日誌：

Linux and macOS

```
~/.aws/atx/custom/<conversation_id>/logs/subagents/<name>.log
```

Windows

```
%USERPROFILE%\.aws\atx\custom\<conversation_id>\logs\subagents\<name>.log
```

這些日誌包含來自子代理程式的輸出，主要代理程式會在轉換期間產生這些輸出。您不需要直接管理子代理程式。

開發人員偵錯日誌：

Linux and macOS

```
~/.aws/atx/logs/debug*.log
~/.aws/atx/logs/error.log
```

Windows

```
%USERPROFILE%\.aws\atx\logs\debug*.log
%USERPROFILE%\.aws\atx\logs\error.log
```

這些日誌提供有關 CLI 操作和錯誤的詳細資訊。每個日誌檔案在滾動之前都有 5MB 的限制。此目錄中可能有多個偵錯日誌，例如 debug1.log 和 debug2.log。

常見問題

安裝問題：

如果安裝失敗，請確保您已安裝 Node.js 22 或更新版本：

```
node --version
```

如有需要，請從 https://nodejs.org/en/download：// 下載 Node.js。

身分驗證問題：

確認您的 AWS 登入資料設定正確：

```
aws sts get-caller-identity
```

確保您的 IAM 使用者或角色具有必要的`transform-custom:*`許可。

網路連線問題：

如果您遇到連線錯誤，請驗證必要端點的網路存取：

- `transform-cli.awsstatic.com`
- `transform-custom.<region>.api.aws`
- `*.s3.amazonaws.com`

如果在網際網路限制的環境中工作，請更新防火牆規則以允許列出這些 URLs。

區域組態問題：

如果您遇到與區域相關的錯誤：

- 驗證您的區域是否受支援
- 檢查可能覆寫您組態的環境變數： `echo $AWS_REGION $AWS_DEFAULT_REGION`
- 檢查您的區域組態： `aws configure get region`
- 如有需要，請更新您的區域： `aws configure set region <your-region>`
- 檢查偵錯日誌以取得區域解析詳細資訊

Git 問題：

確保已安裝 Git，且您的儲存庫受到 git 來源控制：

```
git --version
git status
```

AWS 轉換自訂需要儲存庫在 git 來源控制下。

轉換執行問題：

如果轉換失敗：

1. 在 檢閱對話日誌 `~/.aws/atx/custom/<conversation_id>/logs/`
2. 檢查轉換輸出中是否有建置或測試失敗
3. 確認您的專案的 build 命令正確
4. 嘗試在互動式模式下執行轉換，以提供意見回饋

對話恢復問題：

如果您無法繼續對話：

- 驗證對話是否少於 30 天
- 檢查對話 ID 是否正確
- 確定您有網路連線能力

取得支援

如需其他協助，請透過AWS 主控台前往 AWS 支援。

開啟支援票證時，請包含：

- 來自 的對話日誌 `~/.aws/atx/custom/<conversation_id>/logs/`
- 來自 的子代理程式日誌 `~/.aws/atx/custom/<conversation_id>/logs/subagents/`
- 從 偵錯日誌 `~/.aws/atx/logs/`
- 重現問題的步驟
- AWS 轉換 CLI 版本 (`atx --version`)

S3 存取問題

AWS 轉換自訂服務提供 S3 預先簽章URLs，以協助在用戶端機器之間上傳和下載潛在的大型轉換檔案。這表示 CLI 不僅會與 AWS Transform 服務端點互動，也會與 S3 服務端點互動。這些互動使用預先簽章URLs，因此用戶端的 IAM 登入資料不需要任何 S3 許可，但有時本機電腦的代理伺服器組態和網路的 S3 VPC 端點政策可能會限制此流量。

請檢查 the section called “日誌位置” 以取得更詳細的錯誤訊息，以協助根導致與下載和上傳轉換檔案相關的任何工具失敗或 S3 存取遭拒。

如果您使用的是利用 `https_proxy`和 `no_proxy`環境變數的 VPN/代理伺服器，請考慮將下列值新增至您的`no_proxy`環境變數值，以略過 S3 的代理並 AWS 轉換自訂服務端點，例如：

Linux and macOS

```
export no_proxy=.s3.amazonaws.com,transform-custom.<region>.api.aws
```

Windows (PowerShell)

```
$env:no_proxy=".s3.amazonaws.com,transform-custom.<region>.api.aws"
```

如果您在 VPC 中使用AWS 適用於 Amazon S3 的 PrivateLink，則可能已定義政策來限制 S3 流量。請確保您的 S3 VPC 端點政策允許 GetObject和 PutObject操作 AWS 轉換自訂服務擁有的儲存貯體。這可以透過將下列陳述式新增至您的 VPC 端點政策來完成：

```
{
    "Effect": "Allow",
    "Principal": "*",
    "Action": ["s3:PutObject","s3:GetObject"],
    "Resource": "arn:aws:s3:::aws-transform-custom-*/*"
}
```

政策中的明確Deny陳述式優先於 Allow 陳述式。檢閱 S3 VPC 端點政策是否有可能限制存取的Deny陳述式。

AWS 轉換 CLI 版本歷史記錄

如需 AWS 轉換 CLI 目前和過去版本的詳細資訊，請參閱下表。資料表包含每個版本的版本、發行日期和版本備註。

版本	版本日期	版本備註
3.11.0（最新）	2026 年 8 月 19 日	• 在單一命令中--repos將atx ct remediation create多儲存庫修復新增至 。 • 新增 --transformation-name 至 atx ct remote remediation ，以直接從轉換定義執行修復，而不需要現有的問題清單。 • 新增--json輸出至 atx ct analysis run以取得機器可讀取的結果。 • 已將客服人員分鐘成本摘要新增至 atx ct analysis get和 atx ct remediation status 。 • 新增atx ct remote provision 了在試轉模式下的 本機檔案匯出：產生的 AWS CloudFormation 範本現在會寫入本

版本	版本日期	版本備註
		機檔案（使用 覆寫位置--out-dir），以便在部署之前檢閱。 • 修正代理程式發出的刪除系列命令可能終止 CLI 本身程序的問題。受影響的命令包括 pkill -f node、 xargs kill和 find -exec kill。shell 工具現在會先針對 CLI 自己的程序及其祖鏈進行檢查，再執行它們。 • 修正 GitLab 來源探索使用儲存庫主題做為語言欄位的問題。這可能會導致其主題中具有特殊字元的儲存庫註冊失敗。不再從主題推斷語言。 • 修正以下問題：失敗的atx ct命令可能會在空輸出時以無提示方式結束。CLI 現在會顯示可操作的錯誤訊息。 • 修正當服務回報執行已結束時，完成本機分析執行可能會發生錯誤的問題。 • 已修正 atx ct remote update 未更新共用分派器基礎設施的問題。因此，升級 CLI 並執行 會remote update繼續使用先前部署的分派程式。 remote update 現在會協調分派程式。 • 修正遠端分析執行 (Amazon EC2 或 AWS Batch) 可能會報告錯誤失敗的問題。當範圍執行中的所有儲存庫都已完成服務時，就會發生這種情況。 • 修正儲存atx ct庫探索可能會在無提示的情況下捨棄服務遭拒的儲存庫的問題。CLI 現在會計算並報告略過的儲存庫 (「略過 N 個儲存庫」)，並提供大型組織的溢位摘要。 • 變更使用者面向的錯誤和警告訊息，以參照 AWS 轉換並明確說明後續步驟（重新整理登入資料、重試或聯絡支援）。訊息不再參考內部服務名稱。

版本	版本日期	版本備註
3.10.0	2026 年 8 月 10 日	• 新增 shell 工具background=true 中對長時間執行或非終止命令 (開發伺服器、建置監看器、) 的支援tail -f。它會立即傳回程序 ID，而不是等待命令結束。一次最多可追蹤 5 個背景程序。 • 新增 check_background_shell 和 stop_background_shell 工具來監控和終止背景程序。 • 已llmConfig 新增至 CLI 組態允許清單，讓使用者能夠透過組態檔案自訂 LLM 設定。 • 新增 --mode aws-managed atx ct schedule create和 atx ct remote analysis，以使用全受管 AWS 基礎設施執行分析，而無需佈建您自己的 Amazon EC2 或 AWS Batch 資源。 • 新增 --schedule-id 和 --display-name 選項atx ct analysis，以依排程篩選結果，並依人類可讀標籤識別分析。 • 新增對 --mode aws-managed 操作的--region支援，可讓您將受管分析執行的目標設為特定 AWS 區域。 • 改善 atx ct schedule get、disable、 enable和delete命令的可靠性。 • 改善atx ct schedule list結果的準確性和一致性。 • --stack-name 新增至 atx ct schedule create 以將排程固定到特定目標堆疊。 • 新增從 AWS受管基礎設施分析執行中擷取輸出成品的新 atx ct analysis list-artifacts 和 atx ct analysis get-artifact 命令。 • 修正 CLI 追蹤的背景程序在 CLI 結束時未正確終止的問題，這可能會使孤立的程序保持執行中狀態。 • 修正 與 搭配使用時atx ct schedule create，未拒絕 --workers 和 --batch-name 旗標的問題--mode aws-managed 。 • 已修正排程找不到錯誤訊息中不一致的措辭。 • 修正在所有 CLI 命令中，端點覆寫未一致解析的問題。

版本	版本日期	版本備註
		• 改善重複排程名稱偵測的準確性。 • 修正 `atx ct remote analysis --resume`未繼續部分完成的批次執行的問題。標記現在是 `--resume-incomplete` ，它只會重新執行未完成（失敗、中斷或尚未啟動）的儲存庫，並略過已完成的儲存庫。 • 更新`atx ct schedule --help`以包含 AWS Managed Analysis 執行方案。
3.9.0	2026 年 7 月 31 日	• 改善了 `atx custom def export-ki-markdown` 對包含許多知識項目之轉換定義的效能。命令不會再為每個知識項目進行備援服務呼叫，因此它會在大型定義上執行得更快且不會再逾時。同時修正匯出可能會省略知識項目或報告不一致總計的情況。 • 修正以下問題：代理程式準備度和現代化準備度分析搭配 執行時，`atx ct analysis run`可能會針對特定報告格式報告零問題清單。問題清單現在可可靠地復原。 • 修正以下問題：嘗試擷取登入資料時，使用 `atx ct schedule create` 針對 GitLab、Bitbucket 或本機來源建立的排程分析在每次執行時都可能失敗。來源提供者現在會自動從您的註冊來源決定，而且不再需要 `--provider` 選項。 • 修正安全性分析在遠端 (AWS 批次或 EC2) 環境中執行時，可能不正確地報告 Security Agent 未設定的問題。CLI 現在可正確偵測已設定的安全代理程式，並更正常地報告暫時性登入資料或限流錯誤。

版本	版本日期	版本備註
3.8.0	2026 年 7 月 29 日	• 已將 `--recurrence` 選項新增至 `atx ct schedule create`，因此您可以使用純文字 (`daily`、 或 `monthly:<1..28>`) 設定排程的節奏`weekly:<MONDAY..SUNDAY>` ，而不是撰寫原始 Cron 表達式。 • 已將 `--existing-scheduler-role-arn` 選項新增至 `atx ct remote provision` ，因此您可以重複使用管理員為排程器建立的 IAM 角色，而不是讓 CLI 在佈建期間建立一個角色。 • 已將 `--existing-instance-profile-name` 選項新增至 `atx ct remote provision --mode ec2`，因此您可以連接管理員已建立的 IAM 執行個體描述檔，而不是讓 CLI 建立轉換角色和執行個體描述檔。 • 改善轉換選擇指引，使其現在可在可用時使用偵測中繼資料，例如嚴重性和相符條件。這有助於呈現最適合您的專案及其相對優先順序的轉換。 • 修正取消排程遠端分析會停止執行中容器，但可能會讓分析停滯在 `running` 狀態的問題。取消現在可靠地將分析標記為已取消。 • 已修正 `atx ct schedule delete`可能遺棄分析記錄的問題。刪除排程現在也會移除基礎排程分析。

版本	版本日期	版本備註
3.7.0	2026 年 7 月 22 日	• 新增在 EC2 或 AWS Batch 上遠端執行分析和修復的`atx ct remote`命令群組。您可以在 AWS Secrets Manager 中佈建、更新和銷毀遠端執行基礎設施、檢查提交狀態、偵測部署的堆疊和管理來源憑證。 • 新增週期性排程分析和修復任務的`atx ct schedule`命令群組。您可以建立、列出、啟用、停用和刪除排程（任務選項鏡像 `remote analysis`和 `remote remediation`），以及排程器基礎設施`teardown`的 `setup`和 。排程會在建立時擷取本機原始碼套件。 • 已改善`atx ct analysis run`以使用轉換套件登錄檔中的 tech-debt-quick 比對規則。 • 改善長時間執行的`atx ct`命令以顯示進度輸出，包括分析執行期間的每個儲存庫進度（包括安全性分析），以及修復狀態中的每個儲存庫失敗原因。 • 修正數個遠端執行可靠性問題。EC2 狀態現在會顯示調查結果和提取請求結果，符合批次；堆疊遺失新參數時EC2 更新不會再失敗；以及其他修正地址結束代碼、轉換處理、標籤型偵測和 JSON 輸出。
3.6.0	2026 年 7 月 17 日	• 新增 `atx custom def learnings` 子命令，這會開啟互動式 TUI 工作階段，以檢視和管理根據先前執行之轉換定義自動產生的學習。 • 在轉換執行期間新增用量遙測收集。若要停用遙測，請設定 `ATX_DISABLE_TELEMETRY=true` 環境變數。如需詳細資訊，請參閱用量遙測。 • 修正 Windows 上使用 ~（主目錄）路徑的檔案操作解析至非預期目錄的問題。這會導致工作階段期間檔案讀取/寫入失敗。 • 修正包含特殊字元的 MCP 伺服器和工具名稱可能導致連線失敗的問題。CLI 現在會自動淨化名稱以僅使用有效字元。

版本	版本日期	版本備註
3.5.0	2026 年 7 月 8 日	• 新增原生 Windows 支援。您現在可以直接在 Windows 上執行 AWS Transform Custom 命令。(Windows 尚未支援這些atx ct命令） • 已將轉向輸入新增至 ，atx ct analysis run以便客服人員準備度和現代化準備度分析反映您的偏好設定。使用 --context 進行策略架構、--agent-scope 設定代理程式存取以進行代理程式準備，以及 --prefer/--avoid 將現代化建議導向或遠離特定技術。 • 技能格式的轉換定義現在可以包含scripts/資料夾，讓您將協助程式指令碼與 SKILL.md和 參考一起綁定。 • 已--wait新增至 atx ct remediation create ，等待修復完成。 • 新增了一次性執行的無周邊模式。執行 atx -x "prompt" -t 以傳遞提示、取得回應，然後在沒有互動式提示的情況下結束。無周邊模式需要信任所有工具。
3.4.1	2026 年 7 月 2 日	• 修正 3.4.0 版引進的互動式工作階段問題。代理程式完成回應後，CLI 可能會停留在「思考」提示（在 UI 中顯示省略符號）上，而不是返回輸入提示。CLI 現在會在每次回應後傳回輸入提示。

版本	版本日期	版本備註
3.4.0（不建議）	2026 年 6 月 29 日	⚠ 已知問題 在互動式工作階段中，在客服人員完成回應之後，CLI 可能會停留在「思考」提示（在 UI 中顯示省略符號）。這可防止您輸入下一個訊息。若要解決此問題，請執行 以升級至 3.4atx update.1 版或更新版本。 • 新增 atx ct schema，這是用於指令碼編寫和自動化的完整atx ct命令表面的機器可讀取資訊清單。 • 當您立即新增或更新來源、出現憑證或許可問題，而不是在分析期間失敗時，新增權杖範圍驗證。 • 改善自動修復提取請求，以包含調查結果內容，並支援更可檢閱 PRs的草稿模式。 • 改善了 CLI 進度意見回饋，其中包含目前活動、預估客服人員分鐘數和子客服人員活動的即時內容。 • 透過 ATX_GIT_COMMITTER_NAME 和 ATX_GIT_COMMITTER_EMAIL 環境變數新增可設定的檢查點遞交作者身分。 • 各種小錯誤修正和改進。
3.3.0	2026 年 6 月 18 日	• 新增了跨atx ct命令的一致性--json和--help支援。 • 已修正安全代理程式設定，以便在設定期間建立代理程式空間，並在拆解時移除。 • 各種小錯誤修正和改進。
3.2.0	2026 年 6 月 15 日	• 將持續現代化命令 (atx ct) 新增至所有使用者的標準 CLI 分佈。 • 改善子代理程式執行，在等待伺服器回應時顯示「思考中...」微調器，提供正在進行的清晰視覺回饋。 • 改善了在代理程式輸出後 3 秒無聲後自動重新啟動的旋轉器，因此在處理步驟之間，終端機永遠不會凍結。 • 使用細微的閃粉動畫改善思維旋轉器，使視覺效果更明亮。

版本	版本日期	版本備註
3.1.0	2026 年 6 月 3 日	• 新增ATX_MAX_VALIDATION_LOOPS 環境變數以設定驗證迴圈上限。 • 修正更新檢查不會再顯示已安裝版本比登錄版本更新時的錯誤「可用更新」警告。 • 已修正 delete --transformation-name "" 不再顯示無意義的確認提示；空白值現在會因明確的驗證錯誤而遭到拒絕。 • 已修正無法辨識的子命令現在會顯示「未知命令」，而不是混淆的內部錯誤訊息。 • 修正對更新檢查使用數值比較而非字串不等式的版本比較。
3.0.0	2026 年 5 月 21 日	• 新增了預檢轉換名稱驗證，當找不到名稱時， 會從您的登錄檔建議類似的名稱，協助擷取錯別字，而不需要單獨的清單命令。 • 已新增 shell 命令的選用說明，顯示它們的功能和原因。 • 改善信任設定橫幅，以包含工具許可的詳細資訊。 • 使用do-not-learn旗標時新增學習停用橫幅，提供學習功能的可見性以及如何啟用。 • 重大變更：現在需要 Node.js 22 或更新版本。如果您使用的是舊版，請從 https://nodejs.org/：// 升級。

版本	版本日期	版本備註
2.0.0	2026 年 5 月 14 日	• 已新增遠端 MCP 伺服器支援 – 使用自動 SSE 後援連線至 HTTP 和 HTTPS MCP 伺服器、標頭中具有環境變數擴展的承載字符身分驗證，以及代理支援 (HTTP_PROXY/HTTPS_PROXY)。 • 新增`atx resume`子命令做為 的別名`atx --resume`。 • 新增使用輸出控制進行多檔案文字搜尋`grep`的工具 — 支援 regex 模式、檔案 glob 篩選、不區分大小寫的搜尋、可設定的深度/結果限制，以及輸出截斷。 • 改善了 MCP 實作，以使用標準 MCP 開發套件來實現更一致的行為，並更輕鬆地支援未來的 MCP 功能。 • 改善殼層輸出處理：輸出現在會正常截斷為每個串流 30K 個字元，而不是造成硬錯誤，保留內容的輸出開始和結束。 • 修正互動式工作階段期間的 Ctrl+C 可能過早在 Linux/macOS 上結束 CLI，而不是中止目前的操作並返回提示的問題。 • 修正信任拒絕訊息，顯示信任無法使用的專用原因，與命令需要授權的原因不同。 • 已修正危險命令警告不再提及當命令位於 時的信任`alwaysPromptCommands` 。
1.10.0	2026 年 4 月 29 日	• 透過跨工具指導改善工具描述，協助客服人員為每個任務選擇最佳工具，並減少不必要的 shell 使用量。 • 在 `alwaysPromptCommands` 中新增 `trust-settings.yaml` — 設定一律需要明確許可的 shell 命令模式，無論信任設定為何。針對複合表達式中的每個子命令支援 glob 萬用字元和相符項目。 `trustedShellCommands` 可以覆寫這些模式。未以非互動式模式強制執行，以避免中斷自動化管道。 • 修正未解析為絕對路徑的相對路徑。
1.9.0	2026 年 4 月 23 日	• 改善工具核准提示 – 每個選項現在都會顯示內嵌的動作，「為什麼」訊息說明需要核准的原因，而信任確認包含有關永久信任`trust-settings.yaml` 的提示。

版本	版本日期	版本備註
1.8.0	2026 年 4 月 16 日	• 將客服人員輸出字首從 變更為 `> ATX:` ，以更清楚地區分使用者輸入和客服人員輸出。 • 修正 CLI 重試用盡時繼續命令的顯示。 • 已修正來自不同工作目錄的繼續。在互動式模式中， 會提示修正路徑；在非互動式模式中， 會因描述性錯誤而快速失敗。
1.7.1	2026 年 4 月 9 日	• 當登入資料提供者區域與設定檔的 不同時，修正 SSO 登入失敗 (「找不到工作階段字符或無效」)`sso_region` 。 • 已修正登入資料快取，因此在磁碟上輪換登入資料時，長時間執行的工作階段不會再失敗。
1.7.0	2026 年 4 月 2 日	• 修正在輸入驗證錯誤時以程式碼 1 結束的`exec`命令，讓 CLI 在指令碼和 CI/CD 管道中可靠。 • 新增顯示來自 服務的警告訊息。 • 新增 AWS 憑證設定檔的 MFA 提示支援。 • 修正 STS 登入資料呼叫，以遵守 HTTP(S) 代理設定。
1.6.0	2026 年 3 月 18 日	• 新增設定 `exec`和 `interactive` 命令的客服人員分鐘預算`--limit <minutes>` 的選項。達到限制時，CLI 會顯示用量，並使用繼續指示結束。 • 修正對話日誌中初始使用者訊息的記錄。
1.5.0	2026 年 3 月 11 日	• 新增對並行任務執行的支援，從而實現更快的轉換。 • 新增每次對話結束時的客服人員分鐘用量顯示，並在互動式模式中`/usage`顯示命令，以隨時檢查用量。
1.4.0	2026 年 3 月 2 日	• 改善使用不支援的檔案儲存轉換定義時的錯誤訊息。 • 新增服務呼叫的逾時，以防止 CLI 在連線中斷時懸置。 • 修正成功完成後 CLI 程序停止。 • 已修正繼續對話時的區域驗證。

版本	版本日期	版本備註
1.3.0	2026 年 2 月 19 日	• 已移除 MCP 伺服器路徑的限制 — 使用者現在可以在 MCP 組態中指定 command 屬性的任何路徑。 • 改善 MCP 伺服器連線的穩定性。
1.2.0	2026 年 2 月 9 日	• 新增透過環境變數 (https_proxy 、 no_proxy等) 的代理組態支援。 • 一般穩定性改善和錯誤修正。
1.1.1	2026 年 1 月 16 日	錯誤修正和穩定性改善。
1.1.0	2026 年 1 月 13 日	新增 AWS 了 CLI 區域組態支援、早期憑證驗證檢查，以及固定的行銷活動恢復功能。
1.0.1	2025 年 12 月 18 日	正常關機、清理錯誤日誌和一般改善。
1.0.0	2025 年 12 月 1 日	AWS 轉換 CLI 的初始版本。

AWS 轉換持續現代化

什麼是 AWS 轉型持續現代化？

AWS 轉換持續現代化可為您的原始程式碼儲存庫提供分析和修復。您可以連接 GitHub 組織、GitLab 群組、Bitbucket 工作區和本機儲存庫，然後執行自動化分析，以在整個程式碼庫中識別技術債務、安全漏洞、現代化機會和客服人員就緒度。

所有分析和修復 AWS 帳戶 都會使用您的 登入資料在 中執行。您的原始程式碼仍由您控制。

> **Note**
>
> 我們建議您從 Kiro Power 或代理程式外掛程式開始。客服人員技能會協調持續現代化的設定、加入和持續使用，包括基礎設施佈建、來源組態、分析執行、問題清單分類和修復。如需安裝指示，請參閱開發人員工具。

關鍵功能

AWS 轉型持續現代化提供下列功能：

- 技術債務分析 — 掃描儲存庫是否有過時的相依性、安全漏洞、程式碼品質問題和現代化機會。跨套件資訊清單或全面的程式碼層級分析執行快速中繼資料掃描。使用為您的環境量身打造的轉換定義來定義自訂分析條件。
- 自主修復 — 大規模產生經過驗證的提取請求。每個問題清單都可以使用其相關聯的轉換定義自動修復。修復會在 GitHub、GitLab 和 Bitbucket 中自動建立分支並開啟 PRs/MRs。
- 報告 — 產生 HTML 報告，依嚴重性、儲存庫和分析類型顯示問題清單。追蹤一段時間內的修復進度和問題清單解決方案。
- 持續監控 — 排程重複分析，以持續監控您的產品組合是否有新問題。在沒有設定的情況下在 AWS 轉換受管基礎設施上執行，或使用 Amazon EventBridge 排程器在佈建的 Amazon EC2 或 Batch 堆疊上執行。 EventBridge 設定每日、每週或每月節奏。

分析類型

AWS 轉換持續現代化支援下列分析類型，以滿足您的現代化需求。

Type	說明
`rapid-techdebt-analysis`	快速掃描僅中繼資料的套件資訊清單 (`pom.xml`、`package.json` 、`requirements.txt`)，以識別過時的版本和過時的相依性。不會分析原始程式碼。
`tech-debt-comprehensive`	使用 AWS Transform 代理程式進行深度程式碼層級的技術負債分析。檢查原始程式碼以識別債務模式、程式碼品質問題、架構問題和改善機會。
`security`	使用 Security Agent AWS 的安全漏洞和 CVE 偵測。掃描原始程式碼和相依性是否有已知漏洞、不安全的編碼模式，以及可利用的弱點。需要一次性基礎設施設定。
`agentic-readiness`	AI 和客服人員整合整備度評估。分為五個類別的 56 個條件：基礎設施與平台、應用程式架構、資料基礎、Identity/Security/Governance，以及營運與可觀測性。
`modernization-readiness`	雲端現代化機會評估。評估基礎設施、應用程式、資料、安全性和操作維度的準備程度。識別容器化、無伺服器遷移和平台升級的候選者。
`custom`	執行任何轉換定義 (TD) 做為分析。使用此類型來定義您自己的分析條件，或執行內建類型未涵蓋的 AWS 受管轉換。

了解核心概念

來源

來源會告知儲存庫所在位置的持續現代化。支援的來源類型：

- GitHub — 具有個人存取字符的組織 （傳統）

- GitLab — 群組或使用者，包括自我託管執行個體
- Bitbucket — Workspaces （雲端） 或專案 （資料中心）
- Local — 包含 git 儲存庫的父目錄

儲存庫

掃描來源會探索儲存庫。探索之後，您可以依來源、標籤或其他條件進行篩選；套用組織標籤 （團隊、優先順序、遷移波）；並將特定儲存庫設為目標以進行分析或修復。

分析

分析是使用特定分析類型的一或多個儲存庫的掃描。每個分析都會產生問題清單，以識別程式碼中的問題。您可以隨需執行分析，或將分析排程為自動執行。分析類型包括rapid-techdebt-analysis、tech-debt-comprehensive、 安全性、代理程式就緒性、現代化就緒性和自訂。每個分析都會追蹤其狀態 （待定、執行中、完成、取消或失敗） 及其掃描的儲存庫。

調查結果

調查結果是分析的結果。每個調查結果都包含嚴重性 （高、中或低）、狀態 （開啟、關閉或淘汰），以及可以修復它的修正轉換 （如果可自動修正）。新問題清單開始為開啟。使用者可以根據原因關閉問題清單。重新分析會將已解決的問題清單自動標記為已淘汰。

修復

修復會套用轉換定義來修正問題清單。三種模式：以問題清單為基礎 （每個問題清單都使用自己的修正轉換）、TD 覆寫 （覆寫指定問題清單的轉換定義） 和直接 TD （針對沒有問題清單的儲存庫執行轉換）。輸出取決於來源提供者 (GitHub PR、GitLab MR、Bitbucket PR 或本機分支）。

轉換定義

轉換定義包含執行特定程式碼轉換所需的指示和知識。持續現代化使用轉換定義進行自訂分析 (`--type custom --transformation-name` *`name`*) 和修復 ()`--transformation-name` *`name`*。使用 列出可用的轉換定義`atx custom def list`。

AWS 轉型持續現代化的運作方式

AWS 轉型持續現代化通常用於需要持續分析和修復多個程式碼庫的大規模專案。團隊通常會遵循此工作流程：

1. Connect Sources — 新增 GitHub 組織、GitLab 群組、Bitbucket 工作區或本機目錄做為來源。提供具有適當範圍的身分驗證字符。
2. 探索儲存庫 — 執行探索掃描以列舉來源中的所有儲存庫。使用標籤依團隊、優先順序或遷移波來組織儲存庫。
3. 執行分析 — 跨產品組合執行分析。選擇快速掃描以取得快速結果，或選擇完整分析以取得詳細的調查結果。安全分析需要一次性基礎設施設定。
4. 分類調查結果 — 依嚴重性、儲存庫或分析類型檢閱調查結果。以記錄的原因關閉誤報。重新執行分析，將已解決的問題標記為已淘汰。
5. 修復 — 建立修復以修正問題清單。持續現代化會自動建立分支，並使用修正開啟提取/合併請求。追蹤修復狀態和重試失敗。
6. 設定持續分析 — 使用使用 Amazon EventBridge 排程器的`atx ct schedule`命令來排程週期性分析。設定分析節奏（每日、每週或每月），以持續監控您的產品組合是否有新問題。結合自動化修復，以隨著時間維持程式碼運作狀態。

運算選項

持續現代化支援執行分析和修復的多種運算選項。分析可以在本機、您在 AWS 帳戶 (Amazon EC2 或 AWS Batch) 中佈建和管理的基礎設施，或在不需要設定的 AWS 轉換受管基礎設施上執行。Kiro Power 中的客服人員技能和客服人員外掛程式可協助您設定每個選項。

> **Note**
>
> 無論運算選項為何，您都可以使用登入資料建立和擁有 中的所有 AWS 帳戶 資源，而原始程式碼仍由您控制。執行分析和修復的基礎設施是客戶受管 - 您在帳戶中佈建的堆疊 - 或 AWS Transform 受管，其中 會為您 AWS 操作運算，而且無需佈建。

Local（預設）

根據預設， 分析會在您的本機電腦上執行。此選項不需要額外的基礎設施。伺服器會在本機執行，並使用本機運算資源執行分析。適用於試用工具、小型儲存庫或個別使用。

AWS 轉換受管（無需佈建基礎設施）

在 AWS 轉換受管基礎設施上執行分析，無需佈建或管理堆疊。使用 `--mode aws-managed`，您可以將分析提交至 AWS Transform，以在 AWS操作的基礎設施上執行。沒有 Amazon EC2 執行個體、沒

有 AWS 批次堆疊，也沒有要設定的 VPC 或子網路。無需佈建或縮減 - 提交即為執行。當您不想管理任何基礎設施時，這是遠端執行的最快方法。

此選項需要在支援的 SCM 提供者 (GitHub、 GitLab或) 上託管的來源Bitbucket。 AWS Transform 受管基礎設施不支援本機來源，因為它無法連接機器上的儲存庫。您可以使用 `--region`選項選擇工作負載在其中執行 AWS 的區域。

AWS 轉換受管基礎設施只會執行分析。如需修復或執行自訂轉換定義 (`--type custom`)，請使用 AWS Batch 或 Amazon EC2。

若要在 AWS 轉換受管基礎設施上執行，請使用 `atx ct remote analysis --mode aws-managed`命令 （ 請參閱 遠端執行)，或安裝 Kiro Power 或代理程式外掛程式 （ 請參閱 開發人員工具)，並詢問代理程式：「在沒有基礎設施 AWS 的情況下在 上執行我的分析」。 AWS 轉換受管基礎設施的重複分析需要 執行角色 （ 請參閱 排程週期性分析)。

您也可以從 AWS Transform Web 應用程式中的持續現代化頁面，開始 AWS 對轉換受管基礎設施進行分析 （ 請參閱 AWS 轉換 Web 應用程式)。

AWS Batch (Fargate) （ 建議 ）

對於大多數產品組合，您可以在 AWS Batch with Fargate 上執行分析，這是建議的運算選項。每個分析都會在具有無伺服器運算的容器中做為隔離任務執行，因此沒有要管理的持久性基礎設施，而且任務會橫向擴展以平行分析多個來源或分析類型。

佈建會部署所需的基礎設施，包括：

- AWS 批次任務佇列和運算環境
- 具有持續現代化容器映像的任務定義
- 批次任務執行的 IAM 角色
- 用於提交任務的 Lambda 函數

佈建基礎設施需要管理員許可。若要在已佈建且具有最低權限的批次堆疊上執行分析和修復，請 AWS 連接 受管政策 `AWSTransformInfrastructureExecutorAccessBatch`。

若要設定批次執行，請直接使用`atx ct remote`命令 （ 請參閱遠端執行)，或安裝 Kiro Power 或代理程式外掛程式 （ 請參閱開發人員工具)，並詢問代理程式：「在 Fargate 上執行我的分析」或「設定批次執行以進行持續現代化」。代理程式會部署堆疊、將來源登入資料存放在 Secrets Manager 中，並將分析任務提交至 AWS Batch。

Amazon Amazon EC2

在 中的持久性 Amazon EC2 執行個體上執行分析 AWS 帳戶。此選項會從本機機器卸載運算、支援較大的分析，並啟用週期性排程分析。執行個體會在提交之間保持執行狀態。

佈建會部署 AWS CloudFormation 堆疊，其中包含：

- 具有 Docker 和持續現代化容器的 Amazon EC2 執行個體 (Amazon Linux 2023)
- 具有 AWS Transform、Amazon S3、 AWS KMS、Secrets Manager 和安全代理程式許可的 IAM 角色
- `AmazonSSMManagedInstanceCore` 透過 SSM 進行 Shell 存取（不需要 SSH 金鑰對或傳入連接埠）
- 沒有傳入規則的安全群組

佈建基礎設施需要 Amazon EC2 生命週期管理、 AWS CloudFormation 堆疊操作、IAM 角色建立、Amazon S3 儲存貯體操作、Secrets Manager 秘密管理和 SSM 命令的管理員許可。若要在已佈建且具有最低權限的 Amazon EC2 堆疊上執行分析和修復，請連接 AWS 受管政策 `AWSTransformInfrastructureExecutorAccessEC2`。

若要設定 Amazon EC2 執行，請直接使用 `atx ct remote` 命令（請參閱 遠端執行)，或安裝 Kiro Power 或代理程式外掛程式（請參閱 開發人員工具)，並詢問代理程式：「設定 EC2 執行個體以進行持續現代化分析」。代理程式會佈建基礎設施、驗證容器是否正常運作，並透過 SSM 提交您的分析，而不需要 SSH。

安全代理程式設定

`security` 分析類型使用 AWS Security Agent 服務進行漏洞和 CVE 偵測。與其他分析類型不同，它需要在 中設定一次性基礎設施 AWS 帳戶。

> **Note**
>
> `security` 分析類型不適用於下列區域：加拿大（中部）()`ca-central-1`、歐洲（倫敦）(`eu-west-2`) 和亞太區域（首爾）()`ap-northeast-2`。其他分析類型不受影響。

安裝命令會佈建 AWS CloudFormation 堆疊，其中包含：

- 用於原始碼上傳的 Amazon S3 儲存貯體

- 擔任的 IAM 角色 `securityagent.amazonaws.com`
- 安全代理程式角色的受管政策

若要在設定後以最低權限執行安全分析，請將 AWS 受管政策連接至`AWSTransformSecurityAgentExecutorAccess`您的 IAM 使用者或角色。

您的 IAM 使用者或角色必須具有下列額外許可，才能執行設定：

- `cloudformation:CreateStack`, `cloudformation:UpdateStack`, `cloudformation:DescribeStacks`
- `iam:CreateRole`, `iam:PutRolePolicy`, `iam:AttachRolePolicy`, `iam:CreatePolicy`
- `s3:CreateBucket`, `s3:PutBucketEncryption`, `s3:PutBucketPublicAccessBlock`

使用下列命令來管理安全代理程式基礎設施：

```
# Provision the security agent infrastructure
atx ct setup security-agent

# Check the status
atx ct setup security-agent --status

# Delete the infrastructure
atx ct setup security-agent --delete
```

設定完成後，您可以像其他分析類型一樣執行安全分析。

開始使用

先決條件

若要有效使用持續現代化，您應該對 Git 版本控制有基本的了解、熟悉原始程式碼平台 (GitHub、GitLab 或 Bitbucket)、IAM AWS 許可的工作知識，以及使用命令列工具的經驗。

在使用持續現代化之前，請確認您有下列項目：

- AWS 轉換已安裝的 CLI：

```
curl -fsSL https://transform-cli.awsstatic.com/install.sh | bash
```

- Node.js 22 或更新版本
- 有效的 AWS 登入資料 (AWS_PROFILE 或 環境變數)
- AWSTransformCustomFullAccess 連接至 IAM 使用者或角色的 AWS 受管政策

> **Note**
>
> 在遠端基礎設施或安全代理程式上執行分析和修復需要額外的受管政策。請參閱 中的運算選項和安全代理程式設定AWS 轉型持續現代化的運作方式。

快速入門

> **Note**
>
> 您不再需要啟動本機伺服器。atx ct server 命令已棄用。

1. 新增來源：

   ```
   atx ct source add --name name --provider provider --org org-or-group --token token
   ```

   其中##是來源的描述性識別符，###是平台 (github、bitbucket、 或 local)gitlab，*org-or-group* 是您的組織或群組名稱，##是您的身分驗證字符。

2. 探索儲存庫：

   ```
   atx ct discovery scan --source name
   ```

3. 執行分析：

   ```
   atx ct analysis run --type type --source name --wait
   ```

4. 探索問題清單：

   ```
   atx ct findings list --json
   ```

5. 修復問題清單：

```
atx ct remediation create --ids id1,id2 --name "remediation-name"
```

使用持續現代化

來源管理

使用 `atx ct source` 命令來連接儲存庫。支援的提供者：GitHub、GitLab、Bitbucket、local。

GitHub 組織

權杖：具有`repo`範圍的個人存取權杖（傳統）。用於分析的唯讀、用於修復的完整儲存庫。

```
atx ct source add --name name --provider github --org org --token pat
```

GitLab 群組和使用者

權杖：具有`api`範圍的個人存取權杖。

```
atx ct source add --name name --provider gitlab --org group-or-user --token pat
# Self-hosted:
atx ct source add --name name --provider gitlab --org group-or-user --token pat --url
 https://gitlab.example.com
```

Bitbucket 工作空間和專案

Bitbucket Cloud — 範
圍：`read:repository:bitbucket`、`write:repository:bitbucket`、`read:pullrequest:bitbu`
也需要 `--email`和 `--username`。

```
atx ct source add --name name --provider bitbucket --org workspace --token api-token --
email email --username username
```

Bitbucket 資料中心：

```
atx ct source add --name name --provider bitbucket --org project-key --token http-
access-token --url https://bitbucket.example.com
```

本機儲存庫

```
atx ct source add --name name --provider local --path parent-directory
```

> **Important**
>
> `--path` 必須指向包含 git 儲存庫的父目錄作為子目錄，而不是單一儲存庫。

管理來源

```
atx ct source list
atx ct source remove --name name
```

儲存庫探索和管理

```
atx ct discovery scan --source name
atx ct discovery status --source name
atx ct discovery scan --source name --path new-directory
```

探索後：

```
atx ct repository list
atx ct repository list --source name
atx ct repository list --labels "team:frontend,priority:high"
atx ct repository update --source name --repo "source::repo" --labels
 "team:frontend,priority:high"
atx ct repository update --source name --labels "migration:wave-1"
```

執行分析

`--type` 旗標指定要執行的分析類型：

- `rapid-techdebt-analysis` – 過時的相依性和輕鬆獲勝。
- `tech-debt-comprehensive` – 更深入的 AI 驅動分析，涵蓋相依性、安全性、模式、效能、可維護性、架構、程式碼品質和基礎設施問題清單。
- `security` – 安全漏洞和暴露。

- agentic-readiness – AI 代理器儲存庫的準備程度（架構、APIs、文件）。
- modernization-readiness – 跨基礎設施、應用程式、資料、安全性和操作維度的現代化機會。

```
atx ct analysis run --type type --source name [--repo source::repo] [--wait]
atx ct analysis get --id id --json
atx ct analysis list --json
atx ct analysis list --status pending|running|complete|cancelled|failed --json
atx ct analysis list --type type --json
atx ct analysis cancel --id id
atx ct analysis delete --id id [--cascade-findings]
```

自訂分析

```
atx ct analysis run --type custom --transformation-name name --source source --
repo source::repo --wait
```

具有-g旗標的組態：鍵值、JSON 或檔案路徑。

列出 TDs： atx custom def list

管理調查結果

```
atx ct findings list --json
atx ct findings list --repo source::repo --source name --severity high|medium|low
 --type analysis-type --status open|dismissed|obsolete --analysis-id id --fix-
transform transform-name --json
```

尋找狀態

- open — 作用中
- dismissed — 手動關閉（需要原因）
- obsolete — 重新分析不再產生問題清單時的系統集

```
atx ct findings update --id id --status dismissed --reason "reason"
atx ct findings update --id id --status open
atx ct findings batch-update --ids id1,id2 --status dismissed --reason "reason"
atx ct findings get --id id
```

```
atx ct findings delete --id id
```

尋找過時

重新分析會將已解決的問題清單標記為過時。無法重新開啟。保留以供稽核。

建立修復

三種模式：以調查結果為基礎、TD 覆寫、直接 TD。

```
atx ct remediation create --ids id1,id2 --name "name"
atx ct remediation create --ids id1,id2 --transformation-name TD
atx ct remediation create --transformation-name TD --repo source::repo
```

提供者輸出：GitHub PR、GitLab MR、Bitbucket PR、Local 分支。

> **Note**
>
> 權杖必須具有寫入存取權才能建立 PR/MR。

具有 `--local` 旗標的本機執行。

```
atx ct remediation create --transformation-name TD --repo source::repo -g
 "additionalPlanContext=Upgrade to Node.js 22"
atx ct remediation list
atx ct remediation status --id id
atx ct remediation retry --id id
atx ct remediation cancel --id id
atx ct remediation delete --id id
```

遠端執行

根據預設，分析和修復會在您的本機電腦上執行。對於較大的產品組合，您可以將工作卸載至遠端基礎設施。您可以在 AWS 轉換受管基礎設施上執行，無需佈建 （僅限分析），或是在您在 中佈建和管理的基礎設施上執行 AWS 帳戶，即持久性 Amazon EC2 執行個體或 AWS Batch (Fargate) 任務。`atx ct remote` 命令佈建、執行、監控和銷毀客戶受管基礎設施。無論執行在何處發生，您都會在 中建立所有資源， AWS 帳戶 而您的原始程式碼仍由您控制。

> **Note**
>
> 佈建、更新和銷毀基礎設施會建立和修改 AWS CloudFormation 堆疊和 IAM 角色，且需要管理員許可。傳遞 `--ack` 以確認這一點，並略過互動式提示。在已佈建的基礎設施上執行分析和修復會使用最低權限的執行器政策 — 請參閱 中的 標記和存取控制 中涉及AWS 轉型持續現代化的運作方式的受管政策的運算選項。

在 AWS 轉換受管基礎設施上執行（無佈建）

若要在遠端執行分析而不佈建任何內容，請使用 `--mode aws-managed`。提交會前往 AWS Transform，在 AWS Transform 受管基礎設施上執行分析。無需佈建堆疊、無需設定聯網，也無需在 AWS Secrets Manager 中存放登入資料。提交是執行。選擇工作負載使用 在 中執行 AWS 的區域`--region`。

```
# Run an analysis on AWS Transform-managed infrastructure
atx ct remote analysis --type type --mode aws-managed --sources name [--
repos repo1,repo2] [--region region]

# Poll the submission (there is no remote status command in this mode)
atx ct analysis get --id id --json
```

此模式只會執行分析。它不支援修復、`custom`分析類型或本機來源。由於沒有堆疊，因此 `--stack-name`、`--existing-instance`、 `--tags`和 `--batch-name`選項不適用。單一提交最多涵蓋 100 個儲存庫。若要涵蓋更大的範圍，請使用 將其分割為多個提交`--repos`。與 Amazon EC2 和 Batch 執行不同，您可以使用 `atx ct analysis get`而不是 來監控進度`atx ct remote status`。

聯網

遠端運算必須在私有子網路中執行。在佈建之前，探索現有的聯網或建立新的 VPC：

```
# List VPCs, private subnets, and security groups in the current account and Region
atx ct remote network discover
atx ct remote network discover --vpc vpc-id --json

# Create a new VPC with private subnets, a NAT gateway, and a security group
atx ct remote network create --cidr 10.1.0.0/16 --ack
```

佈建基礎設施

部署 Amazon EC2 或 Batch 堆疊。省略 `--execute`以預覽範本或變更集；新增 `--execute`以套用。

佈建會建立所選模式的運算堆疊，以及排程器堆疊：

- 批次： AWS 批次任務佇列和運算環境、具有持續現代化容器映像的任務定義、任務執行的 IAM 角色，以及任務提交的 Lambda 函數。批次需要安全群組。
- Amazon EC2 — 具有 IAM 執行個體描述檔和安全群組的持久性 Amazon EC2 執行個體。如果您省略 `--securityGroup`，堆疊會建立沒有傳入規則的安全群組；存取是透過 SSM。
- 排程器 — 經常性分析使用的`atx-scheduler`堆疊 (Amazon EventBridge 排程器排程群組和調用角色）。傳遞`--skip-scheduler`以選擇退出。

```
# Preview, then deploy an EC2 stack
atx ct remote provision --mode ec2 --vpc vpc-id --subnets subnet-a,subnet-b
atx ct remote provision --mode ec2 --vpc vpc-id --subnets subnet-a,subnet-b --execute
 --ack

# Deploy a Batch stack
atx ct remote provision --mode batch --vpc vpc-id --subnets subnet-a,subnet-b --
securityGroup sg-id --execute --ack

# Update an existing stack to the latest template, or tear it down
atx ct remote update --mode ec2|batch --execute --ack
atx ct remote teardown --mode ec2|batch --execute --ack
```

容器映像

當您執行遠端分析和修復時，它們會在容器映像中執行。根據預設，當您佈建遠端環境時，它會使用公有 AWS 轉換映像 `public.ecr.aws/d9h8z6l7/aws-transform:latest`。Batch 將其設定為任務定義映像。Amazon EC2 使用它做為執行器映像。

若要執行不同的映像，例如，綁定其他語言或工具的私有 Amazon ECR 映像，請在佈建`--image-uri`時通過：

```
# Batch: provision with a custom image
atx ct remote provision --mode batch --vpc vpc-id --subnets subnet-a,subnet-b --
securityGroup sg-id --image-uri account-id.dkr.ecr.region.amazonaws.com/repo:tag --
execute --ack
```

```
# EC2: provision with a custom image
atx ct remote provision --mode ec2 --vpc vpc-id --subnets subnet-a,subnet-b --image-
uri account-id.dkr.ecr.region.amazonaws.com/repo:tag --execute --ack
```

儲存來源登入資料

遠端容器會使用存放在 AWS Secrets Manager 中的字符複製您的儲存庫。在執行遠端分析或修復之前，為每個 SCM 來源註冊權杖：

```
atx ct remote credentials --source name --token token
atx ct remote credentials --source name --remove
```

遠端執行

遠端分析會為每個儲存庫執行一個容器；遠端修復會為每個調查結果執行一個容器。使用 `--sources`、 `--repos`和 `--labels`來控制廣發功能，以及 `--stack-name`或 `--tags` 來選取要使用的佈建堆疊。

```
# Run analysis across a source on Batch
atx ct remote analysis --type type --mode batch --sources name [--repos repo1,repo2]
 [--labels "team:frontend"]

# Run remediation for specific findings on EC2
atx ct remote remediation --mode ec2 --ids id1,id2
atx ct remote remediation --mode ec2 --sources name --min-severity high
```

監控和管理執行

```
# Check whether infrastructure is deployed
atx ct remote detect --mode ec2|batch

# Track a submission (Batch by batch ID, EC2 by group ID)
atx ct remote status --batch batch-id --stack-name name
atx ct remote status --group ec2-group-id --wait

# Resume a partially-failed Batch run (re-submits only incomplete repos).
# On resume, --batch-name takes the existing batch ID reported by "remote status --
batch".
atx ct remote analysis --type type --mode batch --sources name --resume-incomplete --
batch-name batch-id
```

```
# Cancel a running submission
atx ct remote cancel --mode batch --batch batch-id --stack-name name
atx ct remote cancel --mode ec2 --group ec2-group-id
```

排程週期性分析

使用 `atx ct schedule`以定期自動執行分析。您可以排程分析，但無法修復。任務選項鏡射 `atx ct remote analysis`。排程會以兩種方式之一從遠端執行：

- AWS 轉換受管 (`--mode aws-managed`) - 在 AWS 轉換受管基礎設施上觸發分析的伺服器端排程。沒有 Amazon EventBridge 排程，也不需要佈建。它需要 AWS Transform 在每次執行時擔任的執行角色 (`--execution-role`)（請參閱 AWS 轉換受管排程的執行角色)。
- 客戶受管 (`--mode ec2|batch`) — 帳戶中的 Amazon EventBridge 排程器排程會將每個執行分派至您首先佈建的持久性 Amazon EC2 執行個體或 AWS 批次堆疊（請參閱 遠端執行)。

此`--recurrence`值接受 `daily`、 `weekly:`*DAY*（例如 `weekly:MONDAY`) 或 ，`monthly:`*N*其中 *N* 是從 1 到 28 的一天。 AWS 轉換受管基礎設施在 UTC 中執行的排程。

```
# AWS Transform-managed schedule (no infrastructure; requires an execution role)
atx ct schedule create --name name --mode aws-managed --execution-role role-arn --
recurrence daily --type type --sources name [--repos repo1,repo2]

# Customer-managed schedule (EventBridge Scheduler dispatching to your EC2 or Batch
 stack)
atx ct schedule create --name name --mode ec2|batch --recurrence weekly:MONDAY --
type type --sources name [--repos repo1,repo2]

# Manage schedules of either type by their schedule ID (from schedule list)
atx ct schedule list
atx ct schedule get schedule-id
atx ct schedule disable schedule-id
atx ct schedule enable schedule-id
atx ct schedule delete schedule-id
```

若要檢視排程已執行的分析，請使用 `atx ct analysis list --schedule-id` *schedule-id*，這會先傳回排程的觸發執行。

若要移除客戶受管排程所使用的排程器角色和排程群組，請執行 `atx ct schedule teardown --execute`。

AWS 轉換受管排程的執行角色

使用 建立的排程`--mode aws-managed`需要 AWS 轉換在每次執行排程時擔任的 `--execution-role` ARN。設定角色，如下所示：

- 建立排程的身分必須具有執行角色的`iam:PassRole`許可。
- 角色的信任政策必須允許`transform-custom.amazonaws.com`服務主體擔任該角色。
- 角色至少必須AWSTransformCustomFullAccess連接 AWS 受管政策，加上 字`atx/*`首下秘密的`secretsmanager:GetSecretValue`和 `secretsmanager:DescribeSecret`許可，以便排程的執行可以擷取來源複製登入資料。

下列內嵌政策會授予已排程執行需要擷取來源複製憑證的 AWS Secrets Manager 存取權。將它與AWSTransformCustomFullAccess受管政策一起連接至執行角色，將*##*和*## ID* 取代為執行排程 AWS 的區域和帳戶。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AtxSourceCredentials",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret"
      ],
      "Resource": "arn:aws:secretsmanager:region:account-id:secret:atx/*"
    }
  ]
}
```

標記和存取控制

您可以使用 `--tags`選項將標籤（逗號分隔`key=value`組）套用至來源、分析和修復。遠端基礎設施、儲存的登入資料和聯網資源也支援標籤。透過標籤，您可以組織資源。結合 IAM 標籤條件，標籤會實作屬性型存取控制 (ABAC)，讓團隊只能存取帶有標籤的資源。

```
atx ct source add --name name --provider github --org org --token pat --
tags team=platform,env=prod
atx ct analysis run --type type --source name --tags team=platform
```

```
atx ct remediation create --ids id1,id2 --tags team=platform
```

根據預設，資源會以您在 中定義的標籤進行標記~/.aws/atx/settings.json。新增您要套用至 下每個資源的標籤applyTags，它們會成為您的預設標籤。

```
{
  "applyTags": [
    { "team": "alpha" }
  ]
}
```

> **Note**
>
> 傳遞給 的標籤--tags會合併到任何設定的預設標籤上，並在這兩個位置為任何金鑰集--tags獲勝。

AWS 轉換 Web 應用程式

使用 AWS Transform Web 應用程式來建立和執行分析、檢閱問題清單、建立修復，以及追蹤整個程式碼來源產生的提取請求。

在使用 Web 應用程式之前，您的組織必須啟用您的使用者身分才能存取 AWS Transform。如需設定 AWS 轉換的詳細資訊，請參閱設定 AWS 轉換。

登入

若要存取 AWS Transform Web 應用程式，請完成下列步驟。

1. 使用 AWS IAM Identity Center 登入資料開啟https://aws.amazon.com/transform/並登入。
2. 如果持續現代化未出現，請改用 IAM 登入資料登入：
   a. 在 AWS 管理主控台中，開啟 AWS 轉換，然後選擇設定。
   b. 使用 IAM 登入資料開啟存取 AWS 轉換。
   c. 複製 Web 應用程式 URL （使用 IAM)，並將其貼到開啟主控台的相同瀏覽器視窗。
3. 開啟左側導覽選單，然後選擇持續現代化。

基礎設施模式

當您建立分析時，請選擇下列其中一個基礎設施模式：

- AWS 受管 – 在由 AWS Transform 管理的基礎設施上執行。您不需要佈建任何基礎設施。
- 客戶擁有 – 在您自己的 中部署的堆疊上執行 AWS 帳戶。當您需要控制運算、聯網或安全組態時，請使用此模式。

> **Note**
>
> 若要執行安全分析，請使用客戶擁有的基礎設施。安全分析會在您帳戶中部署的 Security Agent 上執行。

若要使用客戶擁有的基礎設施，請開啟設定索引標籤。使用 AWS CloudFormation 快速建立連結來依序部署下列堆疊：

1. `AtxDispatcherStack` – 訊息發送器 （ 一律為必要 ）。
2. 運算堆疊 – `AtxInfrastructureStack`(AWS 批次 ） 或 `atx-runner`(Amazon EC2)。
3. `atx-scheduler` – 週期性排程分析的必要項目。
4. `AtxSecurityAgentStack-<region>` – 僅適用於安全性分析。

如需 CLI 型佈建和聯網組態，請參閱 遠端執行。

開始使用工作流程

1. 連接來源 – 開啟來源索引標籤，並從 GitHub、 GitLab或 新增儲存庫Bitbucket。
2. 執行或排程分析 – 開啟分析索引標籤、選取儲存庫、選擇分析類型、選取基礎設施模式，然後選擇執行。若要定期執行 （ 每日、每週或每月 ），請改為選擇排程。
3. 檢閱問題清單 – 開啟問題清單索引標籤，依嚴重性檢視結果。
4. 建立修補：選取問題清單，然後選擇建立修補。
5. 檢閱提取請求 – 開啟修復索引標籤，以檢視每個儲存庫產生的 PR 連結。

直接從 Web 應用程式與 AWS Transform 聊天，詢問有關分析、問題清單或修復的問題。

開發人員工具

您可以使用 AWS Transform Power 和代理程式外掛程式，從代理程式 IDEs 存取持續現代化。客服人員透過對話互動協調設定、加入和持續使用持續現代化。

- Kiro IDE — 安裝 AWS Transform Kiro Power。開啟 Kiro Chat，並要求客服人員協助持續現代化工作流程。
- Claude Code、Codex、Cursor — 安裝 awslabs/agent-plugins (`plugins/aws-transform` 目錄）。代理程式外掛程式提供與 Kiro Power 相同的功能。

代理技能

Kiro Power 和代理程式外掛程式包含透過對話互動協調持續現代化工作流程的技能：

技能	說明
指南	互動式入門，逐步引導您完成完整的工作流程
來源	新增、列出和移除來源連線
探索	掃描來源以探索儲存庫
分析	跨所有類型執行和管理分析
調查結果	查詢、篩選和管理分析問題清單
修補	建立和管理修復以修正問題清單
EC2 執行	佈建和管理 Amazon EC2 執行個體以進行遠端分析
批次執行	使用 Fargate 將分析任務提交至 AWS Batch
Schedule	使用 Amazon EventBridge 排程器設定 Cron 排程的週期性分析
報告	產生獨立的 HTML 報告，其中包含顯示問題清單、嚴重性分佈和修復進度的圖表

CLI 參考

下表摘要說明所有`atx ct`子命令。

子命令	說明
`atx ct status`	檢視系統狀態，包括來源、儲存庫、分析、問題清單和修復
`atx ct source add`	新增來源 (GitHub、GitLab、Bitbucket 或本機)
`atx ct source list`	列出設定的來源
`atx ct source get`	顯示單一來源的詳細資訊
`atx ct source update`	更新現有來源的字符
`atx ct source remove`	移除來源
`atx ct discovery scan`	從來源探索儲存庫
`atx ct discovery status`	檢查探索掃描狀態
`atx ct repository list`	使用選用篩選條件列出儲存庫
`atx ct repository get`	取得單一儲存庫
`atx ct repository update`	更新儲存庫標籤
`atx ct repository delete`	刪除儲存庫
`atx ct analysis run`	對儲存庫執行分析
`atx ct analysis get`	取得分析詳細資訊
`atx ct analysis list`	列出具有選用狀態和類型篩選條件的分析
`atx ct analysis cancel`	取消執行中的分析
`atx ct analysis delete`	刪除分析

子命令	說明
`atx ct findings list`	列出具有儲存庫、來源、嚴重性、類型、狀態和分析篩選條件的問題清單
`atx ct findings count`	依嚴重性、儲存庫或分析類型彙總的計數問題清單
`atx ct findings get`	取得單一問題清單
`atx ct findings update`	更新調查結果狀態（開啟或關閉）
`atx ct findings batch-update`	批次更新多個問題清單
`atx ct findings delete`	刪除已關閉或已淘汰的問題清單
`atx ct remediation create`	從問題清單或轉換定義建立修復
`atx ct remediation list`	列出所有修補
`atx ct remediation status`	檢查修復狀態並檢視 PR/MR 連結
`atx ct remediation retry`	重試失敗的修復
`atx ct remediation cancel`	取消執行中的修復
`atx ct remediation delete`	刪除修復
`atx ct remote provision`	部署遠端執行基礎設施 (Amazon EC2 或 Batch AWS CloudFormation 堆疊）
`atx ct remote analysis`	在 Amazon EC2 或 Batch 上遠端執行分析
`atx ct remote remediation`	在 Amazon EC2 或 Batch 上遠端執行修復
`atx ct remote status`	顯示遠端提交的狀態
`atx ct remote detect`	檢查是否已部署遠端基礎設施
`atx ct remote update`	將遠端執行基礎設施更新為最新範本

子命令	說明
`atx ct remote credentials`	在 Secrets Manager 中管理來源字符以進行遠端執行
`atx ct remote cancel`	取消執行中的遠端執行
`atx ct remote teardown`	銷毀遠端執行基礎設施
`atx ct remote network`	探索或建立用於遠端佈建的 VPC、子網路和安全群組
`atx ct schedule create`	建立週期性分析排程 (Amazon EventBridge 排程器)
`atx ct schedule list`	列出排程
`atx ct schedule get`	顯示單一排程
`atx ct schedule enable`	啟用排程
`atx ct schedule disable`	停用排程
`atx ct schedule delete`	刪除排程
`atx ct schedule teardown`	刪除排程器角色和排程群組
`atx ct setup security-agent`	佈建或管理安全代理程式基礎設施
`atx ct mcp`	啟動 MCP 伺服器，公開持續的現代化工具
`atx ct schema`	列印完整`atx ct`命令表面的機器可讀取 JSON 資訊清單，包括每個命令、選項和引數，以便客服人員和自動化可以在不剖析說明文字的情況下探索 CLI

疑難排解

檢查系統運作狀態

您不再需要啟動本機伺服器；`atx ct server`命令已棄用。確認系統可透過 連線`atx ct status --health`。

探索掃描會傳回零個儲存庫

對於本機來源，請確認 `--path`指向包含儲存庫做為子目錄的父目錄（例如 /home/user/repos)，而不是直接指向儲存庫（例如)/home/user/repos/my-app。掃描器會尋找包含`.git`資料夾的子目錄。

SETUP_REQUIRED 錯誤

來源存在於您的帳戶中，但此機器上未設定登入資料。執行 `atx ct source add --name` *name*以在本機設定登入資料。

AUTH_REQUIRED 錯誤

找不到來源的有效權杖。確認您的字符正確且具有所需的範圍。對於 GitHub，請確保字符具有`repo`範圍。對於 GitLab，請確保`api`範圍。

INVALID_INPUT 錯誤

確認您使用的是正確的分析類型名稱。有效值為：`rapid-techdebt-analysis`、`tech-debt-comprehensive`、`security`、`agentic-readiness`、`modernization-readiness`、`custom`。

修復期間的許可錯誤

修復會建立分支和提取/合併請求，這需要對儲存庫的寫入存取權。使用寫入許可更新您的權杖。對於 GitHub，請確保完整`repo`範圍。對於 GitLab，請確保`api`範圍。對於 Bitbucket，請確保`write:repository:bitbucket`和 `write:pullrequest:bitbucket`範圍。

安全代理程式設定失敗

確認您的 IAM 使用者或角色具有 安全代理程式設定區段中列出的必要 AWS CloudFormation IAM 和 Amazon S3 許可AWS 轉型持續現代化的運作方式。使用 檢查狀態`atx ct setup security-agent --status`。

區域中無法使用安全分析或安全代理程式設定

`security` 分析類型不適用於加拿大（中部）()`ca-central-1`、歐洲（倫敦）(`eu-west-2`) 或亞太區域（首爾）()`ap-northeast-2`。`atx ct setup security-agent` 從支援的 區域執行

`security` 分析和 。其他分析類型不受影響。請參閱 的安全代理程式設定一節AWS 轉型持續現代化的運作方式。

遠端佈建失敗並出現許可錯誤

佈建、更新和銷毀遠端基礎設施 (`atx ct remote provision`、`update`、`teardown`) 會建立和修改 AWS CloudFormation 堆疊和 IAM 角色，且需要管理員許可。若要在已佈建且具有最低權限的基礎設施上執行分析和修復，請連接 `AWSTransformInfrastructureExecutorAccessEC2`或 `AWSTransformInfrastructureExecutorAccessBatch`。如需詳細資訊，請參閱 中的運算選項AWS 轉型持續現代化的運作方式。

遠端網路探索不會傳回任何子網路

遠端運算必須在私有子網路中執行，並`atx ct remote network discover`排除公有子網路。如果沒有私有子網路，請使用 建立聯網`atx ct remote network create`。

遠端執行無法複製儲存庫

遠端容器使用存放在 AWS Secrets Manager 中的字符。在執行遠端分析或修復`atx ct remote credentials --source` *`name`* `--token` *`token`*之前，向 註冊每個來源的字符。

排程無法執行

排程在遠端基礎設施上執行。在建立排程`atx ct remote provision`之前，使用 佈建 Amazon EC2 或 Batch 堆疊，並使用 確認已啟用排程`atx ct schedule get` *`name`*。

Web 應用程式中看不到持續現代化

如果登入 AWS Transform Web 應用程式後未出現持續現代化，請使用啟用 AWS Transform 之 的 IAM 登入 AWS 帳戶 資料登入，而非 AWS IAM Identity Center。如需這些步驟，請參閱 AWS 轉換 Web 應用程式。

遷移評估

AWS 轉換評估可協助您評估遷移內部部署基礎設施的成本、可行性和商業價值 AWS。評估透過聊天提供自動調整大小建議、多案例比較和互動式精簡。

您可以使用遷移評估來：

- 取得 Amazon RDS for SQL Server、Amazon EC2、Amazon EBS、Amazon S3 和 Amazon FSx 的成本估算
- 接收自動化適當調整大小建議
- 評估商業價值和永續性影響
- 並排比較多個遷移案例
- 透過聊天以互動方式精簡評估
- 產生執行簡報和詳細報告

先決條件

建立遷移評估之前，請確認您有下列項目：

- AWS 轉換工作區
- 支援格式的庫存資料，或者您可以透過聊天使用粗略估算
- 建立和執行評估的適當許可

遷移評估的運作方式

遷移評估遵循結構化工作流程，引導您從初始資料上傳到最終可交付的產生。

若要完成遷移評估

1. 在 AWS 轉換工作區中建立遷移評估任務。
2. 上傳您的現場部署庫存資料。
3. 檢閱 AWS Transform 從資料產生的探索結果。
4. 透過排除伺服器或調整群組來管理庫存範圍。

5. 使用定價和基礎設施假設來設定您的評估案例。
6. 執行評估。
7. 透過聊天檢閱和精簡結果。

檢閱結果之後，您可以建立其他案例、比較案例，以及產生可交付成果，例如簡報和報告。

上傳庫存資料

AWS 轉換接受來自多個來源的庫存資料。下表列出支援的資料格式。

資料來源	說明
AWS 轉換探索工具匯出	AWS 轉換探索工具探索的自動化伺服器庫存
RVTools	從 VMware 環境以 ZIP/CSV 或 Excel 格式匯出。同時支援完整匯出和僅限 vInfo 匯出。
CMDB 資料	組態管理資料庫匯出
合作夥伴探索工具	來自 AWS 合作夥伴探索工具的資料
遷移評估器	來自遷移評估器主控台的 Quick Insights 檔案
MPA 格式	遷移產品組合評估匯入檔案
AWS 轉換資料範本	從 AWS 轉換評估資料範本建立的 Microsoft Excel 檔案

AWS 轉換會在擷取期間自動識別檔案格式。擷取程序會驗證您的資料、在某些欄位遺失時接受部分資料，並支援增量上傳。您可以隨時上傳其他檔案來補充庫存。

檢閱探索結果

AWS 轉換處理清查資料後，會產生探索摘要。此摘要包含以下資訊：

- 作業系統的伺服器計數
- 實體和虛擬伺服器明細

- SQL Server 偵測
- 儲存摘要
- 資料品質警告

檢閱探索結果，確認 AWS 轉換已正確識別您的基礎設施，然後再繼續評估。

管理庫存範圍

檢閱探索結果後，您可以縮小評估範圍。使用下列動作來管理您的庫存範圍：

- 查詢特定伺服器或工作負載的庫存
- 從評估範圍中排除伺服器
- 檢閱伺服器群組和應用程式相依性
- 識別 SQL Server 工作負載以進行專門評估

設定評估案例

執行評估之前，請設定 AWS Transform 用來產生建議的假設。您可以隨時修改這些假設，並使用不同的組態執行新的案例。

下表列出可用的假設類別。

假設	說明
定價方式	資料庫 Savings Plans （適用於 Amazon RDS for SQL Server)、隨需或預留執行個體
目標 AWS 區域	您計劃託管遷移工作負載 AWS 區域 的 。
執行個體類型排除	要從建議中排除的 Amazon EC2 執行個體系列或類型
Amazon EBS 組態	儲存體的磁碟區類型和效能設定
SQL Server 授權	為 Amazon RDS for SQL Server 使用自有媒體 (BYOM) 或已包含授權 (LI)；為 EC2 上的 SQL Server 使用已包含授權 (LI) 或自有授權 (BYOL)

評估功能

AWS 轉換評估涵蓋遷移的多個維度。以下各節說明每個評估功能。

Amazon EC2 大小適中

AWS Transform 會分析您的內部部署伺服器規格，並建議適當大小的 Amazon EC2 執行個體。建議說明 CPU、記憶體和效能需求。

Amazon EBS 儲存體

AWS Transform 會根據您目前的儲存用量和效能需求，建議 Amazon EBS 磁碟區類型和組態。

Amazon FSx

AWS Transform 會評估檔案儲存工作負載，並提供 Amazon FSx 遷移的建議，包括支援 Amazon FSx 檔案系統類型的成本估算。

Amazon RDS for SQL Server

AWS Transform 會評估將內部部署 SQL Server 資料庫遷移至 Amazon RDS for SQL Server 的成本。使用 AI 代理程式時， AWS Transform 會分析您的內部部署 SQL Server 環境，並在幾分鐘內提供完整的遷移商業案例，並根據您的工作負載需求提供運算和記憶體建議，讓您避免過度佈建，而且只需支付所需的費用。

RDS for SQL Server 評估包含下列功能：

- 使用自有媒體 (BYOM) 授權，可讓您使用現有的 SQL Server 授權
- 已包含授權 (LI) 授權選項
- 使用 Database Savings Plans 進行成本最佳化，相較於隨需定價，可節省高達 20% 的成本
- AWS Migration Acceleration Program (MAP) 的資格評估，可提供抵用金和支援來抵銷遷移成本

您可以使用任何支援的資料格式啟動 RDS for SQL Server 評估，包括 RVTools 匯出、組態管理資料庫 (CMDB) 資料、從 AWS 轉換探索工具匯出，以及其他第三方探索工具。建立假設情境，以比較多個成本模型與自訂假設，包括區域、資源使用率和定價條件。

範例提示：

- 「估計將我的 SQL Server 資料庫遷移至 RDS for SQL Server 的成本」
- 「比較 RDS for SQL Server 的 BYOM 與包含授權定價」
- 「顯示 RDS 工作負載的資料庫 Savings Plans 選項」

Amazon EC2 SQL Server

AWS Transform 會評估 SQL Server 工作負載，並提供在 Amazon EC2 上執行 SQL Server 的建議，包括授權分析和專用主機映射。

內部部署定價

AWS 轉換會預估您目前的現場部署成本，以提供與 AWS 定價比較的基準。您可以透過聊天進行整體成本調整。內部部署成本調整反映在 PDF 報告和聊天回應中，但不反映在 PPTX 匯出中。

範例提示：

- 「將現場部署伺服器成本更新為每月每部伺服器 500 美元」
- 「每年增加 50，000 美元的資料中心設施成本」

永續性

AWS 轉換會預估遷移至 所產生的碳足跡減少 AWS。您可以透過聊天探索永續性指標。

嘗試提示，例如：

- 「顯示此遷移的預估減碳量」
- 「在 上我的工作負載的能源效率改善是什麼 AWS？」

商業價值評估

AWS Transform 會評估比基礎設施成本節省更多遷移的商業價值。評估涵蓋員工生產力、彈性和業務敏捷性。

以下是一些範例提示：

- 「從遷移到 的預估員工生產力提高 AWS」
- 「遷移後我可以預期哪些彈性改善？」

- 「顯示此遷移的業務敏捷性優勢」

網路成本

AWS 轉換會預估遷移的網路相關成本，包括資料傳輸和連線需求。

支援成本

AWS 轉換會根據您選取的 AWS 支援層，在評估中包含支援計劃成本。

最終使用者運算

AWS Transform 會評估最終使用者運算工作負載，並提供 AWS 最終使用者運算服務的建議。

使用聊天式評估

您可以透過聊天與 AWS 轉換互動，以建立和精簡評估。聊天支援三種互動模式。

您可以繼續對話，以反覆方式精簡評估。 AWS Transform 會維護訊息的內容，並根據您的輸入更新評估結果。

資料有限的粗略估算

您可以在聊天中描述您的環境，而無需上傳詳細的庫存檔案，以取得粗略的成本估算。粗略估算是一項獨立功能，無法與透過聊天上傳的庫存資料或資料擴充結合。

您可以使用如下的提示：

- 「我有 200 個 Windows 伺服器和 150 個 Linux 伺服器，預估我的 AWS 成本」
- 「為我提供遷移 500 個 VMs 到 的粗略估計 AWS」
- 「平均 8 個 CPUs 和 32 GB RAM 的 50 個伺服器的預估成本」

透過聊天新增庫存

您可以直接透過聊天提供庫存詳細資訊，以補充或取代上傳的檔案。

使用如下所示的提示：

- 「包含在 4 個 CPUs且具有 128 GB RAM 的資料庫伺服器」

- 「新增 20 個執行 Linux 的 Web 伺服器，其中包含 4 CPUs 和 16 GB RAM」

修改成本和新增服務

您可以調整內部部署成本，並透過聊天將 AWS 服務新增至您的評估。

內部部署調整的範例提示：

- 「將內部部署成本增加 15%，以考慮即將進行的硬體重新整理」
- 「為內部部署基準增加 100，000 美元的年度維護成本」

您也可以為 AWS 轉換評估未完全支援的 AWS 服務新增粗略的成本預估。這可提供更完整的分析，但這些預估值不如自動化建議準確。

- 「為所有遷移伺服器新增 AWS 備份成本」
- 「在預估中包含 Amazon CloudWatch 監控成本」
- 「為 10 Gbps 連線新增 AWS Direct Connect 成本」

比較案例

您可以使用不同的假設建立多個評估案例，並將其進行比較，以識別最佳的遷移策略。

建立案例

嘗試提示，例如：

- 「建立 BYOM 案例以將 SQL Server 資料庫遷移至 RDS for SQL Server」
- 「使用 RDS for SQL Server 的資料庫Savings Plans建立案例」
- 「在 EC2 上為所有 SQL Server 工作負載建立 LI 案例」
- 「使用 us-west-2 中的所有工作負載建立案例」

執行比較

以下是一些範例提示：

- 「在所有案例中顯示成本比較」

- 「哪個案例擁有最低的總擁有成本？」

假設分析

建立特定變更的影響模型，而不建立新的案例。

範例提示：

- 「如果將 SQL Server 工作負載移至 RDS for SQL Server 而不是 EC2，該怎麼辦？」
- 「BYOM 與 RDS for SQL Server 包含的授權之間有何成本差異？」
- 「如果我從遷移中排除 50 個最小的伺服器該怎麼辦？」
- 「如果我只使用儲存體最佳化執行個體，該怎麼辦？」
- 「從 gp3 移至 io2 磁碟區有何影響？」

產生交付項目

完成評估後，您可以產生多種格式的交付項目。下表說明可用的輸出格式。

格式	說明	自訂
PPTX (PowerPoint)	具有摘要調查結果和建議的執行簡報	固定結構
XLSX (Excel)	具有伺服器層級建議和成本明細的詳細資料匯出	固定結構
PDF	報告文件	可透過聊天自訂

相關主題

- 開始使用
- 自訂任務
- 探索工具

探索工具

AWS Transform 探索工具可協助您自動探索組織中的伺服器庫存，以準備遷移。此工具支援 VMware vCenter、Microsoft Hyper-V 和匯入的伺服器。若要使用探索工具，您可以設定一或多個探索來源，讓工具執行，然後在探索的庫存窗格中檢閱結果。

設定探索來源之後，探索工具會開始收集資訊。探索工具完整分析網路所需的時間取決於您環境的大小。對於定向遷移商業案例，您可以使用工具在伺服器集合完成後產生的遷移產品組合評估 (MPA) 檔案。

探索工具工作流程

探索工具工作流程包含兩種類型的活動：

- 組態活動
- 資料檢閱和使用

下列步驟說明如何安裝和使用 探索工具，並使用收集的資料：

1. 安裝 探索工具。
2. 設定探索來源。您可以透過 CSV 檔案匯入設定下列一或多個項目：VMware vCenter、Microsoft Hyper-V 主機或伺服器。資料探索會在您設定任何來源後開始。
3. 設定作業系統存取，然後檢閱伺服器、資料庫和網路連線的集合狀態。
    - 視需要調整作業系統登入資料。
4. （選用）設定 Oracle 登入資料以啟用直接 SQL 集合，或透過 SSH 或 WinRM 使用作業系統層級的備用偵測。
5. 若要產生遷移商業案例，請將 .zip 檔案上傳至遷移評估，或將其解壓縮並從 mpa_exports 目錄上傳 MPA 檔案。匯出包含所有已設定來源的資料，並包含 VMware、Hyper-V 和匯入伺服器的 MPA 檔案。

探索工具支援下列探索路徑：

- VMware vCenter 自動探索 – 自動探索由 VMware vCenter 管理的伺服器。
- Hyper-V 自動探索 – 自動探索由 Microsoft Hyper-V 主機管理的伺服器。

- 伺服器匯入 – 透過 CSV 檔案手動匯入伺服器庫存。

設定 探索工具

先決條件

以下是使用 AWS Transform 探索工具的先決條件：

一般先決條件

- 此工具需要 4 個 vCPU、16 GB RAM 和 35 GB 硬碟。
- DHCP 必須在網路中可用於探索工具 VM。
- 此工具會使用集中式方法收集資料。範圍內的伺服器必須允許來自探索工具 VM 的傳入連線（支援預設連接埠、自訂連接埠組態）：
  - Linux – SSH TCP/22
  - Windows – 適用於 HTTP 的 TCP/5985、適用於 HTTPS 的 TCP/5986
  - SNMP – UDP/161（僅用於網路集合，而非作業系統指標）
- 對於 Linux，可以使用 SSH 連線到伺服器的使用者帳戶。探索工具會透過 SSH 執行命令，用於網路收集和作業系統指標。大多數命令會以一般使用者身分執行。如果無法使用 sudo，則少量命令會嘗試 sudo 並自動回復：`dmidecode`（伺服器 UUID 和製造商）、`lvdisplay`(LVM 偵測）和 `ss`或 `netstat`（具有程序資訊的網路連線）。如果沒有 sudo，探索工具仍會收集大部分的資料，但 UUID、LVM 和程序層級網路詳細資訊將遺失。我們建議為 SSH 使用者設定無密碼 sudo，以確保完整的資料收集。如需完整明細，請參閱 the section called “所需的許可”。

VMware 先決條件

- VMware vCenter Server 6.5、6.7、7.0 或 8.0 版。
- 將 OVA 部署至 VMware vCenter 的許可。
- 對於 VMware vCenter Server 設定，具有在根資料中心層級指派的唯讀角色的 vCenter 使用者。如需詳細資訊，請參閱the section called “所需的許可”。

Hyper-V 先決條件

- 啟用 Hyper-V 角色的 Windows Server。
- 在 Hyper-V 主機上啟用 WinRM。

- 使用者帳戶，是每個 Hyper-V 主機上遠端管理使用者、Hyper-V 管理員和效能監控使用者群組的成員，具有`root\cimv2`命名空間的 WMI 讀取存取權。 如需詳細資訊，請參閱the section called “所需的許可”。
- 支援的身分驗證：NTLM （僅限 HTTPS) 和 Kerberos (HTTP 或 HTTPS)。

伺服器匯入先決條件

- 具有伺服器主機名稱或 IP 地址和登入資料名稱 （選用） 的 CSV 檔案，對應至在探索工具上設定或要設定的作業系統登入資料易記名稱。CSV 必須使用下列標頭：

```
hostname_or_ip,os_credential_name,oracle_credential_name
```

- 伺服器必須可從探索工具 VM 連線。預設連接埠：適用於 Linux 的 SSH 連接埠 22、適用於 Windows 的 WinRM 連接埠 5985/5986。支援自訂連接埠。

Linux 安裝程式先決條件

- 支援的 Linux 發行版本：Amazon Linux 2、Amazon Linux 2023、RHEL 8–9、Rocky Linux 8–9、AlmaLinux 9、Ubuntu 20.04–24.04、Debian 10–12 或 SLES 15 SP5。
- 最少 4 個 vCPU、16 GB RAM、35 GB 可用磁碟空間。
- 連接埠 5000 必須可用 （不適用於其他 服務）。
- 服務管理需要 systemd。
- 探索工具 VM 必須具有目標基礎設施的網路存取權。預設連接埠：連接埠 443 上的 vCenter、連接埠 5985/5986 上的 Hyper-V 主機、連接埠 22 上的伺服器。SSH、WinRM 和 SNMP 支援自訂連接埠。

Oracle 資料庫先決條件

- 從探索工具到連接埠 1521 （或自訂連接埠） 上 Oracle 主機的網路存取。
- 支援的 Oracle 版本：您可以透過直接 SQL 連線收集 Oracle Database 12c 版本 1 (12.1) 和更新版本。作業系統層級備用偵測適用於所有 Oracle 版本。
- 具有 SELECT_CATALOG_ROLE 授予的唯讀 Oracle 服務帳戶。如需詳細資訊，請參閱the section called “Oracle 資料庫 (SQL)”。
- 對於作業系統層級備用偵測：SSH 或 WinRM 存取 Oracle 主機 （使用現有的作業系統登入資料）。

在 VMware 上部署

VMware 虛擬機器規格

- 作業系統 – Amazon Linux 2023
- RAM – 16 GB
- CPU – 4 個核心
- 磁碟 – 35 GB
- VMware 需求 – 請參閱在 VMware 上執行 AL2023 的 VMware 主機需求

部署 VMware OVA

1. 從此 URL 下載 OVA 檔案：https：//https://s3.us-east-1.amazonaws.com/atx.discovery.collector.bundle/releases/latest/AWS-Transform-discovery-tool.ova
2. 以 VMware 管理員身分登入 vCenter。
3. 使用下列其中一種方法來安裝 OVA 檔案：

   a. 使用 UI：選擇檔案，選擇部署 OVF 範本，選取您在步驟 1 中下載的探索工具 OVA 檔案，然後完成精靈。確定伺服器管理儀表板中的代理設定已正確設定。

   b. 使用命令列：若要從命令列安裝探索工具 OVA 檔案，請下載並使用 VMware Open Virtualization Format Tool (ovftool)。若要下載 ovftool，請從 OVF 工具文件頁面選取版本。這是使用 ovftool 命令列工具安裝探索工具 OVA 檔案的範例。

   ```
   ovftool --acceptAllEulas --name='discovery tool' --datastore=datastore1 -
   dm=thin AWS-Transform-discovery-tool.ova 'vi://username:password@vcenterurl/
   Datacenter/host/esxi/'
   ```

   範例中可取代值的描述：

   - 名稱是您要用於探索工具 VM 的名稱。
   - 資料存放區是 vCenter 中資料存放區的名稱。
   - OVA 檔案名稱是下載的探索工具 OVA 檔案的名稱。
   - 使用者名稱/密碼是您的 vCenter 登入資料。
   - vcenterurl 是 vCenter 的 URL。
   - vi 路徑是 VMware ESXi 主機的路徑。

4. 在 vCenter 中尋找已部署的探索工具。在 VM 上按一下滑鼠右鍵，然後選擇開啟電源、開啟電源。
5. 幾分鐘後，探索工具的 IP 地址會顯示在 vCenter 中。您可以使用此 IP 地址連線到 探索工具。

在 Hyper-V 上部署

Hyper-V 虛擬機器規格

- 作業系統 – Amazon Linux 2023
- RAM – 我們建議配置至少 16 GB
- CPU – 我們建議配置至少 4 個核心
- 磁碟 – 35 GB（包含在 VHD 中）
- Hyper-V 需求 – 請參閱在 Hyper-V 上執行 AL2023 的 Hyper-V 主機需求

部署 Hyper-V VHD

1. 從此 URL 下載 VHD 檔案：https：//https://s3.us-east-1.amazonaws.com/atx.discovery.collector.bundle/releases/latest/AWS-Transform-discovery-tool.vhd
2. 將 VHD 檔案複製到已啟用 Hyper-V 角色的 Windows Server 機器。
3. 開啟 Hyper-V Manager。
4. 選擇新增，然後選擇虛擬機器。
5. 完成設定精靈。在指定產生頁面上，選取產生 1。第 2 代虛擬機器不支援 VHD 格式。在指派記憶體頁面上，配置至少 16384 MB。在連線虛擬硬碟頁面上，選擇使用現有的虛擬硬碟，然後選取您複製的 VHD 檔案。
6. 啟動 VM。幾分鐘後，請檢查 Hyper-V Manager 中 VM 的網路索引標籤，以尋找 IP 地址，或連線至 VM 主控台並執行 `ip addr`。您可以使用此 IP 地址連線到 探索工具。

在 Linux 上部署

探索工具可作為獨立 Linux 安裝程式使用，以在支援的 Linux 發行版本上進行部署。當您想要直接在現有的 Linux 伺服器上安裝探索工具，而不是部署虛擬機器時，請使用此選項。

Linux 伺服器規格

- RAM – 我們建議配置至少 16 GB

- CPU – 我們建議配置至少 4 個核心
- 磁碟 – 35 GB

支援的發行版

- Amazon Linux – Amazon Linux 2、Amazon Linux 2023
- Red Hat Enterprise Linux 和衍生產品 – RHEL 8–9、Rocky Linux 8–9、AlmaLinux 9
- Ubuntu – 20.04、22.04、24.04
- Debian – 10、11、12
- SUSE – SLES 15 SP5

安裝 探索工具

從此 URL 下載安裝程式指令碼：https：//https://s3.us-east-1.amazonaws.com/atx.discovery.collector.bundle/releases/latest/AWS-Transform-discovery-tool.sh

在 Linux 上安裝 探索工具

1. 將安裝程式指令碼下載到您的 Linux 伺服器。

```
curl -O https://s3.us-east-1.amazonaws.com/atx.discovery.collector.bundle/releases/latest/AWS-Transform-discovery-tool.sh
chmod +x AWS-Transform-discovery-tool.sh
```

2. （選用）執行相容性檢查，以確認您的系統符合需求。

```
sudo ./AWS-Transform-discovery-tool.sh check
```

3. 安裝 探索工具。請選擇下列其中一個選項：

   選項 1：使用自動相依性安裝來安裝（建議）

   此選項會在安裝服務之前自動安裝任何缺少的系統相依性。

```
sudo ./AWS-Transform-discovery-tool.sh install --install-deps
```

   選項 2：無需自動安裝相依性即可安裝

此選項會檢查是否存在缺少的相依性，並在缺少關鍵相依性時，以手動安裝指示顯示錯誤。如果您的組織限制自動套件安裝，而且您偏好手動管理系統套件，請使用此選項。

```
sudo ./AWS-Transform-discovery-tool.sh install
```

4. 啟動 探索工具服務。

```
sudo ./AWS-Transform-discovery-tool.sh start
```

5. 存取位於 的 探索工具https://*ip_address*:5000。

若要解除安裝 探索工具，請執行 `sudo ./AWS-Transform-discovery-tool.sh uninstall`。

您也可以使用下列命令來管理服務：

- `sudo ./AWS-Transform-discovery-tool.sh status` – 檢查服務是否正在執行。
- `sudo ./AWS-Transform-discovery-tool.sh stop` – 停止服務。
- `sudo ./AWS-Transform-discovery-tool.sh logs` – 檢視服務日誌。

系統相依性

安裝程式會檢查下列系統相依性：

相依性	嚴重性	用途
OpenSSL	嚴重	產生資料庫加密金鑰
libcrypt	嚴重	Python 執行時間需要
Kerberos 程式庫	警告	對 Windows 伺服器進行 Kerberos 身分驗證時需要。如果沒有這樣做，NTLM 和基本身分驗證仍然有效。

探索工具需要關鍵相依性才能啟動。如果缺少它們，且您選擇選項 2（不含 `--install-deps`），安裝程式會顯示錯誤，其中包含手動安裝它們的說明。警告層級相依性是選用的 — 安裝程式會警告您，但會繼續安裝。

> **Note**
>
> 安裝程式會檢查系統相容性，包括 glibc 版本和系統可用性。在具有 systemd 250 或更新版本的系統上 (Amazon Linux 2023、RHEL 9、Rocky 9、AlmaLinux 9、Ubuntu 24.04+、Debian 12+)，會使用 systemd-creds 靜態加密資料庫加密金鑰。在較舊的系統上，加密金鑰會儲存為受許可保護的檔案。

設定 探索工具

存取 探索工具主控台

1. 在 Web 瀏覽器存取中：`https://ip_address:5000`，其中 *ip_address* 是部署探索工具中探索工具的 IP 地址。探索工具使用 HTTPS 連線的自我簽署憑證，這會導致安全警告。選擇接受風險並繼續前往探索工具主控台。
2. 如果您是第一次存取探索工具主控台，請建立探索工具登入密碼。建立密碼，以供日後登入時使用。

> **Important**
>
> 請記住此密碼 - 沒有密碼復原機制。

存取 探索工具 VM

- 探索工具 VM 預設會隨附使用者名稱和密碼 (「探索」、「密碼」)。為了增強安全性，我們建議您在透過 Hypervisor 主控台登入 VM `sudo passwd discovery`之後使用 更新密碼 （例如，vSphere Client for VMware 或 Hyper-V Manager for Hyper-V)。
- SSH 存取預設為停用。使用者可以使用預先設定`enablessh`和別名來啟用/停用探索工具 `disablessh` VM 的 SSH 存取。啟用 SSH 存取`ssh discovery@<VM-IP>`後，使用者可以透過將 SSH 傳入 VM。我們鼓勵使用者在大多數情況下停用 SSH 存取，並只在主動要求時啟用它。執行時會強制執行密碼變更`enablessh`。
- 若要存取位於 的 探索工具資料目錄`/home/ec2-user/.local/share/DiscoveryTool`，建議您`ec2-user`執行 以切換到 `sudo su ec2-user`。

設定 Kerberos 身分驗證

Kerberos 身分驗證是建議從 探索工具連線至 Windows 伺服器的方法。探索工具 VM 使用原生 Amazon Linux 2023 Kerberos 程式庫來驗證 Active Directory 網域。

以下是探索工具 VM 上 Kerberos 身分驗證的重點：

- 使用 `kinit`命令來取得 Kerberos 票證`klist`並驗證票證。
- Kerberos 組態檔案位於 `/etc/krb5.conf`。
- 設定探索工具之前，請在探索工具 VM 上驗證 是否從 CLI `kinit`成功。

Kerberos 先決條件

設定 Kerberos 身分驗證之前，請確認您具有下列資訊和網路連線能力。

1. 從您的 Active Directory 管理員取得下列資訊：
   - Kerberos 領域名稱 （通常是您大寫的網域名稱，例如 `EXAMPLE.COM`)。
   - Key Distribution Center (KDC) 的主機名稱或 IP 地址，通常是網域控制站 （例如 `dc01.example.com`)。
   - 具有對目標 Windows 伺服器進行身分驗證之許可的服務帳戶。
2. 確認探索工具 VM 具有下列項目的網路連線能力：
   - 用於 Kerberos 身分驗證的連接埠 88 (TCP 和 UDP) 上的 KDC。
   - WinRM 連接埠上的目標 Windows 伺服器 (HTTP 為 5985，HTTPS 為 5986)。

設定 Kerberos

完成下列步驟，以在探索工具 VM 上設定 Kerberos 身分驗證。

1. 探索工具 VM 的 SSH。

   ```
   ssh discovery@<discovery-tool-vm-ip>
   ```

2. 在 編輯 Kerberos 組態檔案`/etc/krb5.conf`。

   ```
   sudo nano /etc/krb5.conf
   ```

   新增下列組態，將預留位置值取代為您的環境詳細資訊。

```
[libdefaults]
    default_realm = EXAMPLE.COM
    dns_lookup_realm = false
    dns_lookup_kdc = true

[realms]
    EXAMPLE.COM = {
        kdc = dc01.example.com
    }

[domain_realm]
    .example.com = EXAMPLE.COM
    example.com = EXAMPLE.COM
```

> **Important**
>
> Kerberos 區分大小寫。領域名稱必須為大寫（例如 EXAMPLE.COM，而非 example.com)。[domain_realm] 區段中的網域名稱必須為小寫。

多個 Active Directory 網域

探索工具支援不同 Active Directory 網域的多個 Kerberos 登入資料。每個登入資料都會獨立驗證，因此您可以正常設定多個登入資料，且會自動隔離。

如果您在多個網域中有伺服器，請為 /etc/krb5.conf 檔案中的每個領域新增項目：

```
[libdefaults]
    default_realm = DEV.COMPANY.COM
    dns_lookup_realm = false
    dns_lookup_kdc = true

[realms]
    DEV.COMPANY.COM = {
        kdc = dc01.dev.company.com
    }
    PROD.COMPANY.COM = {
        kdc = dc01.prod.company.com
    }
```

```
[domain_realm]
    .dev.company.com = DEV.COMPANY.COM
    dev.company.com = DEV.COMPANY.COM
    .prod.company.com = PROD.COMPANY.COM
    prod.company.com = PROD.COMPANY.COM
```

3. 執行 `kinit`命令，確認您可以取得 Kerberos 票證。

```
kinit username@REALM.COM
```

出現提示時輸入密碼。如果命令完成時沒有發生錯誤，表示身分驗證成功。

4. 執行 `klist`命令來驗證票證。

```
klist
```

預期的輸出類似於以下內容。

```
Ticket cache: FILE:/tmp/krb5cc_1000
Default principal: username@REALM.COM

Valid starting       Expires              Service principal
01/01/2025 12:00:00  01/01/2025 22:00:00  krbtgt/REALM.COM@REALM.COM
```

5. 使用與 相同的區分大小寫主體來設定探索工具 `kinit`（例如，`username@REALM.COM`)。

如果您的環境已針對 Kerberos 服務探索設定 DNS SRV 記錄，則可能不需要明確的`krb5.conf`組態。如需 Kerberos 組態選項的詳細資訊，請參閱 MIT Kerberos krb5.conf 文件和範例 krb5.conf 檔案。

從加入網域的機器尋找 Kerberos 組態

如果您沒有 Kerberos 組態詳細資訊，您可以從加入網域的 Windows 機器擷取詳細資訊。從加入網域的機器上的命令提示字元執行下列命令。

若要尋找網域名稱，請執行下列命令。

```
echo %USERDNSDOMAIN%
```

輸出範例：

```
EXAMPLE.COM
```

若要尋找網域控制器主機名稱，請執行下列命令。

```
nltest /dsgetdc:EXAMPLE.COM
```

輸出範例：

```
           DC: \\dc01.example.com
      Address: \\10.0.1.100
     Dom Guid: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
     Dom Name: EXAMPLE.COM
  Forest Name: example.com
 Dc Site Name: Default-First-Site-Name
Our Site Name: Default-First-Site-Name
        Flags: 0xe00033fd
The command completed successfully
```

將輸出映射到您的`krb5.conf`組態，如下所示：

- 領域 – 使用 `%USERDNSDOMAIN%`中的大寫值 （ 例如，`EXAMPLE.COM`)。
- KDC – 使用輸出中的 DC 主機名稱 `nltest` (例如 `dc01.example.com`)。

設定 vCenter 存取

1. 在探索工具頁面的步驟 1 下。設定探索來源，選擇設定來源。
2. 在設定探索來源頁面上，提供易記名稱、vCenter FQDN/IP、使用者名稱和密碼。
3. 選擇 Save configuration (儲存組態)。

   探索工具會開始收集 vCenter 資訊，如探索的庫存中所述。

在初始組態後，在探索工具狀態框架中選擇編輯 vCenter 存取，以變更您的 vCenter 存取設定。

探索工具會從所有設定的 vCenter 伺服器平行收集。如果在收集期間無法連線一個 vCenter 伺服器，工具會報告部分成功，並繼續從剩餘的 vCenter 伺服器收集。

如果 VM 出現在多個 vCenter 伺服器上 （ 例如，由於共用 ESXi 主機或跨 vCenter vMotion)，探索工具會自動刪除重複VMs。每個唯一的 VM 只會在庫存中出現一次。

設定 Hyper-V 存取

1. 在探索工具頁面的步驟 1 下。設定探索來源，選擇設定來源。
2. 在設定探索來源頁面上，提供易記的名稱、主機 FQDN 或 IP 地址、身分驗證類型 (NTLM 或 Kerberos)、WinRM 使用者名稱和 WinRM 密碼。
3. 選擇 Save configuration (儲存組態)。

   探索工具會開始收集 Hyper-V 資訊，如探索的庫存中所述。

在您儲存登入資料後，集合會自動開始。

對於 Hyper-V 容錯移轉叢集，您可以在同一個叢集中新增多個主機。此工具會自動刪除出現在多個主機上的 VMs。

匯入伺服器

1. 從探索工具首頁導覽至匯入伺服器頁面。
2. 使用下列資料欄準備 CSV 檔案： `hostname_or_ip`（必要）、 `os_credential_name`（選用）和 `oracle_credential_name`（選用）。
   - `hostname_or_ip` 值必須是有效的 IPv4 地址或完整網域名稱 (FQDN)。
   - 如果提供此`os_credential_name`值，則必須符合您已設定之作業系統登入資料的易記名稱 (SSH、WinRM 或 SNMP)。對於尚未設定作業系統登入資料的伺服器，請保留空白。
   - 如果提供此`oracle_credential_name`值，則必須符合您已設定的 Oracle 登入資料的易記名稱。
3. 上傳 CSV 檔案。工具會驗證所有資料列，並在任何資料列無效時拒絕檔案。

成功匯入後，如果已設定作業系統登入資料，工具會自動開始為匯入的伺服器收集資料庫、網路和作業系統指標。如果您上傳另一個 CSV 檔案，則會更新現有的記錄而不建立重複項目，並將新的記錄合併到清查中。

將自我簽署憑證授權單位匯入探索工具（選用）

當您使用由自我簽署憑證授權單位 (CA) 簽署的 WinRM HTTPS 憑證透過 HTTPS 和目標伺服器使用 WinRM，而且您想要在探索工具上啟用「驗證伺服器 SSL 憑證」時，這是必要的。 WinRM

先決條件

1. 用於在目標伺服器上簽署 WinRM HTTPS 憑證的自我簽署 CA 憑證
2. PEM 格式的憑證 (.pem 或 .crt 延伸）

若要在探索工具 VM 上匯入自我簽署憑證授權單位：

1. Ssh to Discovery 工具 VM
2. 將簽署目標伺服器 WinRM 憑證的 CA 憑證 (CA) 放入探索工具 VM `/etc/pki/ca-trust/source/anchors/`上的信任存放區目錄。例如：`sudo cp winrm-ca.pem /etc/pki/ca-trust/source/anchors/winrm-ca.pem`。注意：如果您的目標伺服器使用不同 CAs憑證，請將所有相關 CA 憑證複製到此目錄。
3. 更新憑證信任存放區： `sudo update-ca-trust`
4. 重新啟動 VM
5. （選用）若要確認憑證已成功匯入，您可以執行下列命令。 `sudo trust list –filter=ca-anchors | grep -A 5 "<certificate_name>"`

請參閱 Windows Remote Management 的安裝和組態

設定作業系統存取的探索工具

設定作業系統存取，以便探索工具可以：

- 探索資料庫以執行資料庫評估並協助 VM 遷移，
- 追蹤庫存中伺服器之間的網路連線，包括與每個連線相關聯的程序，以協助應用程式相依性映射和波規劃。只有兩個端點都位於探索工具清查中的連線才會包含在內。

啟用探索工具作業系統存取

1. 導覽至設定作業系統存取頁面，以提供 Windows 和 Linux 登入資料。
2. 選擇您要為其新增登入資料的通訊協定。
3. 提供所選通訊協定所需的登入資料。
4. 選取自動連線以啟用探索工具，在探索的伺服器上嘗試所有提供的登入資料，直到找到每個伺服器的相符登入資料為止。

   如需自動連線功能的重要安全建議，the section called “謹慎使用自動連線功能”請參閱 。

5. 選擇設定並連線。

當作業系統比對程序完成時，您會看到一則訊息，指出資料收集正在進行中，以及找不到登入資料比對之伺服器的相關錯誤。

支援的通訊協定設定

您必須在目標伺服器上設定 WinRM、SSH 和 SNMP 通訊協定，探索工具才能與其通訊。

設定 WinRM 和 WMI

WinRM 會自動與目前支援的所有 Windows 作業系統版本一起安裝。

若要驗證或編輯 WinRM 組態，請使用`winrm`命令列工具：

- 驗證已安裝的 WinRM 接聽程式： `winrm enumerate winrm/config/listener`
- 驗證 WinRM 組態： `winrm get winrm/config`
- 設定 WinRM 的範例命令： `winrm quickconfig -transport:https`

接聽程式連接埠

預設 HTTP 連接埠為 5985；HTTPS 為 5986。您可以視需要使用其他連接埠。連接埠必須在探索工具和目標伺服器之間開啟。

加密

探索工具使用加密的 WinRM 通訊。我們建議目標伺服器上的 WinRM 接聽程式也使用加密： `winrm set winrm/config/service '@{AllowUnencrypted="false"}'`

NTLM 與 Kerberos

探索工具支援 WinRM 身分驗證通訊協定 Kerberos 和 NTLM。NTLM 只能與 HTTPS 搭配使用，而 Kerberos 可以與 HTTP 或 HTTPS 搭配使用。

WMI 要求

探索工具會查詢下列 WMI 命名空間。WinRM 帳戶需要與您的集合模組相關的每個命名空間的讀取存取權：

WMI 命名空間	使用者：
root\cimv2	作業系統指標、Hyper-V 主機中繼資料、SQL Server 集合
root\virtualization\v2	Hyper-V VM 庫存
root\StandardCIMV2	網路集合
root\Microsoft\SqlServer\ComputerManagement*	SQL Server 集合
root\Microsoft\SqlServer\ReportServer*	SQL Server 集合 (SSRS)

針對網路集合，請確定符合下列條件：

- 允許透過 ICMP 進行網路連線
- 允許透過 TCP 連接埠 135 + 暫時性 TCP 連接埠範圍 (49152 - 65535) 進行網路連線
- 停用 UAC
- 遠端 DCOM 許可已設定
- 建立具有最少必要許可的專用服務帳戶
- 已為具有命名空間的 Windows 帳戶設定 WMI 命名空間許可：\\root\\standardcimv2、MSFT_NetTCPConnection類別

對於 SQL Server 集合，由於複雜的 WMI 物件許可要求，需要屬於本機管理員群組的 Windows 帳戶（本機或網域）。

設定 SSH

- 預設連接埠為 22。支援自訂連接埠。設定的連接埠必須在探索工具和目標伺服器之間開啟。
- 若要讓 SSH 網路集合正常運作，請提供針對無密碼 sudo 設定的使用者。
- 確定下列命令可用於目標 Linux 伺服器（在大多數發行版本上預設安裝）：ss或 netstat用於網路集合，以及 lsblk、iostat、dmidecode、ip、、、 smartctl top ps free和 df用於作業系統指標集合。

探索工具支援兩種 SSH 身分驗證方法：

選項 1：使用者名稱和密碼

提供 SSH 使用者名稱和密碼。這是預設身分驗證方法。

選項 2：SSH 私有金鑰

以 PEM 格式提供 SSH 使用者名稱和私有金鑰。若要使用此選項，請在設定 SSH 登入資料時，從身分驗證類型下拉式清單中選擇 SSH 金鑰。如果使用密碼片語加密私有金鑰，請在選用的金鑰密碼片語欄位中輸入密碼片語。

支援下列金鑰格式：

- RSA
- ECDSA
- Ed25519
- OpenSSH 格式
- PKCS#8 格式

這兩種身分驗證方法都支援自動連線。登入資料會靜態加密儲存。

設定 SNMP

- 預設連接埠為 161/UDP。支援自訂連接埠。設定的連接埠必須在探索工具和目標伺服器之間開啟。
- 對於 SNMP v2：提供可存取 TCP 連線 OIDs唯讀社群字串。
- 對於 SNMP v3：使用可存取 TCP 連線 OIDs唯讀許可，提供使用者名稱/密碼和身分驗證/權限詳細資訊

探索工具需要存取：

- "1.3.6.1.2.1.6.13.1.1." (tcpConnState)
- "1.3.6.1.2.1.6.19.1.8." (tcpConnectionProcess)
- "1.3.6.1.2.1.25.4.2.1.2." (hrSWRunName)

設定 Oracle 資料庫存取

設定 Oracle 資料庫存取，以直接透過 SQL 連線收集詳細的 Oracle 資料庫中繼資料。收集的中繼資料包括 CDB 和 PDB 拓撲、功能用量和安裝選項。此資料可協助您更準確地規劃 Oracle 資料庫遷移。您可以透過直接 SQL 連線收集 Oracle Database 12c 版本 1 (12.1) 和更新版本。作業系統層級備用偵測適用於所有 Oracle 版本。

在 探索工具中設定 Oracle 登入資料

1. 在探索工具頁面的邊欄中，選擇資料庫存取。
2. 選擇新增 Oracle 登入資料。
3. 請提供下列資訊：
   - 易記名稱 – 此登入資料的描述性名稱（例如 `Oracle Production`)。
   - 連接埠 – Oracle 接聽程式連接埠（預設 1521)。
   - 服務名稱 – 目標資料庫的 Oracle 服務名稱。
   - 使用者名稱 – Oracle 服務帳戶使用者名稱。
   - 密碼 – Oracle 服務帳戶密碼。
   - 自動連線 – 開啟此選項，針對庫存中的所有伺服器嘗試登入資料。關閉此選項，以手動將登入資料指派給特定伺服器。
4. 若要新增更多登入資料（例如，針對不同的 Oracle 環境），請再次選擇新增 Oracle 登入資料。
5. 選擇儲存。

登入資料模式

當您設定 Oracle 登入資料時，您可以選擇兩種模式：

- 手動 – 將登入資料固定到特定伺服器。探索工具只會針對該伺服器使用該登入資料。如果連線失敗，則不會發生備用。修正登入資料組態以解決問題。
- 自動連線 – 探索工具會針對庫存中的每個伺服器嘗試每個自動連線憑證。當伺服器登入資料成功時，探索工具會將該登入資料用於所有後續的集合回合。

偵測流程

當您設定 Oracle 登入資料時，探索工具會先嘗試直接 SQL 連線。如果所有資料庫登入資料都失敗，工具會透過 SSH 或 WinRM 回到作業系統層級偵測，因此您仍然可以在沒有資料庫存取權的情況下探索 Oracle 安裝。

更新探索工具

探索工具沒有自動更新功能，但您將在安裝 30 天後收到提醒通知以進行更新。建議您將應用程式保持在up-to-date，以接收最新的功能和安全性修補程式。

手動更新工具

1. 從提供的連結下載最新的探索工具映像檔案（適用於 VMware 的 OVA 或適用於 Hyper-V 的 VHD)。
2. （選用）建議您先刪除先前的探索工具映像檔案，再部署最新的。
3. 請依照部署探索工具區段中的步驟來部署更新版本。

撤銷存取

您可以個別撤銷每個探索來源的存取權。當您撤銷某個來源的存取權時，來自其他來源的資料不會受到影響。

- 撤銷 vCenter 存取 – 刪除 vCenter 登入資料和 VMware 收集的資料。不會刪除 Hyper-V 資料、匯入的伺服器資料或作業系統登入資料。
- 撤銷 Hyper-V 存取 – 僅刪除 Hyper-V 登入資料和 Hyper-V-collected。
- 刪除匯入的伺服器 – 從庫存中移除匯入的伺服器。從這些伺服器收集的下游收集資料（網路、資料庫）會保留。

探索工具的必要許可

探索工具會使用多種通訊協定連接到您的基礎設施。每個通訊協定和收集模組都需要特定的帳戶許可。本節說明完整資料收集所需的最低許可，以及在無法使用特定許可時遺失哪些資料。

VMware vCenter

探索工具會連線至連接埠 443 (HTTPS) 上的 VMware vCenter Server，並執行唯讀操作。您的 vCenter 環境不會進行任何變更。

最低必要角色：唯讀，在 vCenter 根層級指派。

唯讀角色提供探索工具收集 VM 庫存（名稱、UUID、CPU、記憶體、磁碟、網路、電源狀態、訪客作業系統）和效能指標 (CPU 使用率、記憶體使用率、磁碟 IOPS 和輸送量）所需的所有存取權。

建議：在根資料中心層級建立具有內建唯讀角色的專用 vCenter 使用者。

Hyper-V 主機 (Windows)

探索工具會透過 WinRM 連線至 Hyper-V 主機 (HTTP 為連接埠 5985，HTTPS 為連接埠 5986)，並執行 PowerShell 命令來收集 VM 庫存、主機中繼資料和儲存效能。

每個 Hyper-V 主機上所需的群組成員資格下限：

Windows 群組	為什麼需要它
遠端管理使用者	基準 WinRM 遠端存取
Hyper-V 管理員	VM 清查集合 (VM 清單、磁碟、網路、記憶體、訪客作業系統）
效能監視器使用者	儲存 I/O 效能計數器（讀取/寫入 IOPS 和每個 VM 的輸送量）

帳戶也需要主機作業系統版本和硬體 UUID `root\cimv2`命名空間的 WMI 讀取存取權。預設會將此存取權授予本機管理員，但必須針對非管理員帳戶明確設定。

建議：建立專用網域服務帳戶，並將其新增至每個 Hyper-V 主機上的遠端管理使用者、Hyper-V 管理員和效能監控使用者群組。避免使用網域管理員帳戶。

Linux 伺服器 (SSH)

探索工具會透過 SSH（連接埠 22) 連線至 Linux 伺服器，以收集作業系統指標、網路連線和伺服器庫存。大多數資料收集會以一般使用者身分執行。少量命令會嘗試sudo並在 sudo 無法使用時自動回復。

最低必要存取：可登入目標伺服器的 SSH 使用者帳戶。

建議存取：使用無密碼 sudo 設定的相同 SSH 使用者，以進行完整的資料收集。

需要 sudo 的內容，以及沒有它會發生的情況：

收集的資料	Sudo 需要？	如果沒有 sudo，您會遺失什麼
伺服器名稱、作業系統、CPU、記憶體、IP、磁碟計數	否	無 – 以一般使用者身分收集
CPU、記憶體和網路使用率	否	無 – 以一般使用者身分收集
磁碟 IOPS、輸送量和空間	否	無 – 以一般使用者身分收集
網路介面組態	否	無 – 以一般使用者身分收集
執行中程序（名稱、PID、命令）	否	無 – 以一般使用者身分收集
伺服器 UUID 和 SMBIOS UUID	是	匯出中的 UUID 欄位為空白
硬體製造商（實體與虛擬偵測）	是	在較舊的分佈上，資源類型偵測不太準確
LVM 邏輯磁碟區偵測	是	未偵測到 LVM 磁碟區；磁碟區類型可能顯示為「未知」
具有程序名稱和 PID 的網路連線	是	仍會收集連線，但不含程序屬性 (PID 和程序名稱資料欄為空白）
Oracle 資料庫作業系統層級偵測（未設定 Oracle 登入資料時的備用）	是	基本 Oracle 存在偵測 (oratab、程序監控） 在沒有 sudo 的情況下運作。詳細集合 (opatch、lsnrctl、ASM、Grid Infrastructure) 需要無密碼`sudo -u oracle`存取 Oracle 主二進位檔。

> **Note**
>
> 探索工具永遠不會因為缺乏 sudo 而完全失敗。它會收集它可以收集的內容，並報告部分結果。不過，對於最完整的資料，尤其是具有程序名稱的網路相依性映射，我們建議使用無密碼 sudo。

目標伺服器上的必要公用程式：應該可以使用下列命令（在大多數 Linux 發行版本上預設安裝）：`ss`或 `netstat`、`lsblk`、`top`、`ps`、`free`、`ip`、`df`、`hostnamecat`、、 `nproc`和 `grep`。其他資

料的選用項目： `iostat`（磁碟輸入/輸出詳細資訊）、 `dmidecode`（硬體 UUID)、 `smartctl`（磁碟介面類型）、 `lvdisplay`(LVM 偵測）。

Windows 伺服器 (WinRM) — 作業系統指標

探索工具會透過 WinRM 連線至 Windows 伺服器，以收集作業系統指標（伺服器庫存、效能、儲存、網路介面和執行中的程序）。

最低必要存取：已啟用 WinRM 的使用者帳戶，可遠端存取目標伺服器。

建議存取：本機管理員群組中用於完整資料收集的使用者。

許可層級	它啟用了哪些功能	如果沒有它，您會遺失什麼
遠端管理使用者 (WinRM 存取）	所有 Windows 資料收集	沒有從伺服器收集的資料
WMI 讀取存取 `root\cimv2`	伺服器名稱、作業系統版本、記憶體、UUID、BIOS 序列、磁碟空間	伺服器庫存欄位空白
效能監視器使用者	CPU 使用率、網路輸送量、磁碟 IOPS 和輸送量	未收集效能指標
本機管理員	執行程序擁有者名稱	已收集程序清單，但使用者/擁有者資料欄為空白

> **Note**
>
> 本機管理員成員資格會隱含授予效能監視器使用者存取權和 WMI 讀取存取權，以便滿足上述所有要求。

> **Note**
>
> 未設定 Oracle 登入資料時，Windows 上的 Oracle 資料庫作業系統層級備用偵測會使用登錄查詢和 `Get-Service` 和 `Get-Process`命令。這些命令只需要標準遠端管理使用者存取。不需要超出作業系統指標要求的額外許可。

Windows 伺服器 (WinRM) — SQL Server 集合

SQL Server 集合會探索 Windows 伺服器上的 SQL Server 執行個體、Reporting Services (SSRS) 和 Integration Services (SSIS)。

建議存取：每個目標 Windows 伺服器上本機管理員群組中的使用者。

建議使用本機管理員，因為 SQL Server 探索會查詢多個 WMI 命名空間，且某些操作需要更高的存取權：

探索到什麼	需要許可	如果沒有它，您會遺失什麼
SQL Server 資料庫引擎執行個體（版本、版本、狀態）	`root\Microsoft\SqlServer\ComputerManagement*` 命名空間的 WMI 讀取存取	未發現 SQL Server 執行個體
SQL Server Reporting Services (SSRS)	`root\Microsoft\SqlServer\ReportServer` 命名空間的 WMI 讀取存取權	未發現的 SSRS 元件
SSRS URL 和連接埠組態	提升權限（本機管理員）	缺少 SSRS URL 保留詳細資訊
SQL Server Integration Services (SSIS)	登錄檔讀取存取 (HKLM)	SSIS 版本和版本遺失
Port-to-service關聯	存取 TCP 接聽程式列舉	無法將接聽連接埠與 SQL Server 服務建立關聯

> **Note**
>
> SQL Server 集合僅限 Windows。探索工具會略過 Linux 伺服器以進行 SQL Server 探索。

Oracle 資料庫 (SQL)

Oracle 資料庫集合會直接連線至連接埠 1521（或自訂連接埠）上的 Oracle 執行個體，以收集資料庫中繼資料。探索工具不需要 DBA 或 SYSDBA 權限。

最低必要存取：具有 SELECT_CATALOG_ROLE 授權的唯讀 Oracle 服務帳戶。

探索工具不會存取 Diagnostics Pack 或調校套件檢視，因此資料收集不需要額外的 Oracle 授權。

建立帳戶的 SQL：

```
CREATE USER discovery_user IDENTIFIED BY <password>;
GRANT CREATE SESSION TO discovery_user;
GRANT SELECT_CATALOG_ROLE TO discovery_user;
```

作業系統層級備用：如果未設定資料庫登入資料或連線失敗，探索工具會使用現有的 SSH 或 WinRM 作業系統登入資料來偵測 Oracle 安裝。除了作業系統指標模組所需的許可之外，不需要額外的 Oracle 特定作業系統許可。

網路集合

網路集合會根據伺服器的作業系統使用不同的通訊協定：

伺服器作業系統	通訊協定	需要的許可
Linux	SSH	連線資料的一般使用者。無密碼 sudo 建議用於程序層級詳細資訊 (PID 和程序名稱）。
Linux	SNMPv2	可存取 TCP MIB (tcpConnState、tcpConnectionProcess) 和主機資源 MIB (hrSWRunName) 的唯讀社群字串。
Linux	SNMPv3	具有與 SNMPv2 相同 MIBs USM 使用者。支援 noAuthNoPriv、authNoPriv 和 authPriv 安全層級。
Windows	WinRM	`root\StandardCIMV2` 命名空間的 WMI 讀取存取權 (MSFT_NetTCPConnection 類別）。

快速參考：使用案例的最低許可

使用案例	Account type (帳戶類型)	最低許可
VMware VM 探索	vCenter 使用者	根資料中心層級的唯讀角色
Hyper-V VM 探索	Windows 網域或本機帳戶	遠端管理使用者 + Hyper-V 管理員 + 每個主機上的效能監控使用者
Linux 作業系統指標 — 完整資料	SSH 使用者	無密碼 sudo
Linux 作業系統指標 — 部分資料	SSH 使用者	一般使用者（無 sudo)。UUID、製造商、LVM 和網路程序資訊將會遺失。
Windows 作業系統指標 — 完整資料	WinRM 使用者	本機管理員
Windows 作業系統指標 — 基本資料	WinRM 使用者	遠端管理使用者 + WMI 讀取存取權 `root\cimv2`
SQL Server 資料庫探索	WinRM 使用者	本機管理員
Oracle 資料庫探索 (SQL)	Oracle 服務帳戶	SELECT_CATALOG_ROLE（唯讀，無 DBA 或 SYSDBA)
網路集合 — Linux (SSH)	SSH 使用者	程序層級資料的無密碼 sudo；僅限連線資料的一般使用者
網路集合 — Linux (SNMP)	SNMP 社群字串或 USM 使用者	TCP 和主機資源 MIBs讀取存取權
網路集合 — Windows	WinRM 使用者	WMI 讀取存取 `root\StandardCIMV2`

資料收集

探索工具收集排程

在您初始探索集合之後，探索工具會繼續以交錯的排程執行，以避免資源爭用：

- VMware 探索 – 每小時 (UTC 為 ：00)
- Hyper-V 探索 – 每小時 (UTC 為 ：20)

探索工具也會透過下列獨立模組收集作業系統指標，每個模組都有自己的交錯排程：

- 網路指標 – 每 15 秒，大型環境可能較不頻繁
- 伺服器效能指標 – 每 10 分鐘 (UTC 為 ：03、：13、：23、：33、：43、：53)
- 儲存效能指標 – 每 10 分鐘 (UTC 為 ：07、：17、：27、：37、：47、：57)
- 執行中程序 – 每小時 (UTC 為 ：40)
- 伺服器佈建資料 – 每日 (UTC 時間 00：05)
- 儲存佈建資料 – 每日 (UTC 時間 00：35)
- 網路介面 – 每日 (UTC 時間 01：05)
- SQL Server 探索 – 每日 (UTC 時間 03：05)
- Oracle 資料庫探索 – 每日 (UTC 05：05)

您可以使用立即收集資料，獨立啟動、停止或觸發每個作業系統指標模組。

若要手動執行集合，請從動作功能表選擇：

- 開始 – 啟用探索模組。
- 停止 – 停用探索模組。
- 立即收集資料 – 立即開始探索。例如，在您變更網路之後，請使用此選項。

這些動作適用於每個模組。您可以個別控制作業系統指標模組。

作業系統資料收集嘗試

探索新伺服器時，探索工具會嘗試每個 IP 地址和主機名稱的每個已設定登入資料。探索工具找到有效的登入資料後，除非您新增登入資料，否則會繼續使用該登入資料。

收集失敗後，探索工具會嘗試在 3 分鐘、30 分鐘、2 小時，然後 6 小時後收集伺服器的聯網資料。嘗試失敗 4 次後，探索工具會繼續每 6 小時嘗試一次所有設定的登入資料。

探索的庫存

設定探索來源之後，探索工具狀態框架中探索到的伺服器值數量會開始增加。已設定來源的探索狀態會在收集模組框架中變更為已啟用。清查頁面會顯示所有已設定來源的伺服器：VMware VMs、Hyper-V VMs 和匯入的伺服器。每個伺服器都會顯示每個模組的來源和集合狀態。

導覽至探索的庫存頁面，以查看探索工具找到的伺服器。從此頁面中，選擇下載庫存以下載包含最多 30 天收集資料的 ZIP 檔案 (`discovery_tool_export.zip`)，包括所有已設定來源的 MPA 檔案、效能使用率資料、資料庫資訊和server-to-server通訊資訊。

您可以在探索工具繼續運作時下載 ZIP 檔案，並取得部分結果。將此檔案上傳至遷移評估，以取得要遷移的商業案例。

匯出選項

匯出資料時，您可以使用下列選項自訂匯出：

日期範圍

選取開始日期和結束日期，以僅匯出在該期間內收集的資料。兩個日期都包含在內。最大日期範圍為 30 天。

> **Note**
>
> 探索工具最多可存放 30 天收集的資料。如果您需要超過 30 天的資料，請每 30 天執行增量匯出以擷取所有資料。

模組選擇

選擇要包含在匯出中的資料模組。您可以匯出所有模組或選取特定模組：

模組	說明
VMware 資料	來自 vCenter 伺服器的虛擬機器庫存
Hyper-V 資料	Hyper-V 主機的虛擬機器庫存

模組	說明
網路資料	伺服器之間的網路連線
伺服器庫存	伺服器硬體和作業系統資訊
伺服器效能指標	CPU、記憶體和網路使用率
伺服器儲存效能	磁碟 IOPS 和輸送量
儲存組態	磁碟區和磁碟區組態
網路介面	網路轉接器詳細資訊
程序指標	執行中的程序
SQL Server 資料	SQL Server 資料庫庫存
Oracle 資料庫資料	Oracle 資料庫庫存 – CDBs、PDBs、功能、選項和元件

如果您未選取任何模組，探索工具會匯出所有可用的資料。

收集的資料點

探索工具會跨 VMware、Hyper-V、作業系統指標、資料庫和網路元件收集完整資料。以下各節詳細說明為每個元件收集的特定資料點。

VMware 資料收集

此表格說明探索工具所收集的 VMware 虛擬機器資訊：

名稱	類型	Category	範例值
vm_name	String	VM 資訊	「w2k22-snmpd-v2-en-us-mssql-2022-testcase4-1」
vm_id	String	VM 資訊	「vm-30920」
vm_uuid	String	VM 資訊	「4201ecf8-cc44-ee7e-01da-34dfb2acf6c0」

名稱	類型	Category	範例值
powerstate	String	VM 資訊	"poweredOn"
託管	String	VM 資訊	"esxi-70-node1.testlab.local"
primary_ip_address	String	VM 資訊	「192.168.0.52」
cpus	Integer	VM 資訊	2
memory	Integer	VM 資訊	4096
total_disk_capacity_mib	Integer	VM 資訊	32768
os_according_to_the_configuration_file	String	VM 資訊	「Microsoft Windows Server 2016 或更新版本 (64 位元 ）」
max_cpu_usage_pct_dec	Float	VM 效能	79.33
avg_cpu_usage_pct_dec	Float	VM 效能	45.06
max_ram_usage_pct_dec	Float	VM 效能	63.99
avg_ram_utl_pct_dec	Float	VM 效能	29.27

Hyper-V 資料收集

此資料表說明 探索工具所收集的 Hyper-V 虛擬機器資訊：

名稱	類型	Category	範例值
vm_name	String	VM 資訊	「win2022-hyperv-test-01」
vm_id	String	VM 資訊	「a1b2c3d4-e5f6-7890-abcd-ef1234567890」
powerstate	String	VM 資訊	「執行中」
cpus	Integer	VM 資訊	4

名稱	類型	Category	範例值
memory_mb	Integer	VM 資訊	8192
disk_paths	String	Disk	"C：\\VMs\\disk1.vhdx"
disk_size_gb	Float	Disk	127.0
network_adapters	String	網路	「00：15：5D：01：02：03」
ip_addresses	String	網路	「10.0.1.50」
host_name	String	主機	"hyperv-host-01.example.com"
host_os_version	String	主機	「Windows Server 2022 Datacenter」
cluster_name	String	主機	「FailoverCluster01」
hypervisor	String	VM 資訊	「Hyper-V」

匯入的伺服器資料

不會自動探索匯入的伺服器。它們會透過 CSV 檔案匯入。探索工具不會收集匯入伺服器的 Hypervisor 層級資料。反之，它會在匯入期間使用與每個伺服器相關聯的作業系統登入資料來收集資料庫、網路和作業系統指標資料。

探索工具的作業系統相關資料

探索工具會透過 SSH (Linux) 和 WinRM (Windows) 收集伺服器庫存、效能、儲存、網路介面和處理資料。下表說明收集的資料點。

伺服器庫存 (server_inventory.csv)

結合伺服器佈建（硬體和作業系統組態）與彙總儲存效能。每 24 小時收集一次。

名稱	類型	Category	範例值
server_id	String	伺服器資訊	「vm-web-server-01」

名稱	類型	Category	範例值
server_name	String	伺服器資訊	「web-server-01」
resource_type	String	伺服器資訊	「virtual_machine」
power_state	String	伺服器資訊	「執行中」
os_type	String	伺服器資訊	「Linux」
os_name	String	伺服器資訊	「Amazon Linux」
os_version	String	伺服器資訊	"2023"
primary_hostname	String	伺服器資訊	"web-server-01.example.com"
primary_ip_address	String	伺服器資訊	「10.0.2.101」
網路遮罩	String	伺服器資訊	「255.255.255.0」
total_num_network_cards	Integer	伺服器資訊	2
total_num_disks	Integer	伺服器資訊	1
cpu_count	Integer	伺服器資訊	4
total_memory_gb	Float	伺服器資訊	15.88
server_uuid	String	伺服器資訊	「4201ecf8-cc44-ee7e-01da-34dfb2acf6c0」
smbios_uuid	String	伺服器資訊	「4201ecf8-cc44-ee7e-01da-34dfb2acf6c0」
cluster_name	String	伺服器資訊	"production-cluster-01"
Hypervisor_object_id	String	伺服器資訊	「vm-30920」
Hypervisor_type	String	伺服器資訊	「VMware」
Hypervisor_version	String	伺服器資訊	"8.0.0"

名稱	類型	Category	範例值
Hypervisor_hostname	String	伺服器資訊	"esxi-node1.example.com"
Hypervisor_host_id	String	伺服器資訊	"host-1234"
Hypervisor_id	String	伺服器資訊	「4201ecf8-cc44-ee7e-01da-34dfb2acf6c0」
disk_read_iops_avg	Float	儲存效能	12.5
disk_read_iops_peak	Float	儲存效能	245.0
disk_write_iops_avg	Float	儲存效能	8.3
disk_write_iops_peak	Float	儲存效能	180.0
disk_total_iops_avg	Float	儲存效能	20.8
disk_total_iops_peak	Float	儲存效能	425.0
disk_read_throughput_avg_mbps	Float	儲存效能	1.2
disk_read_throughput_peak_mbps	Float	儲存效能	24.5
disk_write_throughput_avg_mbps	Float	儲存效能	0.8
disk_write_throughput_peak_mbps	Float	儲存效能	18.0
disk_total_throughput_avg_mbps	Float	儲存效能	2.0
disk_total_throughput_peak_mbps	Float	儲存效能	42.5

伺服器效能指標 (server_performance_metrics.csv)

CPU、記憶體和網路輸送量使用率。每 10 分鐘取樣一次，並彙總 30 天。

名稱	類型	Category	範例值
server_id	String	伺服器資訊	「vm-web-server-01」
data_source	String	伺服器資訊	「作業系統」
cpu_utilization_avg_pct	Float	CPU	45.06
cpu_utilization_peak_pct	Float	CPU	79.33
cpu_count	Integer	CPU	4
memory_total_gb	Float	記憶體	15.88
memory_utilization_avg_pct	Float	記憶體	29.27
memory_utilization_peak_pct	Float	記憶體	63.99
network_in_avg_mbps	Float	網路	0.52
network_in_peak_mbps	Float	網路	12.3
network_out_avg_mbps	Float	網路	0.31
network_out_peak_mbps	Float	網路	8.7
network_total_avg_mbps	Float	網路	0.83
network_total_peak_mbps	Float	網路	21.0

儲存效能 (server_storage_performance.csv)

每個磁碟區磁碟 I/O 和空間使用率。每 10 分鐘取樣一次，並彙總 30 天。

名稱	類型	Category	範例值
server_id	String	伺服器資訊	「vm-web-server-01」
data_source	String	伺服器資訊	「作業系統」
disk_volume_id	String	磁碟區資訊	"/dev/nvme0n1p1"
disk_mount_point	String	磁碟區資訊	"/"
file_system	String	磁碟區資訊	"xfs"
disk_total_gb	Float	磁碟空間	30.0
disk_used_gb	Float	磁碟空間	12.5
disk_free_gb	Float	磁碟空間	17.5
disk_read_iops_avg	Float	磁碟 I/O 資料	12.5
disk_read_iops_peak	Float	磁碟 I/O 資料	245.0
disk_write_iops_avg	Float	磁碟 I/O 資料	8.3
disk_write_iops_peak	Float	磁碟 I/O 資料	180.0
disk_total_iops_avg	Float	磁碟 I/O 資料	20.8
disk_total_iops_peak	Float	磁碟 I/O 資料	425.0
disk_read_throughput_avg_mbps	Float	磁碟輸送量	1.2
disk_read_throughput_peak_mbps	Float	磁碟輸送量	24.5
disk_write_throughput_avg_mbps	Float	磁碟輸送量	0.8
disk_write_throughput_peak_mbps	Float	磁碟輸送量	18.0

名稱	類型	Category	範例值
disk_total_throughput_avg_mbps	Float	磁碟輸送量	2.0
disk_total_throughput_peak_mbps	Float	磁碟輸送量	42.5

儲存組態 (storage_config.csv)

實體磁碟硬體詳細資訊。每 24 小時收集一次。

名稱	類型	Category	範例值
server_id	String	伺服器資訊	「vm-web-server-01」
disk_controller_id	String	磁碟資訊	"/dev/sda"
vmdk_vhd_file_name	String	磁碟資訊	「web-server-01.vmdk」
disk_volume_type	String	磁碟資訊	「虛擬」
disk_provisioned_gb	Float	磁碟資訊	30.0
disk_device_type	String	磁碟資訊	「SCSI HDD」
disk_interface_type	String	磁碟資訊	「SCSI」
disk_protocol	String	磁碟資訊	「LSI 邏輯 SAS」

網路介面 (network_interfaces.csv)

網路轉接器組態。每 24 小時收集一次。

名稱	類型	Category	範例值
server_id	String	伺服器資訊	「vm-web-server-01」

名稱	類型	Category	範例值
interface_name	String	介面資訊	"eth0"
interface_index	Integer	介面資訊	2
mac_address	String	介面資訊	「0A：1B：2C：3D：4E：5F」
adapter_type	String	介面資訊	「vmxnet3」
virtual_network_name	String	介面資訊	「VM 網路」
virtual_network_id	String	介面資訊	「dvportgroup-1234」
virtual_switch	String	介面資訊	「vSwitch0」
ipv4_address	String	IP 組態	「10.0.2.101」
ipv4_subnet_mask	String	IP 組態	「255.255.255.0」
ipv4_gateway	String	IP 組態	「10.0.2.1」
ipv6_address	String	IP 組態	「fe80：：a1b：2cff：fe3d：4e5f」
ipv6_prefix_length	Integer	IP 組態	64
ipv6_gateway	String	IP 組態	「fe80：：1」
dns_servers	String	IP 組態	「10.0.0.2」
dhcp_enabled	Boolean	IP 組態	false
interface_status	String	介面資訊	「向上」
vlan_id	Integer	介面資訊	100
is_primary	Boolean	介面資訊	true

執行中程序 (process_metrics.csv)

執行中程序的快照。每小時收集一次，在 30 天內重複資料刪除。

名稱	類型	Category	範例值
server_id	String	伺服器資訊	「vm-web-server-01」
process_name	String	程序資訊	"sshd"
process_id	Integer	程序資訊	1234
process_command_line	String	程序資訊	"/usr/sbin/sshd -D"
process_user	String	程序資訊	「根」

網路集合

網路收集模組可協助您探索內部部署資料中心伺服器之間的相依性。此網路資料透過提供應用程式如何跨伺服器通訊的可見性，加速遷移規劃。

此模組會從所有設定的來源收集伺服器的網路資料，包括 VMware、Hyper-V 和匯入的伺服器。它使用 WinRM 從 Windows 伺服器收集資料，並使用 SSH、SNMPv2 和 SNMPv3 從 Linux 伺服器收集資料。

網路資料收集

網路收集模組會以 ESTABLISHED 或 TIME_WAIT 狀態擷取探索庫存中伺服器之間的 TCP IPv4 連線。只有當來源和目標 IP 地址都屬於探索工具探索或匯入的伺服器時， 連線才會出現在輸出中。不包含與庫存外 IP 地址的連線，例如外部服務、雲端端點或尚未新增至探索工具的伺服器。

此設計將網路資料集中在環境中server-to-server相依性上，這是應用程式相依性映射和遷移波規劃所需的資訊。

系統會針對每個連線收集這些資料點：

名稱	類型	Category	範例值
來源 IP	String	連線	「192.168.1.10」

名稱	類型	Category	範例值
來源連接埠	Integer	連線	49152
來源程序 ID	Integer	流程	1234
來源程序名稱	String	流程	"java"
目標 IP	String	連線	「192.168.1.20」
目標連接埠	Integer	連線	5432
目標程序 ID	Integer	流程	5678
目標程序名稱	String	流程	「postgres」
State	String	連線	「ESTABLISHED」
傳輸通訊協定	String	連線	"TCP"
IP 版本	String	連線	「IPv4」
計數	Integer	連線	42

> **Tip**
>
> 若要最大化網路相依性映射的完整性，請設定所有探索來源 (VMware、Hyper-V 和伺服器 CSV 匯入），並在檢閱網路資料之前新增作業系統登入資料。庫存中的伺服器越多，網路模組可以擷取的連線越多。

私有地址網路集合

根據預設，網路收集模組只會擷取兩個端點都是所發現庫存中伺服器的連線。您可以啟用私有地址集合，以擷取不在庫存中的 RFC 1918 私有 IP 地址 (10.0.0.0/8、172.16.0.0/12、192.168.0.0/16) 之間的連線。

開始私有地址集合

1. 在收集器組態頁面上，找到收集模組區段。

2. 在應用程式探索下尋找網路連線探索。
3. 開啟動作下拉式清單。
4. 選擇開始私有地址集合。
5. 如果模組狀態為已啟用，您可以看到它變更為已啟用 · 私有地址開啟。

若要停止私有地址集合，請開啟動作下拉式清單，然後選擇停止私有地址集合。先前收集的私有地址資料即使在停止後仍會保留。

私有地址連線只會出現在完整 CSV 匯出中 (ZIP 檔案中），而不會出現在 MPA CSV 檔案中。如果 IP 地址屬於清查中已有的伺服器，無論此設定為何，一律會以其探索到的伺服器 ID 來識別。

此設定會在重新啟動期間持續存在。您可以隨時開始或停止私有地址集合。無論目前的設定為何，都會匯出先前收集的私有地址資料。

SQL Server 集合

SQL Server 收集模組會從 Windows 伺服器收集所有已設定來源的 SQL Server 資訊，包括 VMware、Hyper-V 和匯入的伺服器。模組使用 WinRM 遠端連線至每個 Windows 伺服器，並執行 PowerShell 查詢。它會使用 WMI 命名空間、登錄檔和檔案屬性，收集所有已安裝 SQL Server 服務（元件）的相關資訊。

SQL Server 元件是做為 SQL Server 部署的一部分安裝在 Windows 伺服器上的特定服務或功能執行個體。探索工具會收集資料庫引擎、分析服務、報告服務和整合服務。

SQL Server 資料收集

SQL Server 集合模組會收集 SQL Server 元件資訊。此表格說明收集的關鍵資料點：

名稱	類型	Category	範例值
引擎類型	String	元件	sql_server
是引擎元件	Boolean	元件	Y
狀態	String	服務	執行中、已停止、StartPending
版本	String	服務	2015.131.5026.0
版本	String	服務	開發人員版本 (64 位元）

名稱	類型	Category	範例值
SQL 服務名稱	String	服務	MsDtsServer130、Mssql
SQL 服務類型	String	服務	SQL Server 服務、整合服務
執行個體名稱	String	執行個體	MSSQLSERVER
顯示名稱	String	服務	SQL Server (MSSQLSERVER2017)
啟動模式	String	服務	自動、手動、已停用
服務帳戶名稱	String	服務	NT Service/MsDtsServer130
已叢集	Boolean	組態	N

> **Note**
>
> 完整格式包含所有服務類型。MPA 格式僅包含資料庫引擎元件。根據 SQL 服務類型和組態，並非所有欄位都可用。

Oracle 資料庫集合

透過 Oracle 資料庫集合，您可以探索所有已設定來源的 Oracle 資料庫執行個體，包括 VMware、Hyper-V 和匯入的伺服器。模組會收集下列資料：

- 容器資料庫 (CDB) 和插入式資料庫 (PDB) 列舉
- 版本和版本
- 已安裝的選項
- 功能用量統計資料
- 元件庫存 (DBA_REGISTRY)
- 資料檔案大小
- 拓撲標記 (RAC、Data Guard 和多租戶架構)

資料庫連線 (SQL)

當您設定 Oracle 登入資料時，探索工具會使用唯讀服務帳戶直接連線至 Oracle 資料庫。這提供完整的 SQL 層級集合，包括 PDB 詳細資訊、功能用量和已安裝的選項。所有 CSV 檔案都包含完整資料。

作業系統層級備用

如果您尚未設定資料庫登入資料，或連線失敗，探索工具會使用 SSH 或 WinRM 來偵測 Oracle 安裝。它探索沒有資料庫存取的 Oracle 首頁、接聽程式、修補程式、版本和版本。對於作業系統偵測到的主機，匯出的 CDB CSV 包含執行個體名稱、主機名稱、版本和版本。PDB、功能、選項和元件 CSV 檔案不包含任何資料列。

Oracle 集合會在匯出 ZIP 中產生下列 CSV 檔案。每個資料表描述每個檔案收集的資料點。

CDB 資料 (oracle_data_cdbs_full.csv)

每個 CDB 執行個體一列。此表格說明收集的 CDB 資料點：

名稱	類型	Category	範例值	來源
執行個體名稱	String	Identity	"ORCL"	SQL、作業系統
Host Name (主機名稱)	String	Identity	"oracledb01.example.com"	SQL、作業系統
資料庫名稱	String	Identity	"ORCL"	僅限 SQL
資料庫唯一名稱	String	Identity	"ORCL_PRIMARY"	僅限 SQL
資料庫 ID	Integer	Identity	1234567890	僅限 SQL
版本	String	版本	「19.0.0.0」	SQL、作業系統
完整版本	String	版本	「19.21.0.0.0」	僅限 SQL
版本	String	版本	「Enterprise Edition」	SQL、作業系統
資料庫類型	String	組態	「單一」	僅限 SQL
資料庫角色	String	組態	「主要」	僅限 SQL

名稱	類型	Category	範例值	來源
開啟模式	String	組態	「讀取寫入」	僅限 SQL
日誌模式	String	組態	"ARCHIVELOG"	僅限 SQL
平台	String	組態	「Linux x86 64 位元」	僅限 SQL
CDB 旗標	String	組態	「是」	僅限 SQL
是 RAC	String	拓撲	「是」或「否」	僅限 SQL
Data Guard 為待命	String	拓撲	「是」或「否」	僅限 SQL
保護模式	String	拓撲	「最高效能」	僅限 SQL
Data Guard 中介裝置	String	拓撲	「已啟用」	僅限 SQL
NLS 字元集	String	組態	「AL32UTF8」	僅限 SQL
PDB 計數	Integer	規模調整	3	僅限 SQL
Flashback on	String	組態	「是」	僅限 SQL
偵測路徑	String	中繼資料	"phase2" 或 "phase1b"	SQL、作業系統

PDB 資料 (oracle_data_pdbs_full.csv)

每個 PDB 一個資料列 （ 可插拔資料庫 ）。此表格說明收集的 PDB 資料點：

> **Note**
>
> PDB 資料需要 Oracle 資料庫登入資料 (SQL 連線 ）。作業系統層級備用不會填入此 CSV。

名稱	類型	Category	範例值	來源
CDB 執行個體名稱	String	Identity	"ORCL"	僅限 SQL

名稱	類型	Category	範例值	來源
PDB 名稱	String	Identity	「APPPDB1」	僅限 SQL
開啟模式	String	狀態	「讀取寫入」	僅限 SQL
生命週期狀態	String	狀態	「正常」	僅限 SQL
資料表空間計數	Integer	規模調整	5	僅限 SQL
資料檔案計數	Integer	規模調整	12	僅限 SQL
大小總計位元組	Integer	規模調整	5368709120	僅限 SQL
使用者結構描述計數	Integer	規模調整	8	僅限 SQL
資料庫連結計數	Integer	連線能力	2	僅限 SQL
已安裝的元件	String	組態	"APEX；JVM；XML"	僅限 SQL
加密的資料表空間計數	Integer	安全	1	僅限 SQL

功能用量資料 (oracle_data_features_full.csv)

來自 DBA_FEATURE_USAGE_STATISTICS 的每個功能用量項目一列。此表格說明所收集的功能用量資料點：

> **Note**
>
> 功能用量資料需要 Oracle 資料庫登入資料 (SQL 連線）。作業系統層級備用不會填入此 CSV。

名稱	類型	Category	範例值	來源
CDB 執行個體名稱	String	Identity	"ORCL"	僅限 SQL
Name	String	功能	「分割（使用者）」	僅限 SQL

名稱	類型	Category	範例值	來源
偵測到的使用量	Integer	Usage	42	僅限 SQL
目前使用	String	Usage	「TRUE」	僅限 SQL
第一次使用日期	DateTime	Usage	"2024-01-15T00：00：00"	僅限 SQL
上次使用日期	DateTime	Usage	"2026-06-01T00：00：00"	僅限 SQL

選項資料 (oracle_data_options_full.csv)

每個 CDB 每個 V$OPTION 項目一列。此資料表說明所收集已安裝的選項資料點：

> **Note**
> 選項資料需要 Oracle 資料庫登入資料 (SQL 連線) 。作業系統層級備用不會填入此 CSV。

名稱	類型	Category	範例值	來源
CDB 執行個體名稱	String	Identity	"ORCL"	僅限 SQL
選項名稱	String	選項	「進階分析」	僅限 SQL
已安裝	String	選項	「TRUE」	僅限 SQL
容器 ID	Integer	選項	0	僅限 SQL

元件資料 (oracle_data_components_full.csv)

每個 DBA_REGISTRY 元件一列。此表格說明收集的元件資料點：

> **Note**
> 元件資料需要 Oracle 資料庫登入資料 (SQL 連線) 。作業系統層級備用不會填入此 CSV。

名稱	類型	Category	範例值	來源
CDB 執行個體名稱	String	Identity	"ORCL"	僅限 SQL
PDB 名稱	String	Identity	「APPPDB1」	僅限 SQL
元件 ID	String	元件	"APEX"	僅限 SQL
元件名稱	String	元件	「Oracle Application Express」	僅限 SQL
版本	String	元件	「22.1.0.15.0」	僅限 SQL
狀態	String	元件	「有效」	僅限 SQL
結構描述	String	元件	"APEX_220100"	僅限 SQL

安全考量

保護探索工具 VM

探索工具 VM 安全性至關重要，因為探索工具會將所有登入資料、日誌和客戶資料存放在探索工具 VM 上。

探索工具 VM 預設已停用 SSH 存取，只能從用戶端 存取`vCenter UI -> "Launch Web Console"`。

探索工具 VM 隨附使用者「探索」的預設登入密碼「密碼」。

- 我們建議您在部署後立即更新此密碼。
- 如果您想要在使用 vCenter 登入`enablessh`後，使用 命令啟用 ssh，我們會要求您更新密碼`Launch Web Console`。請注意，每次呼叫此命令時，您需要將其重設。

保護登入資料

登入資料管理的一般最佳實務

- 安全地存放登入資料

- 定期輪換所有登入資料
- 使用密碼管理員或安全保存庫
- 監控登入資料用量
- 遵循最低權限原則，並僅授予所需的最低必要許可

SNMP v2 登入資料

- 使用複雜的非預設社群字串
- 避免常見的字串，例如「公有」或「私有」
- 將社群字串視為密碼

SNMP v3 登入資料

- 同時啟用身分驗證和隱私權
- 使用強式身分驗證通訊協定 (SHA 優先於 MD5)
- 使用強式加密通訊協定 （ 優於 DES 的 AES)
- 對身分驗證和隱私權使用複雜的密碼
- 使用唯一的使用者名稱 （ 避免常用名稱 ）

WinRM 登入資料

- 避免停用 WinRM 憑證檢查。
- 我們建議您建立具有最少必要許可的專用服務帳戶。
- 除非您需要 SQL Server 集合，否則請避免使用網域管理員或本機管理員帳戶。SQL Server 集合需要本機管理員存取權，因為它會查詢多個 WMI 命名空間並使用提升的命令。對於沒有 SQL Server 探索的作業系統指標，具有遠端管理使用者、效能監視器使用者和 WMI 讀取存取權的非管理員帳戶`root\cimv2`已足夠。如需每個模組的詳細資訊the section called “所需的許可”，請參閱 。

Hyper-V 登入資料

- 使用具有最低 Hyper-V 管理許可的專用服務帳戶。
- 避免使用網域管理員帳戶。
- Hyper-V 登入資料支援 NTLM （ 僅限 HTTPS) 和 Kerberos 身分驗證。

- 探索工具會使用 SQLCipher 存放靜態加密的登入資料。

Oracle 登入資料

- 僅使用 SELECT_CATALOG_ROLE 的專用唯讀服務帳戶。請勿使用 DBA、SYSDBA 或 SYSOPER 權限。
- 探索工具只會執行讀取操作，絕不會寫入 Oracle 資料庫。
- 探索工具不會存取診斷套件或調校套件檢視，因此不需要額外的 Oracle 授權。
- 定期輪換 Oracle 服務帳戶密碼，並在探索工具中更新登入資料。

登入資料儲存

探索工具會使用資料庫加密金鑰加密靜態儲存的登入資料。在具有 systemd 250 或更新版本的系統上，此金鑰會使用 systemd-creds 加密。在較舊的系統上，金鑰會儲存為受許可保護的檔案。在這兩種情況下，具有探索工具主機根存取權的攻擊者都可以存取加密金鑰並解密儲存的憑證。限制對探索工具主機的存取，並將其視為環境中的特權系統。

謹慎使用自動連線功能

探索工具使用兩種機制，在作業系統層級收集期間將登入資料指派給伺服器：自動連線和手動。作業系統層級集合包括網路、SQL Server、Oracle 資料庫和作業系統指標模組。這些模組會從所有來源連線至個別伺服器，包括 VMware VMs、Hyper-V VMs 和匯入的伺服器。

手動：伺服器可以手動與特定登入資料建立關聯。在這種情況下，探索工具只會使用該登入資料，無論成功或失敗。您必須手動監控該伺服器的收集狀態並進行調整。

自動連線：如果沒有與伺服器手動相關聯的登入資料，探索工具會使用該伺服器的自動連線機制。這表示：

- 在每個集合回合開始時，探索工具會取得該伺服器可用的登入資料清單（根據作業系統類型），並設定為「自動連線」。
- 探索工具接著會針對迴圈中的伺服器測試所有登入資料。
  - 如果找到有效的登入資料，表示伺服器集合圓滿成功。探索工具會記住它，下次會先嘗試它。
  - 如果找不到有效的登入資料，表示伺服器的集合四捨五入已失敗。
    - 網路模組：伺服器使用退避排程，在每次失敗後 3 分鐘、30 分鐘、2 小時和 6 小時內開始下一個集合（類似於指數退避）。
    - SQL Server 集合：探索工具不會重試。它會每天對每部伺服器進行一次嘗試。

影響/風險：

只有在您確定系統中的風險已緩解時，才使用自動連線：

風險 1：在多個錯誤登入資料上設定自動連線後，自動對伺服器嘗試這些登入資料，可能會觸發已設定鎖定政策之生產環境的帳戶鎖定。例如，資料中心可以將其 VMs 設定為在 3 次 SSH 登入嘗試失敗後鎖定。在此情況下，如果為 3 個錯誤的 SSH 登入資料設定自動連線，則會發生合法的帳戶鎖定。如果鎖定發生在多個系統中，關鍵業務流程可能會受到影響，這可能會導致相依系統中的層疊失敗。此外，安全營運中心可能會遇到來自大量身分驗證失敗事件的警示風暴，導致誤判安全事件耗盡資源，並可能掩蓋真實攻擊。

風險 2：可存取探索工具（了解探索工具密碼）的演員可以透過設定大量測試憑證並使用自動連線來尋找成功的憑證，在所有伺服器上破解強制作業系統憑證。

緩解措施：

請遵守下列準則：

- 確定探索工具密碼已正確保護，且只有授權執行者知道
- 如果存在鎖定政策，請確保為環境輸入適當的登入資料。即使沒有帳戶鎖定政策，我們建議只設定已知且有效的登入資料，以確保個別 VMs 的營運負載降到最低。
- 「自動連線」是選擇加入功能。如果環境需要帳戶鎖定，請勿選取它並使用手動憑證指派。

CSV Import Security

當您使用 CSV 檔案匯入伺服器時，請考慮下列安全性影響：

- CSV 檔案可能包含內部伺服器的主機名稱或 IP 地址。將其視為敏感資料。
- `os_credential_name` 和 `oracle_credential_name`資料欄會依易記名稱參考預先設定的登入資料。CSV 不包含秘密。
- All-or-nothing驗證：如果 CSV 中的任何資料列無效，則會拒絕整個上傳。這可防止可能造成混淆狀態的部分匯入。
- 匯入的伺服器會立即顯示在清查中，並符合收集資格。匯入之前，請確定作業系統和 Oracle 登入資料的範圍正確。

撤銷存取考量

當您撤銷存取權時，刪除的範圍是特定來源：

- 撤銷 vCenter 存取只會刪除 vCenter 資料。它不會影響 Hyper-V 或匯入的伺服器資料。
- 撤銷 Hyper-V 存取只會刪除 Hyper-V 資料。它不會影響 VMware 或匯入的伺服器資料。
- 刪除匯入的伺服器會從庫存中移除它們，但會保留下游收集資料（網路、資料庫、作業系統指標）。
- 若要移除所有來源特定的庫存資料，您必須獨立撤銷或刪除每個來源。即使撤銷所有來源，也會保留下游收集資料（網路、資料庫、作業系統指標）。

疑難排解

驗證探索工具與 vCenter 的連線

當您遇到 VMware 模組組態錯誤時，請依照下列步驟驗證連線：

存取 探索工具 VM

- 登入探索工具 VM，在 vCenter 中開啟遠端主控台
  - 使用者名稱： 探索
  - 密碼：密碼

測試 vCenter 連線能力

1. 測試 vCenter API 存取：

```
curl -v --insecure -u <username>:<password> https://<vcenter-ip-or-hostname>:443/
mob
```

2. 預期的成功輸出：

```
[ec2-user@discoverytool ~]$ curl -v --insecure -u <user>:<password> https://vcsa/
mob > tmp.txt
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0*
 Trying 192.168.2.125:443...
* Connected to vcsa (192.168.2.125) port 443 (#0)
...
</xml>
```

```
* Connection #0 to host vcsa left intact
```

測試 SSL 憑證

1. 執行此命令：

```
openssl s_client -showcerts -servername <hostname> -connect <hostname>:443
```

2. 預期的成功輸出：

   - 應該顯示 vSphere 憑證詳細資訊
   - 驗證連接埠 443 上的 SSL/TLS 連線

```
[ec2-user@discoverytool ~]$ openssl s_client -showcerts -servername vcsa -connect
 vcsa:443
CONNECTED(00000003)
depth=0 CN = vcsa.onpremsim.env, C = US
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 CN = vcsa.onpremsim.env, C = US
verify error:num=21:unable to verify the first certificate
verify return:1
---
Certificate chain
 0 s:/CN=vcsa.onpremsim.env/C=US
   i:/CN=CA/DC=vsphere/DC=local/C=US/ST=California/O=vcsa.onpremsim.env/OU=VMware
 Engineering
-----BEGIN CERTIFICATE-----
...
-----END CERTIFICATE-----
---
Server certificate
subject=/CN=vcsa.onpremsim.env/C=US
issuer=/CN=CA/DC=vsphere/DC=local/C=US/ST=California/O=vcsa.onpremsim.env/OU=VMware
 Engineering
---
```

WinRM 故障診斷

如果您遇到 WinRM 的連線問題，請依照下列步驟測試連線。這些步驟也適用於 Hyper-V 連線問題，因為探索工具使用 WinRM 與 Hyper-V 主機通訊。

使用連接埠 5985 (HTTP) 和 5986 (HTTPS) 測試基本 WinRM 連線。我們需要確保連線可在連接埠 5986 (HTTPS) 上運作

```
# Check WinRM listener configuration
winrm enumerate winrm/config/listener

# Note: Replace <HOST> with the target computer's hostname or IP address. Adjust the
 username and password as needed.
# Test WinRM connection on port 5985 (HTTP)
$cred = Get-Credential
Test-WSMan -Computer <HOST> -Authentication Negotiate -Credential $cred -Port 5985

# Test WinRM connection on port 5986 (HTTPS)
Test-WSMan -Computer <HOST> -Authentication Negotiate -Credential $cred -Port 5986
```

如果上述測試失敗，請嘗試建立已停用憑證驗證的 PowerShell 工作階段：

```
$cred = Get-Credential
$so = New-PsSessionOption -SkipCACheck -SkipCNCheck -SkipRevocationCheck
Enter-PSSession -ComputerName <HOST> -Credential $cred -Port 5985 -SessionOption $so
```

Kerberos 疑難排解

如果您在從 Windows 伺服器收集資料時遇到 Kerberos 身分驗證失敗，請使用下列各節來診斷和解決常見問題。

驗證網路需求

在對 Kerberos 身分驗證進行疑難排解之前，請確認探索工具可以到達所需的網路端點。

驗證 Kerberos 的網路需求

1. 驗證網域控制器的 DNS 解析。從探索工具 VM 執行下列命令：

   ```
   nslookup dc01.example.com
   ```

或者，您可以使用 dig：

```
dig dc01.example.com
```

如果 DNS 解析失敗，請確認探索工具 VM 已設定為使用可以解析 Active Directory 網域的 DNS 伺服器。檢查/etc/resolv.conf並確認名稱伺服器項目指向您的網域 DNS 伺服器。

2. 驗證連接埠 88 上金鑰分發中心 (KDC) 的連線。執行以下命令：

```
nc -zv dc01.example.com 88
```

預期的輸出結果：

```
Connection to dc01.example.com 88 port [tcp/kerberos] succeeded!
```

如果連線失敗，請確認沒有防火牆規則封鎖從探索工具 VM 到連接埠 88 上網域控制器的流量。

3. 驗證與 WinRM 連接埠上目標 Windows 伺服器的連線。執行下列命令：

```
nc -zv <windows-server> 5985
nc -zv <windows-server> 5986
```

如果連線失敗，請確認目標伺服器上已啟用 WinRM，且防火牆規則允許連接埠 5985 和 5986 上的傳入流量。

Kerberos 常見問題

以下是常見的 Kerberos 問題及其解決方案。

區分大小寫錯誤

徵狀：您在身分驗證期間收到「在 Kerberos 資料庫中找不到伺服器」錯誤。

當 Kerberos 領域名稱不是大寫時，通常會發生此錯誤。Kerberos 領域必須在您的 krb5.conf 檔案中以大寫形式指定。例如，使用 EXAMPLE.COM 代替 example.com。

防止帳戶鎖定

探索工具使用退避機制，以防止帳戶鎖定重複失敗的身分驗證嘗試。如果您的服務帳戶遭到鎖定，您可以停止 ，然後透過位於 的探索工具 Web UI 啟動集合模組，以重設集合程序https://<discovery-tool-vm-ip>:5000。

CLI 的kinit 失敗

下表列出常見的kinit錯誤及其解決方案。

錯誤	原因	解決方案
找不到領域適用的 KDC	無法連線 KDC 主機名稱或 IP 地址，或未在 中設定領域krb5.conf 。	確認krb5.conf 檔案包含正確的 KDC 主機名稱和領域。確認連接埠 88 上 KDC 的 DNS 解析和網路連線能力。
預先驗證失敗	服務帳戶的密碼不正確。	驗證密碼，然後再試一次。如果帳戶遭到鎖定，請先在 Active Directory 中將其解除鎖定，再重試。
在 Kerberos 資料庫中找不到用戶端	主體名稱與 Active Directory 中的任何帳戶不相符。	確認主體名稱完全符合帳戶名稱，包括案例。使用 格式username@REALM 搭配大寫的領域。
無法解析 KDC 的網路地址	DNS 無法解析 KDC 主機名稱。	在 中驗證 DNS 組態/etc/resolv.conf 。確認 DNS 伺服器可以解析 KDC 主機名稱。使用 nslookup或 進行測試dig。

成功綁定後，集合會失敗

如果 kinit成功，但資料收集仍然失敗，請檢查下列項目：

1. 確認用於集合的主體名稱與期間使用的案例kinit完全相符。
2. 確認服務帳戶在目標伺服器上具有必要的許可。
3. 確認目標伺服器上已啟用 WinRM。
4. 確認用於集合的主機名稱符合 Active Directory 中註冊的主機名稱。

Kerberos 適用於某些伺服器，但不適用於其他伺服器

如果 Kerberos 身分驗證在某些伺服器上成功，但其他伺服器失敗，請調查下列領域：

如果您的伺服器跨越多個 Active Directory 網域，請為每個網域設定個別的 Kerberos 登入資料。請確定您的 `/etc/krb5.conf` 檔案包含所有領域的項目。每個網域都需要自己的登入資料與正確的`username@REALM`主體。

比較工作伺服器上的 WinRM 組態與故障伺服器。在每個伺服器上執行下列命令：

```
winrm get winrm/config
```

測試與遠端桌面的連線，以隔離問題。探索工具使用 格式`username@DOMAIN`，而遠端桌面則使用 格式 `DOMAIN\username`。

確認服務帳戶是失敗伺服器上本機管理員群組的成員。在目標伺服器上執行下列命令：

```
net localgroup Administrators
```

WMI 需要本機管理員權限才能存取作業系統資訊。SQL Server 集合也需要服務帳戶在目標伺服器上具有本機管理員存取權。

Kerberos 組態檢查清單

在您開始資料收集之前，請使用下列檢查清單來驗證您的 Kerberos 組態。

- `krb5.conf` 檔案存在於探索工具 VM 上。
- 在 中，領域名稱為大寫`krb5.conf`。
- `kinit` 使用服務帳戶執行 會成功，不會發生錯誤。
- 執行中`klist`顯示有效的未過期票證。
- 主體名稱完全符合 Active Directory 帳戶名稱。
- DNS 解析適用於 KDC 主機名稱。
- 連接埠 88 上 KDC 的網路連線已確認。
- 連接埠 5985 和 5986 上目標 Windows 伺服器的網路連線已確認。
- （多網域）每個 Active Directory 網域都有自己在探索工具中設定的登入資料，並`krb5.conf`包含所有網域的 `[realms]`和 `[domain_realm]`項目。

Oracle 資料庫疑難排解

若要診斷 Oracle 資料庫集合問題，例如資料遺失或錯誤，請檢查下列項目。

連線遭拒或逾時

徵狀：Oracle 集合狀態會顯示伺服器的連線錯誤。

若要疑難排解此問題，請檢查下列項目：

- 確認 Oracle 接聽程式正在目標主機上執行： `lsnrctl status`
- 驗證從探索工具到連接埠 1521 （或您的自訂連接埠）上 Oracle 主機的網路連線： `nc -zv <oracle-host> 1521`
- 確認防火牆規則允許 Oracle 接聽程式連接埠上的傳入連線。
- 在 Oracle 主機`lsnrctl services`上執行 驗證服務名稱。如果服務名稱不正確，Oracle 接聽程式會拒絕連線。

身分驗證失敗 (ORA-01017)

徵狀：集合失敗，使用者名稱或密碼錯誤無效。

若要疑難排解此問題，請檢查下列項目：

- 確認 Oracle 服務帳戶存在且未鎖定： `SELECT account_status FROM dba_users WHERE username = 'DISCOVERY_USER';`
- 手動連線以確認密碼是否正確： `sqlplus discovery_user/<password>@<host>:1521/<service_name>`
- 如果帳戶已鎖定，請將其解除鎖定： `ALTER USER discovery_user ACCOUNT UNLOCK;`

權限不足 (ORA-01031)

徵狀：連線成功，但集合會傳回不完整的資料。

若要疑難排解此問題，請檢查下列項目：

- 確認已授予 SELECT_CATALOG_ROLE： `SELECT * FROM dba_role_privs WHERE grantee = 'DISCOVERY_USER';`
- 如果遺失，請授予必要的角色： `GRANT SELECT_CATALOG_ROLE TO discovery_user;`

手動登入資料顯示錯誤，但自動連線運作

當您手動將登入資料鎖定至伺服器時，如果連線失敗，探索工具不會回復。驗證您在登入資料上設定的連接埠和服務名稱是否符合該特定伺服器上的 Oracle 接聽程式。如果伺服器具有非標準連接埠或服務名稱，請相應地更新登入資料組態。

未偵測 Oracle 的作業系統層級備用

如果未設定資料庫登入資料，且作業系統層級的後援未偵測到 Oracle：

- 確認 SSH 或 WinRM 作業系統登入資料已設定並適用於伺服器（檢查作業系統指標收集狀態）。
- 對於 Linux 主機，請確認 `/etc/oratab`是否存在或 Oracle 程序監控 (pmon) 程序正在執行中。
- 對於 Windows 主機，請確認 Oracle 登錄項目存在於 下`HKLM\SOFTWARE\Oracle`或`oracle.exe`程序正在執行中。

SNMP 故障診斷

存取 探索工具 VM

- 登入探索工具 VM，在 vCenter 中開啟遠端主控台
  - 使用者名稱： 探索
  - 密碼：密碼

安裝 SNMP 工具（如有需要）

- `sudo yum install net-snmp-utils -y`

測試 Linux 伺服器的 SNMP 連線

1. `snmptable -v 2c -c <COMMUNITY_STRING> <REMOTE_SERVER_IP> .1.3.6.1.2.1.6.13.1`
2. 範例：

```
#SNMPv2c:
snmptable -v 2c -c public 192.168.1.100 .1.3.6.1.2.1.6.13.1

#SNMPv3 (with authentication):
snmptable -v 3 -u <username> -a MD5 -A <auth_password>
 192.168.1.100 .1.3.6.1.2.1.6.13.1
```

```
#SNMPv3 (with privacy):
snmptable -v 3 -u <username> -a MD5 -A <auth_password> -x DES -X <priv_password>
 192.168.1.100 .1.3.6.1.2.1.6.13.1
```

網路集合錯誤

讀取密碼需要終端機

錯誤：

```
ss command failed on <host>: sudo: a terminal is required to read the password; either
 use the -S option to read from standard input or configure an askpass helper sudo: a
 password is required
```

ss 命令正在提示使用者密碼。設定的 ssh 使用者必須位於 sudoers 群組中，並使用 ss/netstat 命令的無密碼 sudo 進行設定。若要設定無密碼 sudo：

1. 建立新的 sudoers 檔案：

   ```
   sudo vi -f /etc/sudoers.d/<username>
   ```

2. 新增該行：

   ```
   <username> ALL=(ALL) NOPASSWD: /usr/sbin/ss, /usr/bin/netstat
   ```

3. 在此變更之後，執行 `sudo ss -tnap`和 `sudo netstat -tnap`應該在不提示密碼的情況下執行

網路集合在沒有 sudo 的情況下執行

如果您在探索的庫存頁面上看到下列警告：

```
Network collection ran without sudo. Process-level connection data may be missing.
```

此警告表示 SSH 使用者帳戶在目標伺服器上沒有 sudo 存取。如果沒有 sudo，探索工具仍然可以收集網路連線資料，但無法判斷哪個程序擁有每個連線。若要收集完整的程序層級連線資料，請確定 SSH 使用者在目標伺服器上具有 sudo 存取。

作業系統指標集合錯誤

Linux 伺服器缺少伺服器 UUID

如果探索工具無法收集 Linux 伺服器的伺服器 UUID（顯示為空或遺失），請確認為這些伺服器設定的 SSH 登入資料具有 sudo 權限。此工具使用 dmidecode 讀取伺服器 UUID。如果dmidecode未安裝 ，工具會回到讀取 /sys/class/dmi/id/product_uuid，這也需要 sudo 存取。如果沒有 sudo，則任何方法都無法擷取 UUID。

解決方案：確保提供給探索工具的 SSH 使用者帳戶在目標 Linux 伺服器上具有 sudo 存取。

已探索庫存中的存取問題

如果您在伺服器集合狀態中看到訊息，例如缺少登入資料或存取遭拒：

1. 在探索到的伺服器資料表上選取伺服器。
2. 選擇管理存取憑證 您可以選擇：
   a. 從選取登入資料下拉式清單中選取替代登入資料。
   b. 選取使用新登入資料並提供新登入資料。
3. Save (儲存)。

探索工具會在您儲存變更後重試連線。

SSH 金鑰身分驗證疑難排解

從 探索工具測試 SSH 金鑰連線

如果 SSH 金鑰身分驗證失敗，請確認從探索工具到目標伺服器的連線：

1. 登入探索工具（透過 vSphere 主控台或 SSH 到 Linux 主機）。
2. 使用私有金鑰測試 SSH 連線：

```
ssh -i /path/to/private_key -o StrictHostKeyChecking=no <username>@<target_ip>
```

3. 如果連線成功，問題在於金鑰上傳到探索工具的方式。重新上傳金鑰並驗證使用者名稱是否相符。
4. 如果連線失敗，請檢查下表中的錯誤訊息。

錯誤訊息	原因	Resolution
`Permission denied (publickey)`	公有金鑰不在目標伺服器的 `authorized_keys` 檔案中，或使用者名稱錯誤。	為正確的使用者`~/.ssh/authorized_keys` 將公有金鑰新增至目標伺服器上的 。驗證檔案許可：`chmod 700 ~/.ssh && chmod 600 ~/.ssh/authorized_keys` 。
`Connection timed out after 20s`	無法從探索工具連線連接埠 22。	確認探索工具和目標伺服器之間的連接埠 22 已開啟。檢查防火牆和安全群組。
`Connection refused`	SSH 服務未在目標伺服器上執行。	啟動 SSH 服務：`sudo systemctl start sshd`。
`Invalid SSH key for credential 'name'`	不支援金鑰格式、金鑰資料損毀，或密碼短語遺失或不正確。	驗證金鑰格式為 RSA、ECDSA 或 Ed25519，採用 PEM、OpenSSH 或 PKCS#8 格式。如果金鑰已加密，請確定密碼片語正確。

Linux 安裝程式疑難排解

連接埠 5000 已在使用中

徵狀：安裝後，探索工具服務無法啟動。

解決方案：使用連接埠 5000 識別和停止程序：

```
sudo ss -tlnp | grep :5000
```

停止衝突的程序，然後重新啟動探索工具：

```
sudo ./AWS-Transform-discovery-tool.sh start
```

常見錯誤訊息

此表說明常見的錯誤訊息及其說明：

訊息	Location	說明
已建立密碼	建立密碼頁面	兩個使用者同時建立密碼時的競賽條件；重新整理
匯出失敗	庫存頁面	重試或傳送日誌
隨需集合已在進行中	庫存頁面	當兩個使用者同時啟動手動集合時的競賽條件；在目前的手動集合完成後再試一次
`Command timed out after 60s`	伺服器集合狀態	目標伺服器上的命令未在 60 秒內完成。這可能發生在大量載入的伺服器上。重試集合或調查目標伺服器的負載。
一或多個登入資料包含未知 UUIDs	作業系統存取頁面	兩個使用者同時編輯作業系統登入資料的競賽條件；請再試一次
無效的密碼	登入頁面	登入密碼不正確；請聯絡管理員或聯絡
您的工作階段已過期。請再次登入。	登入頁面	工作階段已逾時，需要再次登入
發生內部錯誤	各種頁面	重試或傳送日誌

版本備註

本節說明 AWS Transform 探索工具的功能、改善和錯誤修正，依發行日期組織。

日期	版本	版本備註
2026 年 6 月 30 日	1.0.1646	新功能 • 新增 Oracle 資料庫探索。此工具會收集 CDB 和 PDB 拓撲、版本、版本、已安裝選項、功能用量和元件庫存。探索工具支援透過 SSH 或 WinRM 的直接 SQL 連線 （ 使用 SELECT_CATALOG_ROLE) 和作業系統層級備用偵測。

日期	版本	版本備註
		• 新增對不同 Active Directory 網域間多個 Kerberos 登入資料的支援。每個登入資料都會獨立驗證，啟用來自多個網域中 Windows 伺服器的集合，而不會發生身分驗證衝突。 改進 • 改善舊版主機的作業系統指標集合。針對無法使用現代命令的較舊作業系統 (RHEL 5、SLES 11、Windows Server 2008 R2) 新增備用資料收集。現在使用替代系統介面收集儲存、效能和網路介面資料。 錯誤修正 • 修正透過 Hyper-V 發現之伺服器的 Kerberos 身分驗證失敗。探索工具現在可從 Hyper-V 訪客中繼資料正確解析伺服器主機名稱 (FQDN)，這是 Kerberos SPN 比對的必要項目。

日期	版本	版本備註
2026 年 5 月 14 日	1.0.1363	新功能 • 新增 Linux 安裝程式，用於在支援的 Linux 發行版本 (Amazon Linux 2、Amazon Linux 2023、RHEL 8–9、Rocky Linux 8–9、AlmaLinux 9、Ubuntu 20.04–24.04、Debian 10–12、SLES 15 SP5) 上部署探索工具。 • 新增對跨 vCenter 使用自動 VM 重複資料刪除設定多個 VMware vCenters伺服器的支援。 • 新增 SSH 私有金鑰身分驗證，做為 Linux 作業系統存取的使用者名稱和密碼的替代方案。支援的金鑰格式包括 RSA、ECDSA、Ed25519、OpenSSH 和 PKCS#8。 • 新增私有地址網路集合，以擷取不在您探索庫存中的 RFC 1918 私有 IP 地址的連線。 • 新增匯出選項以選取自訂日期範圍，並選擇要包含在匯出中的資料模組。 改進 • 透過交錯收集器排程來改善排程收集可靠性。 • 透過 SSH 命令批次處理改善作業系統指標收集效能。 • 現在，登入資料變更會立即重試先前失敗的伺服器。 • 當某些命令傳回空白結果時，作業系統指標集合現在會報告部分狀態。 • 改善儀表板中 vCenter 連線問題的錯誤可見性。

日期	版本	版本備註
2026 年 4 月 7 日	1.0.1074	新功能 • 新增對 Microsoft Hyper-V 探索的支援，包括從具有容錯移轉叢集重複資料刪除的 Hyper-V 主機自動探索 VMs。 • 新增支援透過 CSV 檔案上傳匯入伺服器。 • 新增具有六個獨立模組的作業系統指標集合：伺服器效能、儲存效能、伺服器佈建、儲存佈建、網路介面和執行中程序。 • 使用 VHD 映像檔案新增 Hyper-V 部署選項。 • 透過移除 EC2-specific服務並封鎖對執行個體中繼資料端點的存取，改善內部部署安全性強化。
2026 年 3 月 26 日	1.0.1014	錯誤修正和改善 • 將 Kerberos 網域大寫驗證從後端移至前端。 • 從 Python-kerberos 切換到 Python-pykerberos，並將檔案型快取設為預設值。 • 修正不區分大小寫的大量編輯伺服器 ID 驗證。 • 已修正匯出 ZIP 檔案名稱（現在為 `discovery_tool_export.zip`）。 • 已修正執行檢查的服務，並新增系統登入資料的偵錯日誌。 • 新增網路組態指令碼以建置成品。
2025 年 12 月 16 日	1.0.718	新功能和改進 • 新增 SMBIOS UUID 支援，以防止下游服務中的 VM 重複。 • 引進Min/Max/Avg追蹤和擴展儲存指標，以改善資源監控。 • 新增 API 驗證改進。 • 新增說明面板功能與內容指引。 • 在整個界面中，將術語從「收集器」更新為「工具」。

日期	版本	版本備註
2025 年 10 月 31 日	1.0.0	初始版本 AWS Transform 探索工具的初始啟動。此版本包括： • 離線集合（不依賴 AWS 帳戶或 Application Discovery Service)。 • VMware 探索和監控。 • SQL Server 資料庫探索。 • 透過 SSH、WMI 和 SNMP Server-to-server通訊。

遷移 （ 包括 VMware)

AWS 轉換可協助您使用生成式 AI，包括 VMware、Hyper-V 和其他來源，將虛擬和裸機伺服器環境遷移至 Amazon EC2。採用 AI 技術的代理程式可加速遷移的每個階段，從探索和規劃到網路遷移和伺服器重新託管，減少傳統上大規模遷移所需的手動工作。您可以透過逐步引導您的對話界面與客服人員互動，因此您可以專注於決策而非執行。

功能和主要功能

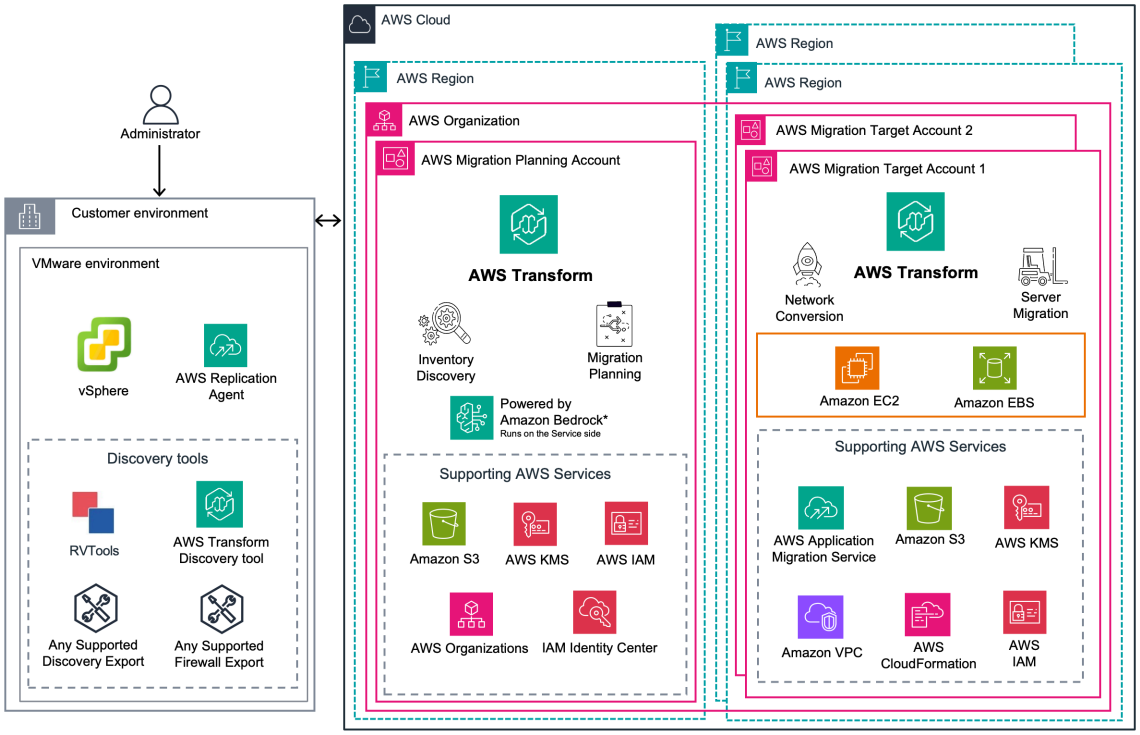
AWS Transform 提供下列功能和主要功能，可讓您將伺服器環境遷移至 AWS。

- 符合您所在位置的靈活探索，提供多種擷取來源環境的選項：
  - 使用 的收集器，協助探索您的 VMware 環境 AWS Application Discovery Service。
  - vCenter 的開放原始碼匯出工具 (VMware 環境）。
  - 匯入獨立收集的探索資料 （任何來源環境）。
- AI 驅動的網路遷移會將來源網路組態轉換為生產就緒的 Amazon VPC 架構，因此您不需要從頭開始設計。
- 智慧型遷移規劃，可自動將應用程式分組並序列化遷移波紋，協助您以較少的規劃週期更快地移動。
- 透過引導式測試和切換工作流程，自動化伺服器重新託管以在 Amazon EC2 上原生執行伺服器。
- 當地語系化界面，可讓您使用 AWS Transform 以偏好的語言進行遷移。如需詳細資訊，請參閱語言設定。

AWS Transform 支援遷移受支援作業系統的 Windows 和 Linux 伺服器。如需支援作業系統的完整清單，請參閱AWS Transform MGN 《 使用者指南》中的支援的作業系統。

AWS 轉換遷移架構

AWS 轉換會從單一界面協調整個遷移生命週期。下圖顯示架構的概觀。



遷移任務

若要開始遷移，請建立工作區並啟動遷移任務。工作區是一或多個遷移任務的邏輯容器，為您提供單一位置來管理整個遷移。

取得工作區

如需建立工作區的相關資訊，請參閱入門。

您的工作區會決定任務、探索資料和 AWS 轉換建議的所在 AWS 區域 位置。若要在不同的 中工作 AWS 區域，請要求您的管理員在該區域中建立工作區。如需有關支援的 AWS 區域的資訊，請參閱支援的區域。

您可以指定不同的 AWS 區域 做為遷移目標。這表示您可以在一個區域中執行探索，但在另一個區域中部署目標環境。如果您這樣做，您的部分資料將跨 傳輸 AWS 區域。伺服器複寫資料不會跨區域傳輸，並直接從您的來源環境傳輸到您的目標帳戶和區域。如需詳細資訊，請參閱the section called “連接目標 AWS 帳戶和區域”。

任務類型

無論您需要end-to-end遷移，還是想要處理特定階段， AWS Transform 都會提供下列類型的遷移任務，您可以根據遷移需求進行選擇。除了這些預設選項之外，您可以隨時動態新增或移除任務中的任何步驟，以自訂遷移工作流程。

End-to-end遷移

最適合您希望 AWS Transform 處理從探索到重新託管的所有內容的完整遷移。

1. 執行探索
2. 建置遷移計劃
3. 連接目標帳戶
4. 建置登陸區域
5. 遷移網路
6. 遷移伺服器

探索和遷移規劃

當您想要評估環境並在承諾執行之前建置波動計畫時，請使用此選項。

1. 執行探索
2. 建置遷移計劃

網路遷移

當您的登陸區域和帳戶已設定且您需要將網路組態遷移至 時，請使用此選項 AWS。

1. 連接目標帳戶
2. 遷移網路

登陸區域

當您需要在遷移工作負載之前設定多帳戶 AWS 基礎時，請使用此選項。

1. 連接目標帳戶

2. 建置登陸區域

登陸區域、網路和伺服器遷移

當您已完成探索和規劃，並希望 AWS Transform 處理基礎設施設定和執行時，請使用此選項。

1. 連接目標帳戶
2. 建置登陸區域
3. 遷移網路
4. 遷移伺服器

遷移規劃和伺服器遷移

當您的網路已就緒，而且您想要直接從探索移至重新託管時，請使用此選項。

1. 執行探索
2. 建置遷移計劃
3. 連接目標帳戶
4. 遷移伺服器

建立和啟動任務

若要建立遷移任務，請完成下列步驟。如需不同任務類型的資訊，請參閱 the section called “任務類型”。

建立和啟動新的遷移任務

1. 在工作區登陸頁面上，選擇建立任務。
2. 選擇遷移選項，然後指定您要建立的遷移任務類型。如需每個遷移任務類型中包含的步驟資訊，請參閱 the section called “任務類型”。
3. 在您回答所有聊天問題後，選擇建立任務。

下載工作區摘要報告

您可以在遷移期間隨時以可下載的 PDF 產生工作區摘要報告。報告提供工作區中所有遷移任務的合併檢視，包括：

- 任務狀態和目前的工作流程步驟
- 使用者動作和核准
- 波規劃詳細資訊
- 網路遷移拓撲
- 登陸區域組態
- 重新託管進度
- 容器化決策
- 產生的關鍵成品

若要產生報告，請在聊天中詢問客服人員。例如，「提供我所有任務遷移進度的工作區摘要。」 客服人員會編譯所有任務的資料，並直接在聊天中交付 PDF。

使用專家模式

專家模式可將遷移任務期間的互動降至最低。您在執行之前提供輸入和偏好設定，代理程式會在任務進行時自動套用。代理程式只會在無法解決問題或錯誤需要動作時暫停。

使用專家模式

1. 建立遷移任務並定義其任務計畫。在開始任何步驟之前，請在聊天中輸入「在專家模式下執行此任務」，或在 Web 應用程式中輸入 /expert-mode-on 命令，以啟用專家模式。
2. 啟動任務。客服人員會新增資料收集做為第一個步驟，並顯示您任務計畫可用的輸入。
3. 提供您的輸入和偏好設定。您可以在一則訊息中包含多個值，或連接 UTF-8 文字檔案 （上限為 256 KB)。例如，輸入「使用多帳戶遷移、平均 Amazon EC2 大小、共用租用，以及每波最多 20 個伺服器」。
4. 或者，指定檢閱檢查點或模式切換。例如，輸入「遷移規劃後暫停檢閱」或「網路遷移後切換至標準模式」。
5. 檢閱收集的值，並更正代理程式標記為無效的任何值，並指示代理程式繼續。

除非您設定檢閱檢查點，否則代理程式會依序處理步驟和波浪，呈現中繼結果而無需等待確認。您可以隨時在聊天中傳送指示，並隨需切換到標準模式。

限制

- 您必須在任何步驟開始之前啟用專家模式。您無法在工作中啟用它。

- 當無法從收集的輸入中解決問題、輸入無效或錯誤需要動作時，客服人員會暫停。
- 專家模式不會略過核准要求。需要核准的操作仍會在核准索引標籤中等待授權。
- 收集的設定會全域套用至所有相關步驟和波浪。波特定指示會在該波執行時進行評估。
- 輸入文字檔案必須使用 UTF-8 編碼，且不得超過 256 KB。此限制不適用於庫存或其他遷移成品。

限制

AWS 轉換有下列限制：

- 如果您停止執行中的遷移任務，然後要求代理程式重新啟動該任務，該任務將從頭開始，而且您會失去在任務中所做的任何進度。不過，在重新啟動之前在任務中建立的成品仍然可用。
- 您可以 AWS 區域 為每個遷移任務指定一個目標。若要將應用程式遷移至不同的目標區域，請建立多個遷移任務。
- 多帳戶遷移 – 僅限單一區域 – 您可以在單一 內遷移至多個帳戶 AWS 區域。對於多區域遷移，您必須為每個目標區域建立單獨的專案。
- 多帳戶遷移 – 每波一個帳戶 – 每個遷移波只能以一個帳戶為目標。需要不同目標帳戶的應用程式必須放置在不同的波浪中。
- 多帳戶遷移 – AWS 需要組織 – 所有目標帳戶都必須是 AWS 組織的一部分。

探索來源資料

上傳您的內部部署伺服器資料和 AWS 轉換會自動偵測檔案格式和結構、剖析和擷取結構化實體記錄、移除多個檔案之間的重複項目、驗證資料品質並報告問題，然後準備摘要以供下游遷移規劃使用。

AWS 轉換接受來自下列來源的資料：

- AWS 轉換探索工具 (CSV 和 JSON ZIP 格式）
- AWS 遷移評估器收集器
- RVTools (Excel 檔案或包含 CSV 檔案的 ZIP 檔案）
- modelizeIT (CSV，ZIP 格式）
- AWS 遷移產品組合評估 (MPA) 格式匯出 （例如，Cloudamize)

對於每個資料來源， AWS Transform 個別接受主要伺服器檔案。連線等補充檔案只有在包含於具有伺服器檔案的 ZIP 檔案中，或包含於具有伺服器工作表的 Excel 檔案中時，才會處理。

上傳最詳細的可用資料。在上傳之前檢閱匯出檔案，以確保資料完整性和準確性。確認所有必要檔案都包含在上傳中，並確認資料反映您目前的環境狀態。這有助於 AWS 轉換更準確地擷取您的內部部署環境，並更好地支援遷移規劃，包括應用程式分組和波動規劃。您可以在取得資料時逐步新增資料。AWS Transform 會在多個上傳之間自動取消重複記錄。

上傳後，在任務計畫中展開探索內部部署資料並選擇庫存準備摘要，以檢閱您的探索資料。 您可以在聊天中提出問題，以驗證擷取或識別問題。例如，您可以詢問有關作業系統和版本的問題。若要修正錯誤，請重新上傳資料， AWS 轉換會自動合併更新的記錄。如果您不想再使用該庫存資料，也可以移除先前上傳的檔案。

建置遷移計劃

Transform AWS for migrations 中的遷移規劃任務步驟是規劃大型遷移的協作聊天式體驗。 AWS Transform 代理程式會套用 AWS 規範性指引，引導客戶從現場部署資料分析到最終遷移波動計劃。

探索內部部署資料任務成功完成後， AWS Transform 會使用探索資料，將應用程式分組到遷移波紋中。 AWS Transform 會引導您完成步驟，以分析和調整伺服器範圍、將伺服器分組到應用程式、產生移動群組，以及建置遷移波紋。

AWS 轉換支援整個程序的反覆規劃：

- 您可以提出問題，以更加了解 AWS Transform 如何分析已安裝的軟體，例如伺服器相依性和網路架構。
- 您可以隨時調整應用程式群組和波浪內的範圍。
- 您可以重新上傳探索資料， AWS 轉換會自動處理、取消複製和合併具有現有資料的新記錄。
- 偵測到變更時，例如新發現的相依性或基礎設施新增， AWS Transform 會標記受影響的相依性群組，並提供波動計畫調整的建議。
- 遷移規劃也可以利用非結構化文字資料來豐富規劃程序。

遷移規劃階段有四個：

- 在範圍和分析中，您可以檢閱探索資料、詢問有關軟體和網路環境的問題，以及判斷遷移範圍內的資源。
- 在群組應用程式中，您可以提供商業和技術規則的組合，例如主機名稱分析、網路相依性和商業規則，以便遷移規劃可以將基礎設施分組到應用程式中。如果您已經有應用程式的清查，遷移規劃可以改用它。

- 在產生移動群組中，您可以為您的技術和業務需求提供遷移規劃，以便它可以確定哪些應用程式必須一起移動。技術相依性包括資料庫、訊息佇列或多個應用程式之間共用的其他資源。業務和營運相依性包括業務關鍵性、RPO 和 RTO、資料中心位置和應用程式擁有者。
- 最後，在建置波浪中，您可以提供有關時間表和優先順序的遷移規劃內容，以便它可以建立您可以遷移的波浪計劃。您可以根據優先順序分數、移動群組大小、使用者計數和應用程式複雜性等因素，選取要包含在波動中的移動群組。

遷移規劃術語

遷移波

一起遷移的應用程式邏輯群組。遷移波由一或多個移動群組組成。

移動群組

必須一起移動的一組共同相依應用程式。它們可能有技術相依性，例如共用資料庫或業務相依性，例如支援共用業務功能。

相依性

系統之間的關係。相依性有數種類型：

- 關鍵或硬相依性。如果沒有相依性，系統將無法運作。常見範例包括依賴資料庫、其他應用程式或服務的應用程式。
- 軟相依性。對系統操作來說並不重要。常見的範例包括不區分延遲的相依性，可以獨立遷移。
- 非技術相依性。與您的組織及其優先順序相關的業務、組織、營運和合規相依性。範例包括共用業務職能和組織擁有權。

工作流程

遷移規劃是一種互動式的反覆工作流程。您可以隨時返回並變更先前的步驟。典型的遷移規劃工作流程是：

1. 遷移規劃從摘要可用的探索資料開始。檢閱可用的資料，並隨時返回探索步驟以提供其他資料。
2. 在範圍界定和分析步驟中，您可以詢問有關內部部署環境的問題，以驗證您已收集的資料。範例問題包括：
   a. 依作業系統列出我的伺服器
   b. 總結我的內部部署網路拓撲
   c. 列出在我的環境中執行的最常見技術。

3. 分析環境時，如果您識別的伺服器不應位於遷移範圍內，您可以指示 AWS Transform 排除這些資源。這些範例包括：
   a. 移除其主機名稱中具有舊版的所有伺服器
   b. 移除 10.0.2.0/24 子網路中的所有伺服器
   c. 移除執行 2022 年以前版本 Windows 的所有伺服器
4. 充分探索環境並確定遷移範圍後，您可以指示 AWS Transform 移至下一個遷移規劃步驟。
5. 下一個步驟是應用程式分組。如果您已將伺服器映射至應用程式，您可以指示 AWS Transform 使用該映射並略過此步驟。如果您沒有預先定義應用程式，您可以提供定義應用程式的技術和商業邏輯。 AWS Transform 將引導您完成應用程式分組程序，並建議您可以提供的資料點，以有效地將伺服器分組到應用程式中。您可以提供的現場部署應用程式相關資訊越多， AWS Transform 就越能將您的伺服器分組到應用程式中。提供足夠的資訊後，您就可以指示 AWS Transform 執行應用程式分組。
6. 執行應用程式群組之後，請檢閱應用程式群組。您可以指示 AWS Transform 進行任何必要的變更，例如：
   a. 將伺服器 example-server 移至 application-5
   b. 重新命名 application-5 "HR App Test Environment"
   c. 從 IIS 開發陣列移除所有 Linux 伺服器
7. 將應用程式分組後，指示 AWS Transform 移至下一個步驟
8. 下一個步驟是移動分組。在移動分組步驟中，您可以識別必須一起移動的應用程式。提供有關技術和非技術相依性的內容。 AWS Transform 將引導您完成程序，並建議您可以提供的資料點，以將應用程式分組在一起。在此階段有幾項考量，包括：
   a. 移動群組的目標大小應該是多少？
   b. 您想要為每個應用程式結合環境，例如開發、測試和生產環境，還是分割環境？
   c. 您想要如何考慮網路相依性？ 所有相依性是否至關重要，或者某些相依性是否可視為軟相依性，並分割為移動群組？
9. 一旦您提供移動分組的規則，請指示 AWS Transform 執行移動分組策略。然後，您可以檢閱和修改移動群組。檢閱移動群組之後，您可以指示 AWS Transform 移至最終遷移規劃步驟。
10. 波浪規劃是遷移規劃的最後一步。在此步驟中，您將移動群組分組為遷移波，並排定這些波的優先順序。在波動規劃步驟中， AWS Transform 將引導您完成提供將移動群組分組為波浪所需的業務優先順序，然後排定這些波浪的優先順序。波動規劃中的考量包括：
    a. 每個移動群組的業務關鍵性
    b. 每個移動群組的遷移時間表和時間表
    c. 與每個移動群組相關聯的風險

d. 每波要遷移的伺服器數量

11.一旦您提供了有關如何分組成波浪的足夠指導，請指示 AWS Transform 執行波動規劃。然後，您可以檢閱您的波浪並進行修改。

12完成波動計畫後，您就可以完成遷移規劃並移至執行。您可以隨時返回遷移規劃，以精簡和迭代您的計畫。

13對於每一波，您可以指派遷移策略：重新託管（將伺服器遷移至 Amazon EC2) 和容器化（合併原始碼並部署至 Amazon Elastic Container Service 或 Amazon Elastic Kubernetes Service)。當您指派波動策略容器化時， AWS Transform 會在遷移執行期間執行該波動的來源碼容器化工作流程。如需詳細資訊，請參閱原始程式碼容器化。若要在指派 7Rs 架構之前取得 AWS建議的策略，請參閱 the section called “7Rs 建議”。

遷移策略 (7R) 建議

在遷移規劃期間， AWS Transform 可以分析您探索到的庫存，並針對每個伺服器和應用程式建議遷移策略，這是業界標準的 7Rs 之一。每個建議都包含建議 AWS 的目標服務、可信度分數，以及背後的推理。這為波動計畫提供了可防禦的起點，並呈現您可能會錯過的現代化機會。

七種策略是重新託管、轉換、重構、重新購買、淘汰、保留和重新放置。 AWS 轉換會讀取資料中的訊號，例如作業系統、使用率和工作負載類型，以提出可解釋的建議。例如，它可以建議淘汰閒置或end-of-life的伺服器、將 SQL Server 或開放原始碼資料庫移至 Amazon RDS、將電子郵件和協同合作工作負載轉移到 Microsoft 365、保留專門的舊版系統，以及在 Amazon EC2 上重新託管剩餘的工作負載。建議會從個別伺服器累積到應用程式，並涵蓋整個產品組合，並依策略和波級摘要提供關鍵性檢視。

若要產生遷移策略 (7R) 報告：

1. 完成探索內部部署資料步驟，並將您的伺服器分組到應用程式中。兩者都是必要的，以便 AWS 轉換可以提供每個伺服器和每個應用程式的建議。
2. 在遷移規劃聊天中，詢問 AWS Transform 以取得遷移策略 (7R) 報告。例如，產生 R-strategy 報告。應用程式分組完成後， AWS Transform 也會提供 來為您產生報告。
3. AWS Transform 會分析您的庫存、套用 7Rs 架構，並產生報告。您可以提供詳細資訊，例如您的組織名稱和任何篩選條件來範圍分析。
4. 檢閱建議。若要調整建議，請在聊天中告知 AWS Transform。您可以變更單一伺服器或應用程式，或大量套用變更（例如，依作業系統、環境、波動或優先順序）。 AWS 轉換會隨您的變更更新報告。

根據預設， AWS Transform 會產生互動式 HTML 儀表板，供您篩選和探索。您也可以根據請求產生 PDF 文件來與利益相關者共用，或產生要呈現的 Microsoft PowerPoint (PPTX) 投影片；PDF 和 PowerPoint 輸出是相同分析的point-in-time快照。報告包含每個伺服器和應用程式的建議策略和 AWS 目標服務、可信度分數和推理、反白顯示的現代化機會、策略的關鍵性檢視、波動層級摘要和風險標記。

此報告中建議的策略補充您在波動規劃期間指派的每波策略。如需來源碼容器化，請參閱 原始程式碼容器化。

圖表和報告

在遷移規劃期間， AWS Transform 會將您探索到的庫存和規劃結果轉換為視覺化圖表和分析報告。您可以在規劃聊天中對話產生它們。例如，「顯示網路拓撲圖」或「產生風險報告」。 AWS 轉換會從您已提供的資料建置它們，而不需要設定。

圖表是互動式的，可讓您以視覺化的方式探索您的環境。可用的圖表包括：

- 網路拓撲 – 伺服器及其網路關係的互動式地圖，旨在擴展到數千個節點的大型環境。
- 應用程式相依性 – 從觀察到的網路連線衍生的導向application-to-application關係。
- Wave Gantt 圖表 – 遷移波的時間軸檢視，顯示排程、相依性、里程碑和進度 （ 在波規劃後提供 ）。
- 一般圖表 – 在您所選資料維度上的圓餅圖、長條圖、長條圖、長條圖和摘要表。

報告提供遷移資料的敘述性分析和建議。可用的報告包括：

- 風險評估 - 對每個應用程式的技術複雜性、相依性風險、遷移準備程度和操作風險進行評分，包括每個應用程式、每波和整個產品組合的摘要。
- 遷移策略 (7R) – 每個伺服器和每個應用程式策略建議。如需詳細資訊，請參閱the section called “7Rs 建議”。
- 一般和自訂報告 – 請求的分析報告，例如執行準備摘要、cost-versus-risk權衡，以及容器化候選評估。

有些輸出取決於您的規劃進度。例如，應用程式相依性圖表使用您的網路連線資料。波動規劃完成後，即可使用波動 Gantt 圖表和波動層級報告摘要。如果缺少先決條件， AWS Transform 會告訴您需要什麼，並且可以先執行必要的步驟。

AWS 轉換會以互動式 HTML 的形式提供圖表，您可以篩選和探索。根據預設， AWS Transform 會以獨立 HTML 檔案的形式交付報告。依請求， AWS Transform 也可以產生 PDF 文件，與利益相關者或要呈現的 Microsoft PowerPoint (PPTX) 投影片集共用。PDF 和 PowerPoint 輸出是point-in-time快照。

連接目標 AWS 帳戶和區域

將 AWS 轉換連接到您的目標 AWS 環境，以便代理程式可以代表您部署基礎設施、遷移網路和重新託管伺服器。這包括三個步驟：選取遷移類型、提供您的 MAP 協議詳細資訊 （ 如適用 ），以及設定連接器。這些設定適用於所有遷移階段，包括網路遷移、登陸區域和伺服器重新託管。

步驟 1：遷移類型選擇

AWS 轉換支援單一帳戶和多帳戶遷移。選擇符合您目標環境的選項：

- 單一帳戶遷移 – 所有工作負載遷移至一個目標 AWS 帳戶。連接器目標帳戶和目標帳戶相同。
- 多帳戶遷移 – 從單一工作區跨組織中的多個帳戶遷移工作負載。連接器必須連接到組織管理帳戶或同時為 AWS Transform MGN 和 CloudFormation StackSets 註冊的委派管理員 (DA) 帳戶。

步驟 2：MAP 協議

如果您的遷移是AWS 遷移加速計劃 (MAP 2.0) 的一部分，請提供遷移產品組合體驗 (MPE) ID。這是使用大寫字母和數字的 10 個字元代碼 （ 例如 ABCDE12345)。當您提供 MPE ID 時，MAP 標籤會套用至跨網路遷移、登陸區域和伺服器重新託管階段建立的所有資源。標籤格式為：

- Key (索引鍵)：`map-migrated` Value (數值)：`mig`*`MPE_ID`*

您必須套用 MAP 標籤才能接收 MAP 點數。如需 MAP 的詳細資訊，請參閱 AWS Migration Acceleration Program。

步驟 3：連接器組態

您可以使用目標帳戶連接器，將遷移任務連線到遷移後工作負載所在的 AWS 環境。開始之前，請確認您的目標 AWS 帳戶 具有支援遷移基礎設施所需的許可、配額和組態。

當您核准連接器請求時，您可以將 AWS 轉換許可授予：

- 管理 VMware 遷移的 Amazon S3 儲存貯體操作 （ 讀取/寫入 ），以及對 AWS Migration Hub 和 AWS Application Migration Service (MGN) 的存取。這包括下列項目的許可，所有限制在目標帳戶中以 `CreatedBy:AWSTransform`或 標記的資源`CreatedFor:AWSTransform`：

  - 管理遷移波紋。
  - 管理網路組態 (Amazon EC2、VPC、傳輸閘道、Direct Connect、負載平衡器、網路防火牆）。
  - 管理 CloudFormation 堆疊部署。
  - 透過 Systems Manager 執行自動代理程式安裝。
- 使用儲存在探索區域中的資訊，將內部部署工作負載遷移至目標 AWS 帳戶 和區域。
- 在目標和區域中佈建和管理登陸區域基礎設施 AWS 帳戶 。這包括下列項目的許可，僅限於適用`CreatedBy:AWSTransform`時標記 的資源：
  - 針對開頭為 的儲存貯體執行 Amazon S3 儲存貯體操作 （建立、讀取、寫入、刪除）`transform-vmware-landing-zone-`。
  - 管理登陸區域 CloudFormation 堆疊的堆疊部署和變更集。
  - 執行 AWS Control Tower 操作。您可以管理登陸區域、啟用基準和啟用控制項。
  - 管理 AWS 組織。您可以建立和管理組織單位、建立帳戶和移動帳戶。
  - 透過 AWS Control Tower 管理服務控制政策 (SCPs)。
  - 管理 AWS Service Catalog 佈建成品。

> **Note**
>
> 當新功能需要許可變更時，連接器類型可能會更新。目標帳戶連接器類型的目前版本為 2.0。當您建立新的連接器時，會使用最新版本。

設定連接器之前，請先了解遷移中涉及的帳戶角色：

帳戶	說明
AWS 轉換帳戶	組織中 AWS 您設定 AWS 轉換的任何成員帳戶。這是 AWS 您的轉換工作區執行的位置。它不需要是管理帳戶。
連接器目標帳戶	您 AWS Transform 連接器所設定的 帳戶。這取決於您的遷移類型： • 單一帳戶遷移 – 連線到您要遷移工作負載的帳戶。連接器目標帳戶和目標帳戶相同。 • 多帳戶遷移 – 連線至組織管理帳戶或委派管理員 (DA) 帳戶。DA 帳戶必須註冊為 Organization AWS 中 MGN 和 CloudFormation StackSets 的

帳戶	說明
	委派管理員。 AWS Transform 會檢查連線帳戶是管理帳戶還是 DA 帳戶，並相應地調整其行為。
目標帳戶	工作負載遷移到 AWS 帳戶 的 。在單一帳戶遷移中，這與連接器目標帳戶相同。在多帳戶遷移中，這些是接收遷移工作負載的個別成員帳戶。

使用委派管理員帳戶

對於多帳戶遷移， AWS 建議您使用委派管理員 (DA) 帳戶，而不是直接使用組織管理帳戶。DA 帳戶透過限制遷移操作所需的許可範圍，遵循最低權限原則。DA 帳戶必須註冊為 AWS 組織中 MGN 和 CloudFormation StackSets 的委派管理員。

這兩個選項之間的主要差異是：

- 管理帳戶 – 可為整個組織的 MGN 和 CloudFormation StackSets 啟用受信任存取。使用 AWS 轉換 call CloudFormation StackSets APIs`CallAs: SELF`。
- 委派的管理員帳戶 – 無法直接啟用受信任的存取（必須從管理帳戶完成），但 可以管理 MGN 來源伺服器、啟動執行個體，以及跨成員帳戶部署 CloudFormation StackSets。 AWS 使用 轉換 call CloudFormation StackSets APIs`CallAs: DELEGATED_ADMIN`。

如需詳細資訊，請參閱 MGN 使用者指南中的 MGN 委派管理員。

連接器設定期間建立的 IAM 角色

在連接器設定期間， AWS Transform 會在您的目標帳戶中建立下列 IAM 角色：

- `AWSTransform-Connector-role-` – 當您在管理帳戶或 AWS Organization 的委派管理員帳戶中設定目標帳戶連接器時建立。此角色允許 AWS Transform 連線到您的目標帳戶，並代表您執行遷移操作。

目標帳戶連接器設定

> **Important**
>
> 在連接器設定期間，會在您的目標 中建立 Amazon S3 儲存貯體 AWS 帳戶。根據預設，此儲存貯體不會強制執行 HTTPS 限定存取 (`SecureTransport`)。如果您希望儲存貯體政策包含安全傳輸，您必須自行更新政策。如需詳細資訊，請參閱 Amazon S3 的安全最佳實務。

使用現有的目標帳戶連接器

1. 在任務計畫窗格中，展開選擇目標帳戶，然後選擇建立或選取連接器。
2. 在協同合作索引標籤中，選取現有的連接器，然後選擇使用連接器。如果連接器無法使用，其版本與您選取的任務類型不相容。

   > **Important**
   >
   > 如果您指定的連接器具有與 AWS 轉換區域不同的目標， AWS Transform AWS 區域 會跨傳輸您的資料 AWS 區域。

3. 選擇繼續。

建立新的連接器

1. 在任務計畫窗格中，展開 Connect 目標帳戶，然後選擇建立或選取連接器。
2. AWS 區域 為您的目標指定 AWS 帳戶 和 ，然後選擇下一步。

   > **Important**
   >
   > 如果目標與探索 AWS 區域 不同 AWS 區域， AWS Transform 會跨 傳輸您的資料 AWS 區域。

3. 選擇是否使用 Amazon S3 受管金鑰進行加密。如果您指定自己的 KMS 金鑰，您可以使用預設金鑰政策或較不寬鬆的金鑰政策。如需有關建立 KMS 金鑰的資訊，請參閱《 AWS Key Management Service 開發人員指南》中的建立 KMS 金鑰。

AWS 轉換會使用 kms:DescribeKey許可來驗證金鑰是否存在，kms:GenerateDataKey以及和 kms:Decrypt 來加密和解密 Amazon S3 儲存貯體中的任務資料。如需詳細資訊，請參閱使用 Amazon S3 儲存貯體金鑰降低 SSE-KMS 成本。

4. 選擇繼續。
5. 複製驗證連結，與目標管理員共用 AWS 帳戶，並要求他們核准連線請求。
6. 管理員核准請求後，從清單中選擇新建立的連接器，然後選擇使用連接器。
7. 選擇傳送以 AWS 轉換。

如果您打算修改 AWS Transform MGN 範本以啟用啟動後動作，請將下列許可新增至目標連接器角色。此 JSON 政策陳述式會授予啟動後動作角色的iam:PassRole許可。建立連接器後，您可以在協同合作索引標籤中找到角色名稱。如需有關將許可新增至角色的資訊，請參閱《IAM 使用者指南》中的更新角色的許可。

```
{
      "Sid": "MGNPostLaunchActions",
      "Effect": "Allow",
      "Action": [
        "iam:PassRole"
      ],
      "Resource": "arn:aws:iam::target-account-ID:role/service-role/
AWSApplicationMigrationLaunchInstanceWithSsmRole"
}
```

支援的目標區域

遷移目標區域是部署遷移資源 AWS 區域 的 ，包括登陸區域、網路基礎設施和伺服器重新託管。當您建立連接器時，請指定目標 AWS 區域。您可以使用下列任何一項 AWS 區域：

- 美國東部 (維吉尼亞北部)
- 美國東部 (俄亥俄)
- 美國西部 (加利佛尼亞北部)
- 美國西部 (奧勒岡)
- 非洲 (開普敦)
- 亞太地區 (香港)
- 亞太區域 (台北)

- 亞太地區 (孟買)
- 亞太地區 (海德拉巴)
- 亞太地區 (東京)
- 亞太地區 (首爾)
- 亞太地區 (大阪)
- 亞太地區 (新加坡)
- 亞太地區 (悉尼)
- 亞太地區 (雅加達)
- 亞太地區 (墨爾本)
- 亞太區域 (馬來西亞)
- 亞太區域 (紐西蘭)
- 亞太區域 (泰國)
- 加拿大 (中部)
- 加拿大西部 (卡加利)
- 歐洲 (法蘭克福)
- 歐洲 (蘇黎世)
- 歐洲 (愛爾蘭)
- 歐洲 (倫敦)
- 歐洲 (巴黎)
- 歐洲 (斯德哥爾摩)
- 歐洲 (米蘭)
- 歐洲 (西班牙)
- 以色列 (特拉維夫)
- 墨西哥 (中部)
- 南美洲 (聖保羅)

Important

如果您指定的目標與 AWS 轉換 AWS 區域 不同 AWS 區域，您的部分資料會跨 傳輸 AWS 區域。

請注意，您的伺服器複寫資料會直接從來源環境傳送至您的目標帳戶和區域。

建置登陸區域

AWS 轉換會引導您設計和部署 AWS 登陸區域，做為遷移專案的一部分。登陸區域是一種多帳戶 AWS 環境，可做為工作負載的基礎，並在任何工作負載到達之前就備妥組織邊界、控管控制和帳戶結構。AWS Transform 會分析您的遷移庫存和業務需求，以建議組織單位 (OU) 和帳戶結構、套用建議的服務控制政策 (SCPs)，以及產生和/或部署基礎設施做為程式碼 (IaC)。手動規劃和組態通常需要幾週的時間， AWS Transform 可以在單一對話中完成。

登陸區域代理程式會自動執行兩個階段：

- 基礎設定 – 建立核心登陸區域結構： AWS Control Tower、基礎 OUs和核心帳戶。
- 工作負載帳戶設計 – 根據您的遷移波紋、業務單位和環境分離需求設計和建立工作負載 OUs 和帳戶。

AWS 轉換支援綠地環境 （沒有現有的登陸區域） 和棕地環境 （已部署的現有 OUs 和帳戶）。在明視野案例中， AWS Transform 會偵測您現有的組織結構，並僅建議根據 AWS 最佳實務填補差距所需的變更，而不需要您從頭開始或執行手動差距分析。

連接器設定

在客服人員可以佈建資源之前，您可以將其連線到您的組織管理帳戶。登陸區域代理程式需要具有下列許可的目標 AWS 帳戶 連接器：

- 設定 AWS Control Tower
- 建立組織單位和帳戶
- 設定服務控制政策 SCPs)

當您核准連接器請求時，您可以將 AWS 轉換許可授予：

- 在目標和區域中佈建和管理登陸區域基礎設施 AWS 帳戶 。這包括下列項目的許可，僅限於標記 `CreatedBy:AWSTransform`和 的資源，`ATWorkspace:{workspace-id}`如適用：
  - 以 開頭之儲存貯體的 S3 儲存貯體操作 （建立、讀取、寫入、刪除） `transform-vmware-landing-zone-`
  - CloudFormation 登陸區域堆疊的堆疊部署和變更集管理
  - AWS Control Tower 操作 （管理登陸區域、啟用基準和控制）
  - AWS 組織管理 （建立和管理組織單位、建立帳戶和移動帳戶）

- 透過 AWS Control Tower 進行服務控制政策 (SCP) 管理
- AWS Service Catalog 佈建成品管理

建立連接器時，您可以指定目標 AWS 區域。此區域應與家用 Control Tower 區域相同。如需 Control Tower 區域的詳細資訊，請參閱如何使用 AWS 區域AWS Control Tower。

在登陸區域設定開始時， AWS Transform 會擷取您的連接器組態，並提供 AWS 組織管理帳戶 ID 和目標區域以供確認。如需詳細資訊，請參閱the section called “連接器”。

> **Important**
>
> IAM Identity Center 區域相依性 – AWS 轉換需要 AWS IAM Identity Center (IAM Identity Center)，這表示您的連接器區域必須符合 AWS Control Tower 主區域和 IAM Identity Center 區域。如果您的組織中已設定 IAM Identity Center， AWS 如果連接器鎖定不同的區域，則 Control Tower 初始化將會失敗。如需詳細資訊，請參閱 Control Tower 使用者指南中的 AWS IAM Identity Center 客戶的考量事項。

基礎設定

基礎設定階段會使用 AWS Control Tower 建立核心登陸區域基礎設施。當 AWS Control Tower 設定登陸區域時，它會自動在您的管理帳戶中佈建一組受管資源，這些資源構成整個 AWS 組織的控管基礎：

- 根 — 包含登陸區域中所有 OUs的最上層父系。
- 安全 OU – 由 Control Tower 自動建立。包含兩個共用帳戶：Log Archive 帳戶 （組織中所有 AWS API 活動和資源變更的集中、不可變記錄） 和 Audit 帳戶 （安全與合規審查的所有帳戶的唯讀存取權）。這些帳戶無法在初始設定後重新命名或取代。
- 強制性控制 （護欄） – Control Tower 會自動在整個組織中套用預防性和偵測性控制，以強制執行基準控管政策。這些無法停用。
- IAM Identity Center 目錄 – Control Tower 會為您的登陸區域使用者建立具有預先設定群組和單一登入存取權的雲端原生目錄。如需詳細資訊，請參閱 AWS IAM Identity Center。

Control Tower 使用 CloudFormation StackSets 在您的組織的所有帳戶和區域一致地部署和管理這些資源。您不得在支援的方法之外修改或刪除 Control Tower 受管資源，因為這樣做可能會導致您的登陸區域進入未知狀態。

帳戶電子郵件慣例

AWS 需要每個帳戶的唯一電子郵件地址。這些電子郵件會收到帳戶的重要通知。 AWS Transform 使用加上定址，從單一信箱產生唯一的帳戶電子郵件。

格式：`prefix+account-name@domain`

您提供字首 （例如 `aws-admin`) 和網域 （例如 `acme.com`)，而 AWS 轉換會自動衍生所有帳戶電子郵件。例如：

- 稽核帳戶： `aws-admin+audit@acme.com`
- Log Archive 帳戶： `aws-admin+log-archive@acme.com`
- 沙盒帳戶： `aws-admin+sandbox@acme.com`

在布朗欄位案例中， AWS Transform 會檢查現有的帳戶電子郵件，以推斷已在使用中的加定地址慣例，並提議繼續使用相同的模式。

建議的基礎結構

根據 AWS 最佳實務， AWS Transform 建議下列基礎 OU 結構。您可以在建立之前加以自訂。

OU	用途	帳戶
安全	集中式稽核記錄和監控。在專用帳戶中隔離這些服務旨在協助將您的稽核線索與工作負載團隊分開。	稽核、日誌封存
基礎設施	共用聯網 （傳輸閘道、VPN)、DNS 和常見服務。建議集中這些項目，以協助減少重複項目，並為網路團隊提供單一位置來管理連線。	無 （空白建立）
沙盒	開發人員實驗支出限制和限制存取。建議為開發人員提供實驗空間，而不會危及生產資源。	沙盒
工作負載	包含生產、非生產和選用的受監管子 OUs。工作負載帳戶是根據您的遷移需求在下一個階段設計。	無 （空白建立）

> **Note**
>
> 具有 Audit 和 Log Archive 帳戶的安全 OU 會建立為 Control Tower 基礎設定的一部分。在您確認結構之後，會分別建立 Infrastructure、Sandbox 和 Workloads OUs。

在明視野案例中， AWS Transform 會將您現有的基礎與此建議的結構進行比較，並僅報告差距。例如：「您的基礎具有安全和基礎設施 OUs但沒有沙盒 OU。」

服務控制政策 (SCP)

SCPs 是組織層級的許可護欄，可為 AWS 組織中的所有帳戶設定最大許可。他們不會授予存取權，而是定義帳戶中沒有人可以超過的界限，甚至是帳戶管理員。

做為 Control Tower 部署的一部分，會自動套用基準護欄。 AWS Transform 也建議旨在協助強化組織狀態的其他 SCPs。這些是根據最低可行登陸區域的 AWS 最佳實務。

SCPs可以套用至基礎設施、沙盒和工作負載 OUs。Security OU 由 Control Tower 管理，SCPs無法透過此工具鎖定目標。

> **Important**
>
> Security OU 是由 Control Tower 管理的基礎 OU。您無法透過登陸區域代理程式新增帳戶、SCPs 或任何資源。

在明視野案例中， AWS 轉換會檢查已套用哪些 SCPs並僅建議會填補差距的 SCP。

基礎部署

基礎設計完成後，您可以選擇如何部署：

- 為我部署 – AWS Transform 會將基礎 OUs、帳戶和 SCPs 部署到您的 AWS 組織。
- 我將自行部署 – AWS Transform 會產生基礎設施即程式碼 (IaC) 成品，以您偏好的格式下載 （ 請參閱 the section called “IaC 格式”)。
- 首先設計工作負載帳戶 – 略過部署並繼續工作負載帳戶設計階段。您可以稍後一起部署所有項目。

Control Tower 初始化

如果 AWS Transform 偵測到 AWS Control Tower 尚未在您的組織中初始化，它會為使用者提供 AWS 轉換主控台頁面的連結。在連結中產生 操作會建立 CloudFormation 堆疊以引導 Control Tower。程序會在 CloudFormation 主控台中為您的目標區域建立此堆疊。堆疊建立完成後， AWS Transform 會繼續部署。

工作負載帳戶設計

在工作負載帳戶設計階段， AWS Transform 會根據您的遷移庫存、業務需求和環境分離偏好設定，為您的應用程式工作負載設計 OU 和帳戶結構。

遷移規劃內容

AWS Transform 會從遷移規劃階段擷取資料，包括波動計畫、server-to-application映射和共用內容。如果遷移規劃資料可用， AWS Transform 會顯示摘要，並要求您確認或調整摘要。如果沒有可用的遷移規劃資料， AWS Transform 會直接詢問探索問題。

探索

AWS 轉換會提出問題，以了解您的工作負載需求。您可以略過任何問題。主題包括：

- 使用 的業務單位或團隊數量 AWS
- 產業和任何適用的架構 (HIPAA、PCI-DSS、SOC2、FedRAMP)
- 工作負載是否處理敏感資料 (PII、PHI、財務）
- 環境分離偏好設定 (dev/test/staging/prod 作為個別帳戶或共用）
- 工作負載隔離要求
- 商業應用程式及其用途
- 伺服器分組到應用程式
- 成本追蹤和分配需求（依業務單位、專案、環境）
- 未來 12–24 個月的預期成長
- 帳戶策略偏好設定（每個帳戶、分組或以環境為基礎的單一應用程式）

建議的工作負載結構

根據您的答案和遷移規劃資料， AWS Transform 會在工作負載 OU 下提供 OU 和帳戶結構。提案包含每個設計決策背後的推理。

AWS 轉換遵循以下設計原則：

- 遷移波動中的所有伺服器都會前往相同的帳戶 — 波無法跨帳戶分割。這是波動執行期間的重新託管限制。
- 如果您請求隔離的環境， AWS Transform 會建立工作負載/生產和工作負載/非生產子 OUs。
- 如果識別適用的架構， AWS Transform 會建立 Workloads/Regulated and Workloads/Standard sub-OUs
- 如果多個業務單位需要不同的控管， AWS Transform 會在工作負載下建立business-unit-specific OUs。
- 關鍵或敏感資料應用程式會取得每個帳戶的單一應用程式。在這種情況下，您可能需要反覆執行波動計畫。
- 具有共用相依性的緊密耦合應用程式會分組在一個帳戶中。

每個提議的帳戶包括：名稱、用途、目標 OU 和業務單位。 AWS Transform 會顯示正在使用的命名慣例（例如 `<business-unit>-<environment>-<workload>`）。

您可以在 AWS 轉換套用變更之前檢閱和修改提議的結構。套用後，您可以反覆執行 - 進行其他變更，直到您滿意為止。

工作負載 SCP 組態

建立工作負載結構之後， AWS Transform 會顯示可用的 SCPs並詢問您是否要將任何 套用至工作負載 OUs。您選取要套用的 SCPs 和 OUs. AWS Transform 套用的 SCPs並顯示具有 SCP 摘要資料表的已更新組織樹狀目錄。

工作負載部署

工作負載設計完成後，您可以選擇如何部署：

- 為我部署 – AWS Transform 會將工作負載 OUs、帳戶和 SCPs 部署到您的 AWS 組織。
- 我將自行部署 – AWS Transform 會產生 IaC 成品，以您偏好的格式下載（請參閱 the section called “IaC 格式”）。

IaC 格式

當您選擇自我部署時， AWS Transform 會以下列格式產生基礎設施做為程式碼成品：

- AWS Cloud Development Kit (AWS CDK) – 用於程式設計基礎設施部署的 TypeScript 專案。

- HashiCorp Terraform – 產生 HashiCorp 組態語言 (HCL) 範本來管理登陸區域資源。
- 登陸區域加速器 (LZA) – 根據 LZA Universal Configuration 1.1.0 版來設定 YAML 檔案。這些企業就緒範本可在 上使用登陸區域加速器 AWS 來建立多帳戶 AWS 環境。產生的檔案包含預先設定的控管、組織結構和聯網設定，以符合 AWS 最佳實務。若要進一步了解，請參閱 LZA 通用組態。

> **Note**
>
> 透過登陸區域加速器 (LZA) 管道部署時，您的 AWS 轉換帳戶和 LZA 安裝必須位於相同的 AWS 組織。如果 AWS 轉換和 LZA 中使用的 Organizations IDs 不相符，部署將會失敗。若要了解如何使用 Organizations 設定 LZA 安裝，請參閱以 AWS Organizations 為基礎的安裝。

選取格式後， AWS Transform 會產生成品並可供下載。

若要驗證下載的檔案尚未損毀或遭到竄改，請產生和下載檢查總和，然後使用 將其與本機產生的雜湊進行比較：

```
openssl dgst -sha256 -binary <file.zip> | base64
```

部署核准程序

登陸區域部署請求在執行之前需要明確核准。當您提交部署請求時，它會透過 AWS 轉換核准索引標籤自動路由至授權核准者。

核准者會檢閱 CloudFormation 範本和登陸區域組態。只有在 AWS 轉換中具有管理員角色的使用者才能核准部署請求。每個提交都會觸發新的檢閱週期，而且只有在收到確認後才會繼續部署。

如果核准者拒絕您的請求，請直接聯絡他們以討論必要的修改。系統會針對稽核目的追蹤所有核准決策，並維護部署歷史記錄。

標記登陸區域資源

AWS 轉換會自動標記所有產生的資源`"CreatedBy": "AWSTransform"`以及定義和執行 IDs以供追蹤之用。

自動標籤

所有登陸區域資源都會收到下列標籤：

- `CreatedBy` – AWSTransform
- `ATWorkspace` – 工作區識別符

> **Note**
>
> 如果您的遷移是 AWS Migration Acceleration Program (MAP 2.0) 的一部分，您可以包含必要的 MAP 標籤：金鑰：`map-migrated`值： `migMPE_ID`（其中 MPE_ID 是您的遷移產品組合評估識別符）。在連接器設定階段請求 MAP 標籤。 AWS Transform 會在登陸區域部署期間套用這些標籤。

反轉變更

只能移除未部署的元素。部署 OU 或帳戶後，就無法透過登陸區域代理程式移除。

移除元素時，順序很重要 — 您必須在父系之前移除子系：

1. 先移除帳戶 （透過電子郵件）。
2. 從 OUs 移除 SCPs。
3. 移除子 OUs — 如果 OU 仍有帳戶或巢狀 OUs，則無法移除。

相關資源

- the section called “連接目標 AWS 帳戶和區域”
- the section called “將您的網路遷移至 AWS”
- AWS Control Tower 使用者指南
- AWS Organizations 使用者指南
- AWS IAM Identity Center 使用者指南
- CloudFormation 使用者指南
- 上的登陸區域加速器 AWS
- AWS Well-Architected 架構
- AWS 方案指引：建置登陸區域

將您的網路遷移至 AWS

使用 AWS 轉換，您可以在手動設計和部署所需的一 AWS 小部分時間內將網路遷移到 。 AWS 轉換使用 AI 支援的代理程式，將您的來源環境組態轉譯為生產就緒 AWS 的網路資源，包括 VPCs、子網路、安全群組、NAT 閘道、傳輸閘道、彈性 IPs、路由和路由表。您可以在部署之前，透過對話界面檢閱和修改產生的網路組態。您可以使用 AWS Transform 直接部署，或選擇自我部署，並以您偏好的格式接收基礎設施即程式碼 (IaC)： AWS Cloud Development Kit (AWS CDK)、登陸區域加速器 (LZA) 或 HashiCorp Terraform。

AWS 轉換代理程式會引導您完成下列步驟，在您做出決策時處理分析和產生：

1. 上傳您的來源網路檔案。
2. 上傳其他組態檔案 （選用，適用於 RVTools 環境）。
3. 選取網路拓撲。
4. 選取安全群組映射策略。
5. 檢閱並最佳化您的網路。
6. 產生網路圖表 （選用）。
7. 設定資源標記。
8. 部署您的網路。

> **Note**
>
> 對於多帳戶部署，您必須在開始網路遷移之前為 AWS Organizations 設定跨帳戶 IAM 角色和受信任存取。如需遷移類型的詳細資訊，請參閱 the section called “步驟 1：遷移類型選擇”。

步驟 1：來源網路映射

AWS 轉換會從各種來源網路組態檔案產生目標網路基礎設施。從來源環境上傳一或多個組態檔案，而 AWS Transform 會使用資訊來產生目標網路，包括 Amazon VPCs、子網路和安全群組。雖然 AWS 轉換不會產生防火牆或負載平衡器資源，但來自這些網路元素的組態可以用作產生目標網路的輸入。

AWS Transform 接受來自下列來源類型的組態檔案：

- 軟體定義網路 (SDN)：適用於 VMware NSX 網路虛擬化的匯入/匯出，或適用於 Cisco Application Centric Infrastructure 的 Cisco ACI 組態。

- VMware vSphere 網路：RVTools。當您使用 RVTools 檔案時， AWS Transform 只會產生 Amazon VPC 組態。安全群組組態需要防火牆或軟體定義網路檔案的額外輸入。如需從其他檔案產生安全群組的詳細資訊，請參閱其他組態檔案。
- 以防火牆組態資料為基礎的網路：從 Palo Alto Networks Firewall、Fortinet FortiGate Firewall 或 Cisco ACI 匯出檔案。如需支援版本和擷取指示的詳細資訊，請參閱組態檔案擷取。
- 同時執行 VMware 和非 VMware 工作負載的混合網路：AWS 轉換探索工具或modelizeIT。
- 其他檔案類型： AWS Transform 也接受其他網路組態檔案，例如檢查點和 F5 組態。如果您的組態檔案不是上面列出的格式之一， AWS Transform 會自動轉換它並使用它來產生目標網路。根據檔案大小和複雜性，此轉換最多可能需要兩個小時。

> **Note**
>
> 支援的來源網路檔案大小上限為 70 MB。

> **Note**
>
> 若要在網路檢閱期間啟用過時的安全群組規則移除，請從AWS 轉換探索工具提交觀察到的網路流量資料，或與您的來源網路組態一起modelizeIT。如需詳細資訊，請參閱引導式網路建議。

> **Warning**
>
> 僅從官方 Dell 網站 https：//https://www.dell.com/en-us/shop/vmware/sl/rvtools 下載 RVTools。請勿從非官方來源下載 RVTools。

每個來源網路區段都會對應至自己的不同 VPC。網路分割因來源類型而異：

- vNetwork： AWS 依 vSwitch 和虛擬 LAN (VLAN) 將 VMs 分組。VLANs可以顯示在多個 vSwitches 下 (VLAN 0 除外）。
- NSX 網路： AWS Transform 會根據 Tier-1 路由器分割網路，將路由器分組並收集其區段。

步驟 2：其他組態檔案

對於 RVTools 來源環境，您可以選擇上傳其他組態檔案，以啟用安全群組產生。如果您未上傳其他組態檔案，則不會為 RVTools 型遷移產生安全群組。

AWS 轉換支援下列其他組態檔案類型。您只能從一個平台上傳一個組態檔案。

- Cisco Application Centric Infrastructure (ACI) 提供網路政策組態。
- Palo Alto Networks 提供防火牆安全政策。
- Fortinet FortiGate 提供防火牆安全政策。

當您上傳防火牆或 Cisco ACI 檔案時， AWS Transform 會產生網路基礎設施和安全群組。當您單獨上傳 RVTools 檔案時， AWS Transform 只會產生網路基礎設施。

如需支援版本和擷取指示的詳細資訊，請參閱組態檔案擷取。

步驟 3：網路拓撲

在網路定義步驟期間，您可以選取網路拓撲。您可以選擇隔離VPCs 拓撲或 Hub 和 Spoke 拓撲。

隔離的 VPC

部署的項目

隔離VPCs 是獨立的網路環境，可在其中做為個別單位運作 AWS。您的 VPCs完全隔離，兩者之間沒有內建的通訊路徑。此區隔可提供最高層級的網路邊界保護。

AWS 轉換會建立下列資源：

- 每個偵測到來源網路區段的專用 VPC。
- 根據您的來源網路組態的私有子網路。
- 安全群組 （如果您提供防火牆或 SDN 組態檔案）。

完成您的設定

AWS Transform 會為您部署核心網路基礎設施。您完成最終連線和安全性組態，以符合組織的需求。

若要啟用隔離 VPC 的網際網路存取，請完成下列步驟：

1. 建立網際網路閘道並將其連接到 VPC。
2. 在您需要網際網路存取的每個可用區域中建立公有子網路。新增`0.0.0.0/0`指向網際網路閘道的路由。如需子網路組態的詳細資訊，請參閱 VPC 的子網路。
3. 在公有子網路中建立 NAT 閘道（每個可用區域一個，以實現高可用性）。為每個 NAT 閘道配置彈性 IP。
4. 更新您的私有子網路路由表。新增`0.0.0.0/0`指向相同 AZ 中 NAT 閘道的路由。
5. 檢閱您的安全群組規則。確保傳出規則允許工作負載所需的流量 (HTTPS、DNS 等）。

對於 VPC-to-VPC通訊，請設定 VPC 對等互連或 Transit Gateway，並更新每個 VPC 中的路由表，將流量路由到對等互連或 TGW 連接。

中樞和發言

在此模型中，AWS Transit Gateway 充當連接多個工作負載 VPCs（輻條）的中樞。

部署的項目

AWS 轉換會建立下列資源：

- 呼叫 VPCs：每個偵測到的來源網路區段一個 VPC，具有私有子網路和 Transit Gateway 連接。
- 檢查 VPC：託管防火牆設備以進行流量檢查。所有跨 VPC 流量都會透過此 VPC 路由。Transit Gateway 連接使用設備模式，此設定可確保流量對稱地流經相同的設備，以雙向連線。
- 傳入 VPC：處理從公有網際網路（南北傳入）進入您網路的流量。包括跨多個可用區域的網際網路閘道和公有子網路。
- 傳出 VPC：處理從網路到公有網際網路的流量（南北傳出）。包括網際網路閘道、每個可用區域中具有彈性 IP 地址的 NAT 閘道以獲得高可用性，以及 Transit Gateway 連接的私有子網路。
- 傳輸閘道路由表：兩個路由表透過檢查 VPC 引導流量。未檢查的資料表與輻條 VPCs、傳入 VPC 和傳出 VPC 相關聯。它將所有流量 (0.0.0.0/0) 路由到檢測 VPC 附件，並且是預設關聯路由表。檢查的資料表與檢查 VPC 相關聯。它包含來自所有語音 VPCs傳播路由，並且是預設傳播路由表。

對於多帳戶部署，傳輸閘道會透過 AWS Resource Access Manager (RAM) 跨帳戶共用。

流量

所有跨 VPC 流量都遵循此路徑：

1. 來自語音 VPC 的流量會傳送至 Transit Gateway（預設路由 0.0.0.0/0)。

2. 未檢查的路由表會將流量路由到檢查 VPC。
3. 檢查 VPC 中的防火牆會檢查流量，並將其轉傳到 Transit Gateway。
4. 檢查的路由表會使用傳播的路由，將流量路由到目的地輻條 VPC。

對於傳出網際網路流量，檢查的路由表會將流量路由到傳出 VPC。NAT 閘道會在流量轉送至網際網路閘道之前轉譯私有 IP 地址。傳出 VPC 公有路由表包含傳回 Transit Gateway 的每個發言 VPC 無類別網域間路由 (CIDR) 範圍的特定路由。這些路由可讓傳回流量到達正確的語音 VPC。

傳入網際網路流量會透過傳入 VPC 的網際網路閘道進入，並遵循相同的檢查路徑來到達語音 VPCs。

完成您的設定

AWS Transform 會為您部署核心網路基礎設施，包括 Transit Gateway、語音 VPCs和流量路由。您可以完成防火牆組態和傳入服務設定，以符合組織的安全需求。

> **Note**
>
> 根據預設，跨 VPC 流量會通過檢查 VPC，無需檢查。您必須部署防火牆才能啟用流量檢查。

部署防火牆：在防火牆端點的檢查 VPC 中建立其他子網路。 AWS Transform 只會為 Transit Gateway 連接建立子網路。將流量從 TGW 連接子網路路由到防火牆端點，以及從防火牆子網路路由回 Transit Gateway。您可以部署 AWS Network Firewall 或第三方設備。如需使用 Transit Gateway 部署防火牆的詳細資訊，請參閱使用 Transit Gateway 建立防火牆。

驗證連線：部署防火牆後，測試來自語音 VPC 執行個體的傳出網際網路存取（例如 `curl https://aws.amazon.com`)。您可以使用 Reachability Analyzer 對連線問題進行疑難排解。

設定傳入服務：若要託管面向公有的服務，請在傳入 VPC 公有子網路中部署 Application Load Balancer 或 Network Load Balancer。透過 Transit Gateway 設定指向語音 VPCs中執行個體的目標群組，並確認檢查的路由表具有傳回傳入 VPC 的路由。

如果您想要精細控制 VPCs之間的通訊，請選擇隔離的 VPCs選項，然後修改產生的網路，以建立所需的特定通訊路徑。

步驟 4：安全群組映射

選擇來源安全政策如何轉換為 AWS 安全群組。 AWS Transform 會根據來源環境組態建立安全群組。安全政策、安全政策規則、閘道政策和閘道政策規則會轉換為安全群組。

> **Important**
>
> AWS 轉換會盡力建立安全群組，以符合您的來源環境。檢閱和修改產生的安全群組，以確保它們符合您公司的需求和安全政策。

安全群組參考

產生安全群組時， AWS Transform 會使用支援的安全群組參考。參考安全群組會根據另一個安全群組 ID 而非特定 IP 地址範圍 (CIDR 區塊） 來設定安全規則。此方法提供更靈活且可維護的安全組態。

您的安全群組規則只能參考相同 VPC 內的其他安全群組，或在相同區域內連接的 VPC 中。也支援跨帳戶參考。您無法在未連線的 VPC 中或跨區域參考安全群組。對於連線VPCs，只有傳入規則支援跨 VPC 安全群組參考。傳出規則必須使用以 CIDR 為基礎的規則。 AWS 轉換如何建立安全群組規則取決於您選擇的網路拓撲：

- 中樞和發言：傳輸閘道提供 VPCs之間的網路連線。 AWS Transform 使用 VPC 內和跨 VPC/跨帳戶傳入規則的參考。跨 VPC/跨帳戶輸出 （傳出） 規則使用以 CIDR 為基礎的規則。
- 隔離VPCs：您的 VPCs之間沒有網路連線。 AWS Transform 只會針對 VPC 內規則使用參考。所有跨 VPC 和跨帳戶規則都使用以 CIDR 為基礎的規則。

當來源組態非對稱時，也會使用 CIDR 型規則。

選擇下列其中一個安全群組映射策略：

- MAP：將安全規則從來源環境轉換為 AWS 安全群組和規則。針對使用靜態 IP 定址的遷移，請使用此選項。
- MAP_DHCP （使用 DHCP 支援翻譯）：使用 DHCP 相容性從您的來源環境翻譯安全規則。DHCP 會從子網路的 CIDR 範圍動態指派 IP 地址。因此，跨 VPC 輸出規則會擴大，以符合完整的目的地子網路 CIDR。較窄的 CIDR 會封鎖超出該範圍的 IPs。遷移後檢閱這些規則。

  使用此選項支援跨 VPC Transit Gateway 通訊的 DHCP。也適用於靜態 IPs，但可能會產生比 MAP 更廣泛的規則。
- SKIP：不翻譯安全規則。遷移後手動設定 AWS 安全群組。適用於靜態 IP 和 DHCP 環境。對於沒有其他組態檔案的 RVTools 來源環境， AWS Transform 會自動使用 SKIP。

> **Note**
>
> 您的映射策略會決定您的 IP 指派選項。MAP 僅支援靜態 IP。MAP_DHCP 和 SKIP 同時支援靜態和 DHCP。

IP 遷移方法

您的遷移有兩種網路組態選擇：

網路範圍選擇

- 保留現有範圍 (IP 地址範圍保留）：在遷移期間保留原始 IP 地址範圍。非常適合在沒有修改 AWS 的情況下將應用程式移至 (lift-and-shift) 的遷移，尤其是具有硬式編碼 IP 相依性或現有防火牆規則的舊版應用程式。
- 更新至新的 IP 範圍 (CIDR 更新）：您可以在遷移期間修改每個 VPC CIDR 範圍， AWS 轉換會自動傳播子網路、路由表和安全群組的變更。

IP 地址指派

- 固定 IP 地址 （靜態）： AWS Transform 會根據 CIDR 指派靜態 IPs。這最適合需要可預測網路行為、DNS 管理或 IP 型存取控制的應用程式。IPs會透過彈性網路界面 (ENIs) 在整個執行個體重新啟動之間保留，ENI 是連接到執行個體的虛擬網路卡。
- 動態 IP 指派 (AWS DHCP)：執行個體啟動時自動從子網路集區指派 IPs。最適合在雲端和自動擴展工作負載中執行的應用程式。減少營運開銷，但需要應用程式使用 DNS 或服務探索。

您可以將任一範圍選擇與任一 IP 指派方法合併。

> **Note**
>
> IP 地址指派策略是在波動層級設定。您可以自訂 wave 檔案，將不同的策略指派給特定伺服器。例如，如果您為波動選擇靜態 IP 地址方法，但想要將動態方法指派給特定伺服器，您可以使用 [RESET_VALUE]，如 MGN 使用者指南中的編輯組態中所述。

步驟 5：檢閱和最佳化您的網路

AWS 轉換產生目標網路組態後，您可以檢閱與 AWS 基礎設施整合的內部部署網路區段。使用視覺化界面來檢閱您的網路，並使用聊天界面進行變更並接收引導式建議。 AWS Transform 會執行層疊影響分析並實作必要的變更，以維持網路一致性並符合最佳實務。您也可以要求 AWS Transform 分析您的網路並建議最佳化。如需詳細資訊，請參閱引導式建議。

目標帳戶中VPCs

如果您的目標帳戶已包含 VPCs，則從先前的遷移階段或平行基礎設施專案， AWS Transform 會自動偵測它們，並在審核過程中與您的映射 VPCs一起顯示它們。對於多帳戶遷移， AWS Transform 會偵測 AWS 組織中所有帳戶的現有 VPCs。

此可見性可協助您了解規劃的網路與現有基礎設施的關係、識別潛在的 CIDR 衝突，以及在部署之前做出明智的決策。

> **Note**
>
> AWS 轉換只會偵測現有的 VPCs （而非子網路或其他資源）。偵測為唯讀。 AWS Transform 不會修改您現有的 VPCs。

最佳化您的網路

> **Note**
>
> 這些操作僅適用於工作負載 VPCs。對於 Hub 和 Spoke 拓撲中的設備 VPCs （檢查、傳入、傳出），僅支援變更 IP 地址。
> 您無法復原刪除、合併和分割操作。套用這些變更之前，請仔細檢閱您的組態。

下列操作適用於 VPCs：

- 刪除：從組態永久移除 VPC。將此用於不應遷移至的過時網路區段 AWS。
- 排除：暫時從分階段遷移策略的遷移中移除 VPC。未部署排除VPCs，但稍後可以重新包含。
- 包含：將先前排除的 VPC 新增至遷移。
- 合併：將兩個 VPCs 合併為一個。第一個 VPC 會保留其身分，並從第二個 VPC 吸收所有子網路。安全群組會移至合併的 VPC，並相應地重建其關聯。第一個 VPC 的 CIDR 會擴展到包含兩個原始 CIDR 的最小 CIDRs範圍，且路由會自動更新。第二個 VPC 會從組態中移除。

合併需求：

- 子網路 CIDRs不得在兩個 VPCs之間重疊。
- 合併的 CIDR 不得超過 /16。
- 對於多帳戶部署，兩個 VPCs 必須指派給相同的帳戶。

- 變更 IP 地址：變更 VPC CIDR 的基本 IP 地址，同時保留相同的字首長度。 AWS Transform 會自動以相同的位移平移所有子網路 CIDRs。例如，將 VPC 從 `10.0.0.0/16` 變更為 會將子網路從 `10.20.0.0/16`轉移到 `10.0.1.0/24` `10.20.1.0/24`。

  完全符合舊 VPC CIDR 的安全群組規則會自動更新。部分重疊或不符合舊 CIDR 的規則不會變更。在變更後檢閱這些規則。
- 重新命名：變更 VPC 的名稱，以符合組織的成本分配、合規追蹤和操作標準的命名慣例。
- 調整大小：變更 VPC CIDR 的字首長度，以展開或減少 IP 地址範圍。
  - 字首長度減少 （更多 IPs，例如 /20 到 /16)：子網路仍位於較大的範圍內。不需要變更子網路。
  - 字首長度增加 （較少 IPs，例如 /16 到 /20)：超出新範圍的子網路必須先使用子網路調整大小操作來調整大小。

  完全符合舊 VPC CIDR 的安全群組規則會自動更新。部分重疊或不符合舊 CIDR 的規則不會變更。調整大小後檢閱這些規則。

  調整需求大小：
  - 新的 CIDR 必須介於 /16 和 /28 之間。
  - 新的 CIDR 不得與網路中的其他 VPCs重疊 (Hub 和 Spoke 拓撲）。
  - 減少 CIDR 時，所有現有的子網路都必須符合新的 CIDR。如有需要，請先調整子網路的大小。
- 分割：根據您提供的 CIDR 邊界，將 VPC 分割成兩個 VPCs。子網路會指派給 CIDR 包含它們的新 VPC。安全群組會複製到兩個新的 VPCs，但安全群組規則 CIDRs 不會自動更新。在分割後檢閱您的規則，以確保跨 VPC 通訊如預期般運作。原始 VPC 會由兩個新的 VPCs取代。

  分割需求：
  - 您必須提供剛好兩個 CIDR 範圍。
  - 兩個 CIDRs不得重疊。
  - 每個 CIDR 必須介於 /16 和 /28 之間。
  - 每個子網路都必須完全符合兩個 CIDRs的其中之一。如果有任何子網路不適用，則會拒絕操作。

子網路可使用下列操作：

- 變更 IP 地址：變更子網路 CIDR 的基本 IP 地址，同時保留相同的字首長度。
- 刪除：從組態永久移除子網路，而不會影響父 VPC。
- 調整大小：變更子網路 CIDR 的字首長度，以展開或減少 IP 地址範圍。

  子網路調整大小需求：

  - 新的 CIDR 必須介於 /16 和 /28 之間。
  - 新的 CIDR 不得與相同 VPC 中的其他子網路重疊。
  - 新的 CIDR 必須在父 VPC CIDR 內。

在每次操作之後， AWS Transform 會重新評估安全群組參考，這可能會將 CIDR 型規則轉換為安全群組參考，反之亦然。在您進行變更以確認它們符合您的需求後，請檢閱您的安全群組規則。

引導式網路建議

AWS 轉換會自動透過聊天介面分析映射的網路和表面優先順序建議，識別通常需要網路架構師手動檢閱的最佳化。建議是以您的網路資料為基礎，並且在套用任何變更之前需要您的確認。

AWS 轉換可能會建議下列最佳化：

- CIDR 衝突解決：標記映射 VPCs與 AWS 組織中所有帳戶現有 VPCs 之間的重疊 CIDR 範圍。首先顯示衝突VPCs。您可以透過重新定址映射的 VPC、排除或刪除 VPC，或確認衝突並在部署後自行解決衝突來解決衝突。
- 命名標準化：標記不符合一致模式的 VPC 名稱（例如，包含硬體參考的名稱）。 AWS 在提議替換之前，轉換會要求您的雲端命名慣例。
- 範圍檢閱：識別可能不需要遷移到的網路區段 AWS，例如等待解除委任的舊版系統或建構。 AWS Transform 會在排除任何建構之前請求您的確認。
- VPC 容量適當調整大小：CIDR 顯示為超大或過小VPCs 包含的子網路。 AWS Transform 會顯示目前的容量資料，並讓您決定是否要調整大小。
- 安全檢閱：標記允許無限制傳入流量 (0.0.0.0/0) 供您檢閱的安全群組規則。
- 移除過時的安全群組規則：識別從內部部署環境遷移的未使用傳入防火牆規則，並建議將其移除，因此您不會繼續執行不再提供用途的安全暴露。為了識別未使用的規則， AWS Transform 會使用 AWS Transform 探索工具或 modelizeIT 收集的觀察網路流量資料。您必須將此流量資料與來源網路輸入一起提交。 AWS Transform 會將遷移的防火牆規則與在該資料中擷取的觀察視窗中觀察到的流量進行比較，並在沒有傳入流量符合規則時，將規則標記為未使用。如果沒有流量資料， AWS Transform 無法判斷哪些規則未使用，也不建議移除。 AWS Transform 只會移除未使用的輸入（傳

入）規則。沒有觀察到的傳入流量是規則未使用的可靠訊號。在套用之前，請檢閱建議的移除，以確認它們符合您的安全政策。

- VPC 整合：識別以實體基礎設施限制分隔VPCs，而不是邏輯隔離要求，並建議合併它們。

> **Note**
>
> 在 AWS 轉換套用任何變更之前，所有建議都需要您明確確認。當建議影響您網路的多個層面時， AWS 轉換會顯示權衡。

步驟 6：網路圖表

檢閱產生的 VPC 組態後，您可以選擇產生網路圖表以視覺化您的網路拓撲。 AWS Transform 支援下列圖表格式：

- Mermaid 程式碼 (.mmd)：此格式會產生以文字為基礎的圖表定義檔案，您可以使用 Mermaid 相容工具進行轉譯。
- 影像 (.png)：此格式會產生網路拓撲的轉譯影像。

步驟 7：設定資源標記

您的網路資源會標記為啟動和複寫。您也可以新增自訂標籤和 AWS Migration Acceleration Program (MAP) 標籤。

啟動和複寫的自動標籤

AWS 轉換會使用下列標籤自動標記遷移的網路資源 (VPCs、子網路、安全群組和路由表）：

- Key (索引鍵)：`CreatedBy` Value (數值)：`AWSApplicationMigrationService`
- Key (索引鍵)：`ATWorkspace` Value (數值)：*`workspace-id`*

這些標籤允許使用 VPC 和子網路在其中啟動測試和切換執行個體 AWS。

> **Note**
>
> 您遷移VPCs 和子網路預設不包含網際網路連線，因此不適合做為複寫的預備區域。

若要使用 VPC 和子網路做為預備區域（複寫），請手動新增下列標籤：

- Key (索引鍵)：`CreatedFor` Value (數值)：`AWSTransform`
- Key (索引鍵)：`ATWorkspace` Value (數值)：*`workspace-id`*

您也可以將這些標籤套用至任何現有的 AWS 網路資源，使其可用於複寫。

在 AWS 轉換 Web 應用程式 URL 中尋找您的工作區 ID：https：//... /workspace/*`workspace-id`*/job/job-id

自訂標籤

除了 AWS Transform 自動套用的標籤之外，您還可以選擇新增自訂標籤，以組織、追蹤成本和管理遷移網路資源的合規性。您可以在兩個層級套用自訂標籤：

- 任務層級標籤：套用至此任務建立的所有資源，包括所有 VPCs、子網路、安全群組和路由表。
- VPC 層級標籤：套用至特定 VPC，並自動串聯至其所有相關聯的資源（子網路、安全群組、路由表）。

> **Note**
>
> 每個請求最多 40 個標籤。每個標籤都需要金鑰和 value. AWS tagging 慣例。

AWS 轉換會在產生基礎設施做為程式碼範本時套用這些標籤。

AWS 遷移加速計劃

如果您的遷移是 AWS Migration Acceleration Program (MAP 2.0) 的一部分， AWS Transform 會將 MAP 標籤套用至您的 資源。如果您先前在遷移程序中提供了 MPE ID，則會自動套用標籤。否則，在您完成檢閱產生的 VPC 組態後， AWS Transform 會詢問您是否擁有 MAP 協議，並提示您提供 MPE ID。MPE ID 是使用大寫字母和數字的 10 個字元代碼（例如 ABCDE12345)。套用的標籤使用 格式：

- Key (索引鍵)：`map-migrated` Value (數值)：`mig`*`MPE_ID`*

步驟 8：部署您的網路

標記後，選取您的部署策略：

- AWS 轉換受管部署： AWS Transform 使用 CloudFormation 範本來部署您的網路，並執行 Reachability Analyzer 來檢查跨多個 VPCs 和相同 VPC 內子網路之間的連線。

  > **Note**
  >
  > 您必須先取得明確核准，網路部署請求才會執行。請參閱部署核准程序。

- 自我部署： AWS Transform 會產生基礎設施即程式碼 (IaC) 範本。 CloudFormation 範本預設為產生。您也可以選取其他輸出格式：
  - AWS CDK 會產生用於程式設計基礎設施部署的 TypeScript 專案。
  - HashiCorp Terraform 會產生 HashiCorp 組態語言 (HCL) 範本來管理網路資源。
  - 登陸區域加速器 (LZA) 會為 LZA 網路組態產生 network-config.yaml 檔案。

> **Note**
>
> 當您透過登陸區域加速器 (LZA) 管道部署 時， AWS 轉換帳戶和 LZA 安裝必須位於相同的 AWS 組織。如果組織 IDs 不相符，部署將會失敗。

對於自我部署，請使用提供的連結下載包含產生範本的 zip 檔案。zip 資料夾包含 README.md 檔案，說明如何使用產生的範本。

若要驗證下載的檔案尚未損毀或遭到竄改，請產生和下載檢查總和，然後使用 `openssl dgst -sha256 -binary <file.zip> | base64`命令將其與本機產生的雜湊進行比較。

部署核准程序

為了確保網路變更符合組織的安全標準和架構需求，所有部署請求都會經過核准工作流程。您必須先取得明確核准，網路部署請求才會執行。當您提交部署請求時，它會透過 AWS 轉換核准索引標籤自動路由至授權核准者。核准者會驗證 CloudFormation 範本和網路組態，以確保符合安全標準和架構需求。每個提交都會觸發新的檢閱週期，而且只有在收到確認後才會繼續部署。如果核准者拒絕您的請求，請直接聯絡他們以討論必要的修改。 AWS Transform 會追蹤所有核准決策以進行稽核，並維護部署歷史記錄。

刪除部署的網路資源

如果您需要復原部署，您可以刪除 AWS 轉換部署的網路資源。您可以在部署完成後立即刪除資源。如果您在部署後修改已部署的網路資源，則無法自動刪除資源。

- AWS 轉換受管部署： AWS 轉換會移除部署期間建立的所有 CloudFormation 堆疊。此動作需要透過 AWS 轉換核准索引標籤進行核准。
- 自我部署：您必須透過 AWS 管理主控台或 CLI AWS 手動刪除部署的資源。

組態檔案擷取

如果您的來源環境使用 Cisco ACI、Palo Alto Networks 或 Fortinet FortiGate，您需要擷取組態檔案以提供給 AWS Transform。您可以使用這些檔案做為獨立來源檔案來產生網路基礎設施和安全群組，或搭配使用 RVTools 上傳來新增安全群組產生。在這兩種情況下，擷取程序都相同。

若要從防火牆和網路環境擷取組態檔案，請遵循下列程序。如需最新資訊，請參閱廠商文件。

Fortinet FortiGate

- 韌體版本必須是 v7.0 或更新版本。
- 您需要 `super_admin`或 全域層級`super_admin_readonly`的權限。
- 步驟：
  1. 透過 SSH 或內建 CLI 用戶端連線至防火牆
  2. 執行：`show | grep ""`(`| grep ""` 停用分頁）
  3. 從 `show`命令開始將所有輸出儲存至檔案

Palo Alto Networks

- 韌體版本必須為 10.1 或更新版本。
- 您需要 superadmin 角色。
- 透過 SSH 連線至防火牆、執行下列命令來停用分頁、設定輸出格式、進入組態模式，以及匯出組態和預先定義的物件。儲存輸出：

```
set cli pager off
set cli config-output-format set
configure
show              # Save as palo-conf.txt
show predefined   # Save as palo-default.txt
```

Cisco ACI

- 韌體版本必須為 6.0 或更新版本。
- 您需要具有所有權限的管理員角色，以及已設定的安全複製通訊協定 (SCP)、SSH 檔案傳輸通訊協定 (SFTP) 或檔案傳輸通訊協定 (FTP) 目的地。
- 步驟：
  1. 透過瀏覽器連線至應用程式政策基礎設施控制器 (APIC)
  2. 開啟管理員功能表，然後選擇組態轉返
  3. 在拍攝快照對話方塊中，選取遠端位置選項，然後選擇立即建立快照。
  4. 收到「傳輸成功」訊息後，連線至遠端位置伺服器並擷取最新的快照檔案 (.gz 檔案)

遷移伺服器

AWS Transform 會自動大規模將伺服器重新託管至 Amazon EC2。採用 AI 技術的代理程式會引導您完成每次遷移波動，從庫存驗證和複寫代理程式部署到測試和最終切換。 AWS Transform 可處理數百部伺服器的協同運作，同時維持對組態和核准決策的控制。在幕後， AWS Transform 使用 AWS Transform MGN (MGN) 進行資料複寫。如需 MGN 的詳細資訊，請參閱什麼是 AWS Transform MGN？ MGN 使用者指南中的 。

您可以從幾乎任何來源環境遷移伺服器，包括內部部署資料中心、其他雲端供應商或其他 AWS 區域。AWS Transform 支援在 VMware、Hyper-V、KVM 或其他虛擬化平台上執行的實體伺服器和虛擬伺服器。只要支援來源作業系統，來源基礎設施和 Hypervisor 就不重要。

伺服器遷移由波浪組織。每個波動代表一起遷移的一組伺服器。對於每個波動，代理程式會逐步引導您完成下列階段：

對於具有容器化遷移策略的波， AWS Transform 會執行原始程式碼容器化工作流程，而不是以下所述的重新託管步驟。容器化工作流程會引導您複製原始程式碼、產生 Docker 成品、發佈容器映像，以及部署至 Amazon Elastic Container Service 或 Amazon Elastic Kubernetes Service。如需完整的容器化工作流程，請參閱 原始程式碼容器化。

1. 先決條件和設定遷移預設值。設定目標帳戶並設定執行個體的啟動方式。 AWS Transform 提供智慧型預設值，讓您可以快速開始使用。
2. 步驟 1：設定遷移波。代理程式會設定您的目標帳戶、驗證許可，以及自動設定資源標記。
3. 步驟 2：驗證並確認庫存。遷移開始之前，請檢閱您的伺服器組態、執行個體類型建議和網路指派。

4. 步驟 3：部署複寫代理程式。代理程式可以在批次中在所有伺服器上部署代理程式，而不需要個別手動存取每個伺服器。
5. 步驟 4：資料複寫。持續區塊層級複寫可讓您的目標環境與來源伺服器同步，直到您準備好進行切換為止。
6. 步驟 5：測試。啟動測試執行個體來驗證遷移的伺服器，然後再進行最終切換。
7. 步驟 6：切換。以最短的停機時間完成遷移。代理程式會協調最終切換並驗證成功。

先決條件和設定遷移預設值

先決條件

如果您在 AWS 轉換中完成end-to-end遷移任務的所有步驟，您的目標帳戶、庫存檔案和網路基礎設施已經準備好。您可以繼續設定遷移預設值。

如果您獨立開始伺服器遷移，請確定您已備妥下列項目：

- 支援的作業系統 – 來源伺服器必須執行支援的作業系統。如需完整清單，請參閱 MGN 使用者指南中的支援的作業系統。
- 遷移的目標帳戶 – 您需要遷移伺服器的 AWS 帳戶 IDs。您可以使用 AWS 轉換登陸區域或任何其他工具來設定您的基礎設施。
- 網路基礎設施就地 – 部署和設定 VPCs、子網路和安全群組。您可以使用 AWS 轉換網路遷移或任何其他工具來設定您的網路基礎設施。
- 庫存檔案 – 準備伺服器詳細資訊、波動指派、目標帳戶資訊和 Amazon EC2 執行個體類型偏好設定。您可以使用 AWS 轉換遷移規劃來產生此檔案。

設定遷移預設值

AWS Transform 為您的遷移組態提供智慧型預設值，包括如何啟動 Amazon EC2 執行個體以及如何設定複寫。您可以接受這些預設值並立即開始遷移，或透過聊天界面或視覺化檢閱來自訂它們。預設值會套用至所有目標帳戶，並且可以在波動設定期間於波動層級覆寫。

Amazon EC2 建議偏好設定

AWS Transform 會分析來源伺服器使用率，並建議大小最佳的 Amazon EC2 執行個體，協助您避免從第一天開始過度佈建。您可以設定 Amazon EC2 建議偏好設定，以控制如何為遷移的伺服器選取執行個體類型。

如需產生 Amazon EC2 建議的詳細資訊，請參閱在 中產生 Amazon EC2 建議 AWS Migration Hub。

> **Note**
>
> 您可以修改建議的 Amazon EC2 執行個體類型，以包含來自遷移評估器、AWS 最佳化和授權評估 (OLA) 或 AWS 轉換評估任務的建議。

遷移初始化

AWS 轉換會在遷移開始之前，在您的目標帳戶中自動設定所需的遷移基礎設施。這包括為您 AWS 區域 計劃遷移的每個帳戶初始化 MGN，以及所有目標帳戶。在初始化過程中：

- 建立所需的 IAM 角色和政策。
- 已設定所需的預設範本。

如需初始化程序的資訊，請參閱 MGN 使用者指南中的AWS Transform MGN 使用 主控台初始化。

Amazon EC2 啟動範本

啟動設定包含兩個部分：一般啟動設定和 Amazon EC2 啟動範本，這會決定如何針對每個來源伺服器啟動測試或切換執行個體 AWS。

啟動設定，包括 Amazon EC2 啟動範本，可以在帳戶層級定義，然後在每次將來源伺服器新增至 AWS Transform MGN 時自動套用至每個來源伺服器。本節中定義的啟動設定預設值可自動套用至所有目標帳戶。

AWS 轉換會顯示可用的啟動範本設定清單。您可以選擇繼續使用預設值或設定啟動範本。如果您選擇設定， AWS Transform human-in-the-loop(HITL) 檢閱的連結，其中包含啟動範本設定的所有參數。您也可以直接透過聊天介面對您想要的任何參數進行修改。

使用帳戶啟動範本設定建立來源伺服器。使用這些預設設定建立來源伺服器後，您可以在來源伺服器啟動設定層級進行變更。您可以使用聊天介面變更任何參數上的來源伺服器設定，或在 期間使用庫存 Excel 檔案進行大量操作步驟 2：驗證並確認庫存。

若要檢閱啟動範本設定和詳細資訊的完整清單，請參閱 MGN 使用者指南中的啟動一般設定。

其他 Amazon EC2 啟動範本變更

對於其他 Amazon EC2 啟動範本變更，您應該在每個目標帳戶的範本 ID 上執行這些變更。此選項可在波動設定中使用。 AWS Transform 會引導您完成該設定，並提供適當的連結。

啟動後動作

啟動後動作會在 中以測試或切換執行個體的形式啟動後立即自動化在每個來源伺服器上執行的現代化和驗證任務 AWS。 AWS Transform Rehost 會採用 MGN 中可用的啟動後動作，並提供這些功能，讓代理程式可以代表您建議、設定和執行這些動作，做為遷移工作流程的一部分。動作是透過 AWS Systems Manager (Systems Manager) 執行，可以是 MGN 中可用的預先定義動作之一，也可以是從現有 Systems Manager 文件建立的自訂動作。

啟動後動作可以在帳戶層級定義，然後在每次將來源伺服器新增至 MGN 時自動套用至每個來源伺服器。本節中定義的啟動後動作預設值可自動套用至所有目標帳戶。

AWS 首先轉換會顯示目標帳戶中可用的啟動後動作清單。然後，它提供 來定義新的啟動後動作，並將其套用至您的目標帳戶遷移。 AWS Transform 也會根據作業系統和庫存的最佳實務提供 AI 支援的建議。您可以選擇繼續使用預設值或設定您自己的動作。

您也可以選擇已在 MGN 中定義的啟動後動作。提示客服人員顯示可用的預先定義啟動後動作清單。如需此清單的詳細資訊，請參閱 MGN 使用者指南中的預先定義啟動後動作。

建立新的啟動後動作

如果您選擇建立新的啟動後動作，代理程式會提示您提供 Systems Manager 文件名稱或 Systems Manager ARN，以使用 建置啟動後動作。Systems Manager 文件應事先透過 AWS Systems Manager 主控台建立。如需建立 Systems Manager 文件的詳細資訊，請參閱AWS Systems Manager 《使用者指南》中的建立 Systems Manager 文件。

然後，代理程式會產生human-in-the-loop(HITL) 界面，您可以在其中提供必要欄位：

- 啟動後動作名稱 – 代理程式會提供預設名稱，您可以變更此名稱。
- 啟動後動作順序 – 預設順序值為 1001，除非帳戶已定義啟動後動作，在這種情況下，新動作會放在執行順序的最後。您可以變更順序。如需啟動後動作順序的詳細資訊，請參閱 MGN 使用者指南中的啟動後設定。
- 必要的 Systems Manager 參數值 – 為 Systems Manager 文件所需的任何參數提供值。

您也可以直接透過聊天介面對您想要的任何參數進行修改。

使用 帳戶啟動後動作設定建立來源伺服器。使用這些預設設定建立來源伺服器後，您可以在來源伺服器層級變更它們。您可以使用聊天介面變更任何動作的來源伺服器設定，或在 期間使用庫存 Excel 檔案進行大量操作步驟 2：驗證並確認庫存。

庫存檔案中的啟動後動作

Rehost 代理程式會使用為每個來源伺服器定義的啟動後動作範本來擴展庫存檔案。這可讓客戶在託管至 MGN 匯入程序期間，更新或新增每個來源伺服器的啟動後動作。若要從來源伺服器刪除特定啟動後動作，請使用 active欄來指出 FALSE。庫存檔案中的啟動後動作使用以下命名慣例：

mgn:launch:post-actions:<ACTION_NAME>:<FIELD_NAME>

全域切換會控制啟動後動作是否執行：

mgn:launch:post-actions:enabled (TRUE/FALSE)

每個動作的欄位數

- ssmDocumentName （字串，必要） – 要執行的 Systems Manager 文件。
- order （整數，必要） – 執行順序；必須介於 1000 和 10000 之間。動作會以遞增順序執行 — 較低的值會先執行。
- active (TRUE/FALSE，選用） – 動作是否作用中。
- mustSucceedForCutover (TRUE/FALSE，選用） – 在切換之前，動作是否必須成功。
- timeoutSeconds （整數，選用） – 以秒為單位的逾時。
- description （字串，選用） – 人類可讀描述。
- parameters (JSON，選用） – Systems Manager 文件參數。

參數 JSON 結構

parameters 欄位以 JSON 結構提供：

```
{
  "parameters": {
    "Operation": [
      {"value": "Scan", "type": "String"}
    ]
  },
  "externalParameters": {
    "InstanceId": "ec2.InstanceId"
  }
}
```

- parameters – 將文件參數名稱映射至值參考清單 （每個項目都有 value和選用的 type，預設為 String)。

- `externalParameters` – 將文件參數名稱映射至動態路徑字串（不會建立 Systems Manager 參數）。

步驟 1：設定遷移波

在此階段， AWS Transform 會透過設定目標帳戶、驗證服務許可、設定資源標籤、將聯網資料新增至庫存，以及設定複寫和啟動設定來準備遷移波動。

遷移模式和帳戶組態

AWS 轉換支援兩種遷移模式：

- 單一帳戶遷移 – 波動中的所有伺服器都會遷移至連接器中設定的相同目標帳戶。
- 多帳戶遷移 – 伺服器遷移到庫存檔案中指定的不同目標帳戶。對於多帳戶遷移，您的庫存檔案必須包含具有每個伺服器目標帳戶 ID 的資料`mgn:account-id`欄。

AWS 轉換會確認目標帳戶組態，並驗證每個目標帳戶中是否初始化 MGN。如果 MGN 尚未初始化，AWS Transform 會提供完成初始化的指示。在初始化期間，MDN 會建立下列 IAM 服務角色，以進行複寫和啟動操作：

- `AWSApplicationMigrationReplicationServerRole`
- `AWSApplicationMigrationConversionServerRole`
- `AWSApplicationMigrationMGHRole`
- `AWSApplicationMigrationLaunchInstanceWithDrsRole`
- `AWSApplicationMigrationLaunchInstanceWithSsmRole`
- `AWSApplicationMigrationAgentRole`

若要進一步了解這些角色，請參閱《MDN 使用者指南》中的使用主控台初始化 MGN 或使用 API 初始化 MGN。

對於多帳戶遷移， AWS Transform 也會在初始化步驟期間建立下列角色：`AWSTransformRehostSharingRole_<management-or-delegated-admin-account-id>`。此角色會部署在所有遷移目標帳戶。

資源標記驗證

確認服務許可後， AWS Transform 會驗證所有必要的資源都已正確標記，以便代理程式成功操作遷移。如果有任何資源缺少必要的標籤， AWS Transform 會提供標記頁面的連結，您可以在其中套用缺少的標籤，然後再繼續。需要下列標籤：

- 現有的來源伺服器必須具有標籤 `CreatedBy: AWSTransform`和 `ATWorkspace: <workspace_id>`。如果您已在來源伺服器上開始複寫，並在 AWS Transform MGN 服務中建立它們，您需要標記這些伺服器，以便 AWS Transform 可以將它們與從內部部署環境發現的來源伺服器建立關聯，並避免不必要的建立重複來源伺服器。 AWS Transform 會使用使用者提供的 ID、FQDN 或主機名稱金鑰自動建立它們之間的關聯。
- 網路資源必須正確標記複寫（暫存區域）和啟動執行個體。 AWS Transform 會顯示目標帳戶中網路資源的完整清單，並指出每個資源是否已標記。您可以檢閱清單，然後選取您要新增的任何未標記資源。對於您選取的每個資源， AWS Transform 會套用相關標籤：
  - `CreatedBy: AWSTransform` 或 `CreatedFor: AWSTransform`，取決於資源類型。
  - `ATWorkspace: <workspace_id>` 會套用至所有選取的資源。

  AWS 轉換網路遷移代理程式建立的 VPCs 和子網路會自動加上標籤。
- 除了 VPCs和子網路之外， AWS Transform 也會顯示目標帳戶中所有現有的彈性網路界面 (ENIs)。如果您希望 AWS Transform 將它們用作執行個體啟動的一部分，則必須使用 `CreatedFor: AWSTransform`和 標記它們`ATWorkspace: <workspace_id>`。如需如何將 ENIs 附加或新增至 Amazon EC2 啟動範本的詳細資訊，請參閱 MGN 使用者指南中的詳細考量事項。

將網路資料新增至庫存

AWS 轉換會將網路資訊從網路遷移到庫存檔案。此步驟會根據遷移網路階段期間產生的網路組態，將您的伺服器映射至適當的目標子網路和安全群組。

複寫和啟動設定

複寫設定組態

複寫設定會決定如何從來源伺服器複寫資料 AWS。在將來源伺服器新增至 AWS Transform MGN 之前，請在複寫範本中設定複寫設定。 AWS 轉換會顯示所有複寫設定參數 — 您可以透過專用 HITL 或透過聊天介面進行設定。

如需複寫設定參數的詳細資訊，請參閱 MGN 使用者指南中的複寫設定範本。

啟動範本設定

啟動範本可讓您控制 AWS Transform MGN 在其中啟動執行個體的方式 AWS。範本中定義的預設組態會自動套用至每個新增的伺服器。您可以透過專用 HITL 或透過聊天介面來設定啟動範本設定。

如需啟動範本設定參數的詳細資訊，請參閱 MGN 使用者指南中的啟動範本。

AWS Transform 也提供與啟動範本相關聯的 Amazon EC2 啟動範本 ID 連結，可讓您變更其他 Amazon EC2 啟動範本屬性。若要編輯 Amazon EC2 啟動範本，請遵循 MGN 使用者指南中的啟動範本中的指示。

IP 指派策略

您可以選擇將 IP 地址指派給遷移伺服器的方式：

- 靜態 IP – 維護來源伺服器的 IP 地址。如果需要 CIDR 轉換， AWS 轉換會自動轉換 IP 地址以符合新的 CIDR。
- 動態 IP (DHCP) – 每個伺服器都會從子網路的 IP 集區指派新的 IP 地址。

> **Note**
>
> 如果您在網路遷移期間選取了 MAP 安全群組映射策略，則只有靜態 IP 指派可用。如需詳細資訊，請參閱安全群組映射。

步驟 2：驗證並確認庫存

在將伺服器資料載入 MGN 之前， AWS Transform 會準備庫存檔案供您檢閱。您可以下載 CSV 或 XLSX 格式的檔案、檢閱伺服器組態，並視需要進行變更。

清查檔案包含伺服器名稱、作業系統、Amazon EC2 執行個體類型建議、目標子網路、安全群組、IP 指派和授權選項等詳細資訊。必要欄位包括：

- 伺服器資訊 – 伺服器名稱、VMID 和來源規格。
- 波指派 – 遷移波分組。
- 應用程式分組 – 邏輯應用程式關聯。
- 目標組態 – 目標帳戶、區域和 Amazon EC2 執行個體類型。
- 網路組態 – 目標子網路和安全群組。

您可以修改 檔案來調整 Amazon EC2 組態、變更作業系統授權選項 (BYOL 或已包含授權），以及更新租用設定。

檢閱清查之後，您可以接受如下所示的清查，或上傳修改後的版本。 AWS Transform 接著會將資料載入 MGN，以為波動中的每個伺服器建立來源伺服器記錄。

> **Note**
>
> 請勿移除庫存檔案中的資料欄或變更資料欄標頭。 AWS 轉換需要原始檔案結構才能正確處理資料。

> **Note**
>
> AWS 轉換允許 AWS 區域 一次匯入一個指定目標 AWS 帳戶 和目標。如果您同時處理多個波動，或者有多個遷移任務使用相同的目標帳戶執行，則必須先等待匯入完成，才能在不同的波動或任務中執行另一個匯入。

您可以在庫存檔案欄 和 中指定組態，以控制作業系統授權選項 (BYOL 或已包含授權） `mgn:launch:placement:operating-system-licensing`和租用`mgn:launch:placement:tenancy`。如需詳細資訊，請參閱 MGN 使用者指南中的匯入參數。

步驟 3：部署複寫代理程式

若要開始從來源伺服器複寫資料到 AWS，您可以在每個來源伺服器上安裝 AWS 複寫代理程式。 AWS Transform 提供三種安裝方法：

- 組織工具 – 使用您組織的現有部署工具 （ 例如 SCCM、Ansible 或 Chef) 在您的伺服器上安裝代理程式。 AWS Transform 提供安裝命令，其中包含靜音安裝的其他參數，包括 `--no-prompt`、`--aws-access-key-id`、 `--aws-secret-access-key`和 `--aws-session-token`。
- MGN 連接器 – 使用 MGN 連接器自動安裝代理程式。連接器會透過 SSH (Linux) 或 WinRM (Windows) 連接到來源機器，並自動安裝複寫代理程式。設定完成後，即可跨多個波和不同目標重複使用連接器 AWS 帳戶。如需 MGN 連接器的詳細資訊，請參閱 MGN 使用者指南中的設定 MGN 連接器。

> **Note**
>
> 在搭配 AWS Transform 使用 MGN 連接器之前，您必須在 AWS Systems Manager Fleet Manager 中使用下列標籤來標記連接器的受管執行個體：
>
> - 金鑰：`CreatedFor`值： `AWSTransform`
> - 索引鍵：`ATWorkspace`值：*`Workspace-id`*
>
> 若要標記受管執行個體，請開啟 AWS Systems Manager 主控台，導覽至 Node Tools 下的 Fleet Manager，選擇 MGN 連接器的受管執行個體，然後套用上述標籤。在 AWS 轉換 Web 應用程式 URL 中尋找您的工作區 ID：`https://.../workspace/`*`workspace-id`*`/job/`*`job-id`*。

- 手動安裝 – 直接在每個來源伺服器上安裝代理程式。此方法需要直接存取每個伺服器，但可讓您完全控制安裝程序。

AWS 轉換 MGN 連接器設定

AWS 轉換 MGN 連接器可自動化跨來源伺服器的複寫代理程式部署，無需個別登入每個伺服器。連接器是部署在內部部署環境中專用 Linux 機器上的輕量型用戶端。它透過 SSH (Linux) 或 WinRM (Windows) 連接到來源伺服器，以安裝和設定複寫代理程式，無需在多個 AWS 服務之間手動協調。

連接器的運作方式

連接器透過下列元件運作：

- 連接器用戶端 – 在環境中的專用 Linux 機器上部署。
- SSM Agent – 安裝在相同的機器上，以啟用與 的安全通訊 AWS。
- SSM 混合啟用 – 將連接器機器連結至 AWS Systems Manager 以安全執行命令。
- 登入資料管理 – 從 AWS Secrets Manager 擷取來源伺服器登入資料。

部署代理程式時， AWS Transform 會將 SSM 文件傳送至連接器機器。連接器接著會從 AWS Secrets Manager 擷取來源伺服器憑證、建立與每個來源伺服器的連線、驗證來源伺服器是否符合先決條件、安裝和設定複寫代理程式，以及驗證成功安裝。

連接器機器需求

需求	詳細資訊
作業系統	支援的 Linux 作業系統。如需完整清單，請參閱 MGN 使用者指南中的 MGN 連接器先決條件。
網路存取	必須連接所有來源伺服器 (Linux over SSH、Windows over WinRM)
網際網路連線	傳出 HTTPS (443) 到 AWS 端點 (Systems Manager、Secrets Manager、GN)
磁碟空間	最少 200 MB 可用
許可	根或 sudo 存取

> **Note**
>
> 連接器必須安裝在 Linux 機器上，但可以將代理程式部署到 Linux 和 Windows 來源伺服器。

設定程序

AWS 轉換會引導您完成下列步驟來設定連接器：

步驟 1：連接器組態

為您的連接器提供名稱，或使用自動產生的預設名稱。連接器可以安裝在 MGN 的管理帳戶或委派管理員帳戶中。對於多帳戶遷移，連接器可以將代理程式部署到跨成員帳戶的伺服器。

步驟 2： AWS 資源設定

AWS 轉換會開啟使用 AWS 登入資料在瀏覽器中執行的設定頁面。您必須使用 AWS 管理帳戶或委派管理員帳戶登入 管理主控台。這必須是 AWS 轉換目標連接器所連線的相同帳戶。

設定頁面會自動建立下列資源：

- IAM 角色（以等冪方式建立 — 如果已存在，則略過）：

  - `AWSApplicationMigrationConnectorManagementRole` – 在代理程式安裝期間用來存取登入資料。
  - `AWSApplicationMigrationConnectorSharingRole_<ACCOUNT-ID>` – 包含代理程式安裝的許可。
- SSM 混合啟用 – 30 天的過期期間。將連接器機器 AWS 連結至 Systems Manager，並產生安全啟用憑證。

或者，您可以從設定頁面下載 CloudFormation 範本，自行部署 IAM 角色。

設定頁面會產生一行安裝命令，其中包含所有必要的登入資料和組態。

> **Important**
>
> 保持設定頁面開啟，直到安裝完成。關閉它需要重新啟動程序。所有登入資料僅存在於您的瀏覽器中，不會由 AWS Transform 存放。

步驟 3：連接器安裝

在您環境中的 Linux 機器上安裝連接器：

1. 從設定頁面複製安裝連結。
2. SSH 至您選擇的 Linux 機器。
3. 貼上並執行安裝命令。
4. 等待安裝完成（通常為 2-3 分鐘）。

步驟 4：連接來源伺服器

安裝後， AWS Transform 會識別屬於目前波動的所有來源伺服器，並自動將其連接至 MGN 連接器。

步驟 5：設定登入資料

為您的來源伺服器憑證提供 AWS Secrets Manager ARNs。 AWS Transform 提供三種登入資料組態選項：

- Linux 伺服器的單一秘密 – 包含所有 Linux 來源伺服器的 SSH 金鑰或使用者名稱/密碼的共用秘密。
- Windows 伺服器的單一秘密 – 一個包含所有 Windows 來源伺服器的使用者名稱和密碼的共用秘密。

- 每個伺服器多個秘密 – 每個伺服器或一組伺服器的不同秘密。當伺服器有不同的登入資料時，請使用此選項。 AWS 轉換會產生預先填入伺服器清單的 CSV 檔案。您填寫每個伺服器的 `secret_arn`欄，並上傳完成的檔案。

> **Note**
>
> 如果您的兩種伺服器類型各有一個共用秘密，則可以合併 Linux 和 Windows 單一秘密選項。每個伺服器秘密選項與單一秘密選項互斥。

登入資料秘密格式。若要進一步了解，請參閱 MGN 使用者指南中的 MGN 連接器憑證：

```
{
  "WinConnectionProtocol": "HTTPS",
  "WinUserName": "windows_username",
  "WinPassword": "windows_password",
  "LinuxUserName": "linux_username",
  "LinuxPrivateKey": "linux_private_key",
  "LinuxHostKeyValidation": false
}
```

代理程式部署

設定並驗證登入資料後， AWS Transform 會將複寫代理程式部署到您的來源伺服器。您可以部署到目前波動中的所有伺服器，或選取特定伺服器。

每個伺服器的部署程序：

1. AWS Transform 會透過 SSM 將部署命令傳送至連接器。
2. 連接器會從 AWS Secrets Manager 擷取登入資料。
3. 連接器會使用設定的登入資料連接到來源伺服器。
4. 連接器會驗證來源伺服器是否符合執行複寫代理程式所需的所有先決條件。
5. 連接器會安裝和設定複寫代理程式。
6. 連接器會驗證安裝和連線是否成功。

您可以使用每個伺服器狀態追蹤即時監控部署進度，包括目前的安裝步驟、經過時間和預估剩餘時間。如果任何伺服器失敗， AWS Transform 會顯示失敗原因，並提供每個伺服器的重試選項。成功部署的伺服器可以在重試失敗的伺服器時獨立繼續。

連接器重複使用和生命週期

部署後續波紋的代理程式時，您可以重複使用現有的連接器或建立新的連接器。 AWS 轉換會列出您帳戶中設定的所有連接器，顯示連接器名稱、狀態（作用中或已過期）、連接的伺服器計數和混合啟用過期日期。

- 作用中連接器 – 混合啟用仍然有效。 AWS Transform 會驗證新波的 IAM 角色，並繼續進行登入資料組態。不需要新的混合啟用。
- 連接器已過期 – SSM 混合啟用已過期。過期的啟用無法續約。您必須選取不同的連接器或建立新的連接器。

SSM 混合啟用會在 30 天後過期。只有在 Linux 機器上安裝連接器時，才需要啟用。安裝連接器後，即使啟用過期，您也可以繼續使用它在來源伺服器上安裝複寫代理程式。如果您需要在啟用過期後在新機器上安裝連接器，則需要透過設定程序建立新的連接器。

手動代理程式安裝

對於手動安裝，您會先產生 AWS 登入資料（暫時或永久），然後在每個來源伺服器上安裝代理程式。

登入資料選項：

- 臨時登入資料（建議）– 使用 AWSApplicationMigrationAgentInstallationPolicy受管政策建立 IAM 角色，然後使用 aws sts assume-role 產生臨時登入資料。若要進一步了解，請參閱 MGN 使用者指南中的客服人員安裝許可。
- 永久登入資料 – 使用 AWSApplicationMigrationAgentInstallationPolicy受管政策建立 IAM 使用者並產生存取金鑰。

安裝步驟：

對於 Linux 伺服器，請下載並執行安裝程式：

```
wget -O ./aws-replication-installer-init \
  https://aws-application-migration-service-region.s3.region.amazonaws.com/latest/
linux/aws-replication-installer-init
sudo chmod +x aws-replication-installer-init
sudo ./aws-replication-installer-init --region region --user-provided-id server-
identifier
```

對於 Windows 伺服器，請以管理員身分使用 PowerShell 下載並執行適當的安裝程式：

```
Invoke-WebRequest -Uri "https://aws-application-migration-
service-region.s3.region.amazonaws.com/latest/windows/
AwsReplicationWindowsInstaller.exe" `
  -OutFile "C:\AwsReplicationWindowsInstaller.exe"
C:\AwsReplicationWindowsInstaller.exe --region region --user-provided-id server-
identifier
```

> **Important**
>
> `--user-provided-id` 參數是必要參數。將`######`取代為庫存檔案中資料`mgn:server:user-provided-id`欄的確切值。此識別符會將實體伺服器連結至其 MGN 來源伺服器記錄。

如需代理程式安裝的詳細資訊，請參閱 MGN 使用者指南中的 Linux 代理程式和 Windows 代理程式。

安裝後， AWS Transform 會檢查伺服器是否顯示複寫狀態為 `INITIATING`或 ，藉此驗證所有代理程式是否成功連線`INITIAL_SYNC`。

> **Note**
>
> AWS 轉換不支援 MGN 無代理程式複寫。如需有關無代理程式複寫的資訊，請參閱 MGN 使用者指南中的無代理程式複寫概觀。

> **Note**
>
> 您必須在批次中的所有伺服器上安裝複寫代理程式。中斷連接並封存未安裝複寫代理程式的伺服器。您可以使用 `disconnect-from-service`命令來中斷連線伺服器，並使用 `mark-as-archived`命令來封存中斷連線的伺服器。封存命令僅適用於生命週期狀態為 的來源伺服器`DISCONNECTED`。

如需與複寫相關的配額，請參閱 MGN 使用者指南中的 MGN 服務配額限制。

步驟 4：資料複寫

安裝複寫代理程式後，資料複寫會自動開始。 AWS Transform 會使用連續區塊層級複寫，將資料從來源伺服器同步至 AWS。

複寫程序包含兩個階段：

- 初始同步 – 來源伺服器資料的完整副本 AWS。資料會以 Amazon Elastic Block Store (Amazon EBS) 快照或 Amazon FSx for NetApp ONTAP (FSx for ONTAP) 磁碟區儲存在目標帳戶中，視您設定的目標儲存類型而定。如需詳細資訊，請參閱 MGN 使用者指南中的目標儲存體類型。持續時間取決於資料磁碟區和網路頻寬。
- 持續複寫 – 持續同步變更的區塊，將對來源伺服器效能的影響降至最低。維護 up-to-date複本 AWS。

複寫伺服器是部署在預備區域子網路中的臨時 Amazon EC2 執行個體。它們會從來源伺服器接收複寫資料，並由 MGN 自動管理。若要進一步了解，請參閱 MGN 使用者指南中的複寫伺服器設定。

AWS 轉換會監控複寫進度並提供狀態更新，包括複寫狀態、複寫延遲 （來源和複寫資料之間的時間差異） 和頻寬使用量。

在複寫期間，每個伺服器都會進行下列狀態：

- 尚未就緒 – 伺服器正在進行初始同步程序，尚未準備好進行測試。
- 準備好進行測試 – 已成功新增伺服器，並已開始資料複寫。現在可以啟動測試或切換執行個體。

一旦波動中的所有伺服器都超過 `NOT_READY` 狀態，資料複寫階段即完成，您可以繼續測試。

您可以隨時控制個別伺服器的複寫或整個波動：

- 暫停複寫 – 暫時暫停特定伺服器的複寫或整個波動。
- 繼續複寫 – 繼續先前暫停的複寫。
- 停止複寫 – 永久停止複寫。停止的複寫可以重新啟動，但從初始同步開始。

步驟 5：測試

資料複寫完成後，您可以啟動測試執行個體，在執行最終切換之前驗證遷移的伺服器。若要進一步了解，請參閱 MGN 使用者指南中的啟動測試執行個體。 AWS Transform 支援兩個測試選項：

- 全波測試 – 啟動波中所有伺服器的測試執行個體。
- 選擇性測試 – 透過從庫存檔案中提供使用者提供的 IDs，為您選擇的特定伺服器啟動測試執行個體。

AWS 轉換會從複寫的資料啟動 Amazon EC2 執行個體，並提供執行個體 IDs，讓您可以連線至 並驗證測試執行個體。測試之後，您可以：

- 如果測試成功，請繼續切換。
- 啟動新的測試執行個體以重新測試。
- 終止測試執行個體，並在重新測試之前解決任何問題。

步驟 5b：將應用程式標記為準備好進行切換

測試完成後，您對結果感到滿意，請將您的應用程式標記為準備好進行切換。 AWS Transform 會檢閱每個應用程式的複寫狀態，並在允許您繼續之前解決任何複寫提醒。只有具有乾淨複寫狀態的應用程式才能標記為切換。

步驟 6：切換

切換是將生產工作負載移至其中的最終遷移步驟 AWS。若要進一步了解，請參閱 MGN 使用者指南中的啟動切換執行個體。與測試類似， AWS Transform 支援特定伺服器的全波切換或選擇性切換。

在切換期間， AWS Transform 會從最新的複寫資料啟動 Amazon EC2 執行個體，並提供每個伺服器的執行個體 IDs。驗證切換執行個體之後，您會完成切換，這會停止持續的來源機器複寫。

切換程序包括下列步驟：

1. 啟動切換執行個體 – AWS 轉換會啟動所選伺服器的 Amazon EC2 執行個體。您可以選擇全波切換或選擇性切換。
2. 驗證切換執行個體 – 連線至啟動的執行個體，並驗證它們是否正常運作。
3. 完成切換 – 確認切換以停止來源機器複寫。您可以完成波動中的所有伺服器，或選取特定伺服器。完成會停止複寫代理程式傳送資料、從來源伺服器移除複寫代理程式，以及鎖定伺服器生命週期狀態。此動作無法輕鬆復原。若要進一步了解，請參閱 MGN 使用者指南中的完成切換。
4. 封存來源伺服器 （選用） – 完成之後，您可以將來源伺服器標記為已封存，以釋放帳戶中的來源伺服器配額。

> **Important**
>
> 完成切換會停止持續的來源機器複寫。在最終確定之前，請確定您已驗證您的切換執行個體。

> **Note**
>
> 在來源關閉和切換執行個體可用性之間發生停機。相應地規劃您的切換時段。

伺服器生命週期狀態

在遷移期間，每個伺服器都會進行下列生命週期狀態。若要進一步了解，請參閱 MGN 使用者指南中的來源伺服器生命週期。

- 未就緒 – 伺服器正在進行初始同步程序，尚未準備好進行測試。
- 準備好進行測試 – 資料複寫已開始，可以啟動測試或切換執行個體。
- 測試進行中 – 測試執行個體目前正在啟動。
- 準備好進行切換 – 伺服器已經過測試，已準備好進行切換。
- 切換進行中 – 目前正在啟動切換執行個體。
- 切換完成 – 伺服器已切換。所有資料都已遷移至 AWS 切換執行個體。
- 已中斷連線 – 伺服器已從 MGN 中斷連線。

您可以在遷移期間隨時詢問 AWS 轉換伺服器的狀態。 AWS Transform 提供互動式波狀狀態表，顯示所有相關伺服器資訊，包括遷移生命週期、複寫狀態和建議的後續步驟。您也可以使用自然語言來詢問 ，例如：

- 我的伺服器的狀態為何？
- 我的波浪狀態如何？
- 我目前處於哪個步驟的狀態？

在波動遷移期間，您可以要求 AWS 轉換更新或變更個別伺服器的狀態。例如，如果 Wave 中的 10 部伺服器中有 9 部通過測試階段，但其中一部失敗，您可以允許 AWS Transform 繼續將 9 部伺服器移至下一個階段，同時在失敗的伺服器上重新執行測試。

部署核准

AWS 轉換包含內建的核准工作流程，以確保生產變更通過組織的審核程序。當 操作需要核准時，AWS Transform 會透過核准索引標籤將請求路由至授權核准者。只有在 AWS 轉換中具有管理員角色的使用者才能核准部署請求。部署只有在收到確認後才會繼續。

版本備註

下列版本備註涵蓋 的最新變更遷移 （包括 VMware)。如需完整 AWS 轉換服務的變更清單，請參閱變更日誌。如需支援的 AWS 轉換區域，請參閱支援的 區域。如需支援的目標區域，請參閱帳戶連接器設定頁面。

2026 年 8 月

- AWS 遷移的轉換現在可識別從內部部署環境遷移的未使用傳入防火牆規則，並建議將其移除作為引導式網路建議的一部分。這可協助您避免轉發不再提供目的的安全暴露，例如開放傳入存取。移除僅限於未使用的輸入規則。進一步了解引導式網路建議。

2026 年 7 月

- AWS 遷移的轉換現在支援從幾乎任何來源遷移虛擬和裸機伺服器環境，包括 VMware、Hyper-V 和其他平台。無論您的來源基礎設施為何，都可以使用遷移功能，包括探索、遷移規劃、登陸區域建立、網路遷移和伺服器重新託管。Web 應用程式工作流程已從「VMware Migrations」重新命名為「Migrations （包括 VMware)」。進一步了解遷移。
- AWS 現在轉換可讓您產生工作區摘要報告做為可下載的 PDF。報告會合併工作區中所有遷移任務的資料，包括任務狀態、工作流程步驟進度、波動規劃、網路遷移、登陸區域組態、重新託管進度和產生的成品。進一步了解工作區摘要報告。
- AWS 轉換探索工具現在會直接從 VMware、Hyper-V 和裸機伺服器的資料庫收集詳細的 Oracle 中繼資料。您可以透過直接 SQL 連線探索 Oracle 執行個體。此工具會收集容器資料庫/可插入資料庫 (CDB/PDB) 列舉、元件庫存和資料檔案大小。進一步了解 Oracle 資料庫探索。
- AWS 遷移的轉換現在提供啟動後動作的增強功能。您現在可以在帳戶層級定義啟動後動作，並自動將其套用至所有來源伺服器，或在庫存驗證期間為每個來源伺服器自訂這些動作。啟動後動作會在做為測試或切換執行個體啟動之後，立即自動化每個來源伺服器的現代化和驗證任務。進一步了解啟動後動作。

2026 年 6 月

- AWS 遷移的轉換現在支援當地語系化。您可以在使用遷移工作流程時變更 Web 應用程式的顯示語言。進一步了解語言設定。
- AWS 現在轉換可讓您為遷移設定複寫設定和啟動設定。您可以根據目標帳戶或跨特定來源伺服器設定組態。進一步了解複寫和啟動設定。
- AWS 立即轉換可讓您將現有的彈性網路界面 (ENIs) 連接至啟動範本。您可以在目標帳戶中標記 ENIs，以便在執行個體啟動時使用。進一步了解網路資源標記。
- AWS 遷移的轉換現在支援所有 AWS 商業區域作為遷移目標，中東 （巴林） 和中東 （阿拉伯聯合大公國） 除外。進一步了解支援的目標區域。
- 您現在可以使用 AWS Transform 探索工具作為網路遷移的來源，並搭配 modelizeIT，為同時執行 VMware 和非 VMware 工作負載的環境啟用混合網路遷移。進一步了解網路遷移輸入來源。

2026 年 5 月

- AWS 轉換現在會在網路遷移檢閱期間偵測目標帳戶中VPCs。您可以在映射VPCs 旁查看現有的 VPCs、識別 CIDR 衝突，並在部署之前解決它們。進一步了解現有的 VPC 偵測。
- AWS 轉換支援在遷移至 期間將原始程式碼儲存庫轉換至容器 AWS。進一步了解容器化。
- AWS 轉換現在可以分析您探索到的庫存，並為每個伺服器和應用程式提供遷移策略建議。建議遵循業界標準的七種遷移策略 (7R)。每個建議都包含建議 AWS 的目標服務、可信度分數，以及背後的推理。進一步了解 7Rs 建議。

2026 年 4 月

- 直接在遷移工作流程中新增了登陸區域建立。 AWS 轉換現有基礎的檢查、建議組織單位 (OU) 結構和目標帳戶，並提供自動化部署或基礎設施即程式碼 (IaC) 輸出 (CloudFormation AWS CDK、 或登陸區域加速器 (LZA) 格式）。進一步了解登陸區域建立。
- 在網路遷移期間新增對具有安全群組映射的 DHCP 的支援。進一步了解安全群組建立。
- 您現在可以在遷移規劃期間產生互動式圖表和分析報告。圖表類型包括網路拓撲貼圖、應用程式相依性圖表、波浪 Gantt 圖表和一般圖表。報告類型包括風險評估、7Rs 建議和自訂分析報告。輸出提供互動式 HTML、PDF 或 Microsoft PowerPoint (.pptx) 檔案。進一步了解遷移規劃圖表和報告。

2026 年 3 月

- 新增用於網路遷移的公APIs，讓合作夥伴和程式設計存取網路遷移功能。請參閱網路遷移 API 參考。

2026 年 2 月

- 網路遷移現在支援擷取防火牆或軟體定義的網路 (SDN) 組態檔案，而不需要 RVTools 探索資料。您可以獨立使用防火牆或 SDN 組態檔案，或與 RVTools 匯出結合。

2026 年 1 月

- 新增對 Migration Acceleration Program (MAP) 標記和網路遷移元素的使用者定義標記的支援，可讓您追蹤遷移資源以用於 MAP 點數和組織目的。

2025 年 12 月

- 新增了重新設計工作流程和改善可用性的新遷移體驗。如需詳細資訊，請參閱加速 VMware 遷移：AWS Transform 的新體驗。
- 新增了自動登陸區域設定的登陸區域加速器 (LZA) 網路組態。
- 新增對遷移執行中多個目標 AWS 帳戶的支援，讓您能夠跨帳戶遷移工作負載。
- 新增 Cisco ACI、Palo Alto、FortiGate 和 ModelizeIT 來源格式的網路遷移支援。

2025 年 10 月

- 新增亞太區域 （ 大阪 ），將遷移執行擴展至 16 個目標區域。

2025 年 9 月

- 新增對重新託管波中的授權組態的支援，可讓您指定每波自攜授權 (BYOL) 或包含授權的選項。
- 新增對網路遷移中 Terraform 的支援，可讓您使用 Terraform 範本部署網路基礎設施。
- 新增更新複寫子網路組態的支援，移除目標帳戶中預設 VPC 的需求。

2025 年 8 月

- 透過新增美國東部（俄亥俄）、歐洲（斯德哥爾摩）和歐洲（愛爾蘭），將遷移執行（網路遷移和重新託管）擴展至 15 個目標區域。
- 新增了靈活的網路遷移 CIDR 範圍功能，可讓您在網路部署期間自訂 IP 地址範圍。

2025 年 5 月

- 啟動 的初始服務遷移（包括 VMware)，提供end-to-end遷移功能，包括探索、評估、遷移規劃、網路遷移和伺服器重新託管。
- 在 12 個目標區域中支援的遷移執行：美國東部（維吉尼亞北部）、美國西部（奧勒岡）、加拿大（中部）、南美洲（聖保羅）、歐洲（法蘭克福）、歐洲（倫敦）、歐洲（巴黎）、亞太區域（孟買）、亞太區域（首爾）、亞太區域（東京）、亞太區域（新加坡）和亞太區域（雪梨）。

原始程式碼容器化

AWS 轉換支援在遷移至 期間將應用程式轉換至容器 AWS。本章說明 AWS Transform 的代理式 AI 功能，以自動化原始程式碼的容器化。您可以平行遷移和現代化，減少從內部部署遷移到雲端原生架構的時間和複雜性。您可以從 GitHub、Bitbucket、GitLab 或 .zip 檔案容器化原始碼、產生 Docker 映像、發佈至 Amazon Elastic Container Registry (Amazon ECR)，以及部署至 Amazon Elastic Container Service (Amazon ECS) 或 Amazon Elastic Kubernetes Service (Amazon EKS)。這將容器化帶入您用來規劃和執行重新託管遷移的相同工作流程。

功能和主要功能

AWS Transform 提供下列將應用程式容器化的功能。

- AI 驅動的原始程式碼分析。分析您的應用程式原始碼，並自動產生 Docker 成品，包括 Dockerfile 和相關的組態檔案。不需要 Docker 專業知識。
- 容器映像建置和發佈。自動建置和測試容器映像，並透過自動漏洞掃描將其發佈至 Amazon Elastic Container Registry。
- 基礎設施即程式碼產生。透過自動驗證和安全性掃描，為 Amazon Elastic Kubernetes Service (Helm Charts) 或 Amazon Elastic Container Service (Terraform 模組） 產生生產就緒部署基礎設施。不需要從頭開始寫入 IaC。
- 私有相依性支援。您可以選擇將 AWS CodeArtifact 儲存庫 (Maven、PyPI、npm) 和私有 Amazon ECR 基礎映像設定為建置的相依性來源。
- 反覆測試和切換部署。部署測試基礎設施以進行驗證，然後部署最終基礎設施以進行生產切換。

> **Note**
>
> 原始程式碼容器化是專為尚未容器化的應用程式所設計。它需要存取您的應用程式原始碼，且不支援遷移現有的容器化工作負載。若要將現有容器遷移至 AWS，請使用 Amazon Elastic Container Service 或 Amazon Elastic Kubernetes Service 的標準部署方法。

容器化的運作方式

AWS 轉換使用 AI 支援的代理程式，在聊天式工作流程中引導您完成容器化程序。代理程式會處理從程式碼分析到已部署容器的整個程序，將手動 Dockerfile 撰寫和基礎設施設定天數縮短為數小時。

AWS Transform 會協調特殊任務，例如原始程式碼分析、Docker 映像產生和基礎設施建立。在工作流程的關鍵點，您可以在繼續之前檢閱和核准輸出。

您可以透過建立遷移任務來存取原始程式碼容器化。在任務中，您可以將容器化作為獨立工作流程執行，或在將波的遷移策略設定為容器化時作為end-to-end遷移的一部分執行。如需詳細資訊，請參閱遷移（包括 VMware)。

先決條件

開始之前，請務必備妥下列項目：

- AWS 轉換工作區。如需取得工作區的相關資訊，請參閱入門。
- 您可以透過 AWS CodeConnections 存取的 Git 儲存庫中的應用程式原始碼，或封裝為 zip 檔案以進行上傳。個別檔案不得超過 1 GB，且所有原始碼的總大小不得超過 8 GB。
- （選用）用於發佈容器映像的 Amazon ECR 儲存庫。當您準備好發佈時，可以在工作流程中稍後設定 Amazon ECR 存取。
- 對於 Amazon EKS 部署：現有的 Amazon EKS 叢集，或建立所需基礎設施的許可。
- 對於 Amazon ECS 部署：使用 Terraform 或 建立 Amazon ECS 叢集 AWS CloudFormation、服務和相關資源的許可 AWS Cloud Development Kit (AWS CDK)。

容器化工作流程

容器化工作流程包含下列步驟。 AWS 轉換代理程式會引導您完成聊天界面中的每個步驟。

1. the section called “步驟 1：安全免責聲明”。 檢閱並接受安全性免責聲明。
2. the section called “步驟 2：複製原始程式碼”。 提供您的應用程式原始碼。
3. the section called “步驟 3：容器化”。 AI 代理器會分析您的程式碼並產生 Docker 成品。
4. the section called “步驟 4：檢閱成品”。 檢閱產生的成品並核准程式碼變更。
5. the section called “步驟 5：發佈映像”。 將容器映像發佈至 Amazon ECR。
6. the section called “步驟 6：產生 IaC”。 產生 Amazon EKS 或 Amazon ECS 部署範本。
7. the section called “步驟 7：部署測試基礎設施”。 部署和驗證測試基礎設施。
8. the section called “步驟 8：清除測試基礎設施”。 向下傾斜測試資源。
9. the section called “步驟 9：部署切換基礎設施”。 部署生產基礎設施。

啟動容器化任務

若要容器化應用程式，您必須先在 AWS 轉換工作區中建立 VMware 遷移任務。在任務中，您可以選擇執行獨立容器化工作流程或包含容器化的end-to-end遷移流程。

- 獨立容器化 — 在不執行完整 VMware 遷移的情況下容器化原始程式碼。當您想要獨立於任何基礎設施遷移容器化應用程式時，請選擇此選項。
- 使用容器化End-to-end遷移 — 使用指派給一或多個波的容器化遷移策略來執行完整的 VMware 遷移工作流程。容器化工作流程會做為這些波遷移的一部分執行。如需 VMware 遷移的詳細資訊，請參閱 遷移（包括 VMware)。

啟動容器化任務

1. 在工作區登陸頁面上，選擇建立任務。
2. 選擇 VMware 遷移。
3. 選擇是否執行獨立容器化工作流程或包含容器化的end-to-end遷移流程。
4. AWS 轉換會引導您完成工作流程步驟，從 開始the section called “步驟 1：安全免責聲明”。

容器化許可

在容器化工作流程期間， AWS Transform 會將 IAM 角色部署到 AWS 帳戶 ，以使用 建置容器映像和部署基礎設施。在工作流程繼續之前，系統會要求您檢閱並核准此角色的建立。

角色名為 `AWSTransformCodeBuildExecutionRole`，並透過 AWS CloudFormation 堆疊部署。它包含下列 受管政策。

基本政策

提供容器化工作流程的核心許可：

- Amazon S3 — 在`aws-transform-*`儲存貯體中讀取和寫入物件
- Amazon ECR — 驗證、提取映像（以 標記`Project: atx-migration`)，並將映像推送至以 標記的儲存庫 `CreatedBy: AWSTransform`
- AWS CodeArtifact – 從標記 的儲存庫讀取`Project: atx-migration`、列出儲存庫、取得授權字符，以及讀取儲存庫端點。這些許可支援在工作流程期間設定的公有相依性解析和私有相依性來源
- Amazon CloudWatch Logs — 建立日誌群組和串流，並為 和 Amazon ECS 日誌群組寫入日誌事件

- AWS KMS — 描述和解密金鑰（範圍限定為 Amazon S3 透過服務條件）
- Amazon EC2 — 為啟用 VPC 的專案建立和管理網路介面
- AWS CodeConnections — 使用連線透過設定的 CodeConnections ARN 存取來源碼儲存庫

網路政策

管理已部署應用程式的聯網資源：

- Elastic Load Balancing — 建立、描述和管理負載平衡器、目標群組、接聽程式和規則（以 標記`CreatedBy: AWSTransform`）
- Route 53 — 建立和管理託管區域和 DNS 記錄
- AWS Cloud Map — 建立和管理用於服務探索的命名空間和服務（使用 標記`CreatedBy: AWSTransform`）

儲存政策

管理已部署應用程式的儲存資源：

- Amazon S3 — 建立和管理儲存貯體，包括加密、版本控制、生命週期和存取政策
- Amazon EFS — 建立和管理檔案系統、掛載目標和存取點（使用 標記`CreatedBy: AWSTransform`）
- Amazon EBS — 建立和管理磁碟區和快照（以 標記`CreatedBy: AWSTransform`）

AWS KMS 政策

管理加密金鑰操作：

- 描述金鑰、列出別名和讀取金鑰政策
- 加密、解密和產生資料金鑰（範圍限定為 Amazon CloudWatch Logs、Amazon EFS、Amazon EC2 和 Amazon S3 透過服務條件）

Amazon ECS 政策

管理容器部署的 Amazon Elastic Container Service 資源：

- 建立和管理叢集、服務和任務定義 （ 以 標記CreatedBy: AWSTransform)
- 註冊和取消註冊任務定義、執行任務
- 將 IAM 角色傳遞至 Amazon ECS 任務和服務
- 讀取 IAM 角色資訊和 ACM 憑證
- 描述 Amazon EC2 VPCs、子網路、安全群組和網路介面

Amazon EKS 政策

管理 Kubernetes 部署的 Amazon Elastic Kubernetes Service 資源：

- 存取 Kubernetes API、描述叢集和列出附加元件
- 將 IAM 角色傳遞至 Amazon EKS

> **Note**
>
> 所有許可都限定在您的 AWS 帳戶 和 範圍內 AWS 區域。由 AWS Transform 建立的資源會加上 標籤CreatedBy: AWSTransform，且寫入操作僅限於具有此標籤的資源，如適用。

步驟 1：檢閱安全性免責聲明

在容器化工作流程開始之前， AWS Transform 會顯示您必須檢閱並接受的安全性免責聲明。

免責聲明涵蓋的內容

容器化程序需要網際網路存取才能下載應用程式相依性 （ 例如來自公有登錄檔的套件，例如 npm、PyPI 或 Maven Central)。安全免責聲明會通知您：

- 建置環境將具有傳出網際網路存取權，以解析和下載應用程式建置組態中指定的相依性。
- 您有責任檢閱應用程式所需的相依性，並確保它們符合您組織的安全政策。
- 您可以選擇性地在後續步驟中設定私有相依性來源 （ 例如 AWS CodeArtifact 儲存庫或私有 Amazon ECR 基礎映像 ），以避免從公有登錄檔下載。

您需要執行的事項

檢閱並接受安全性免責聲明

1. 閱讀 AWS Transform 顯示的安全性免責聲明。
2. 接受免責聲明以繼續容器化工作流程。

接受免責聲明之後， AWS Transform 會繼續進行下一個提供原始碼的步驟。

> **Note**
>
> 不再需要預先使用 AWS CodeConnections 和 Amazon ECR 的連接器組態。 AWS Transform 會提示您稍後在工作流程中設定對這些服務的存取，但僅限於需要時。例如，當您選擇從 Git 儲存庫複製時設定 CodeConnections，並在準備好發佈容器映像時設定 Amazon ECR 存取。

步驟 2：複製原始程式碼

在此步驟中，您會提供要 AWS 轉換的應用程式原始碼。您可以從 Git 儲存庫或上傳 zip 檔案提供原始碼。

選項 1：Git 儲存庫

您可以從 Git 儲存庫提供原始程式碼。如果您尚未設定 AWS CodeConnections， AWS Transform 會在此時提示您提供 CodeConnections ARN。您有兩種方式可以指定儲存庫：

- 上傳 CSV 檔案 — 準備具有資料欄 `repo_name`和 的 CSV 檔案`branch`。`repo_name` 必須為 `owner/repo-name` 格式。資料`branch`欄是選用的；請保留空白，以使用儲存庫的預設分支。範例：

```
repo_name,branch
owner/my-app,main
owner/api-service,develop
owner/another-repo,
```

- 在聊天中提供儲存庫詳細資訊 - 直接在聊天中告知 AWS 轉換儲存庫名稱 (s) 和分支 (s)，而不是上傳 CSV。

AWS 轉換會驗證每個儲存庫是否存在，並可透過 CodeConnections 組態存取，然後複製儲存庫。

> **Note**
>
> 個別檔案不得超過 1 GB，且所有儲存庫的總大小不得超過 8 GB。 AWS Transform 會同時複製多個儲存庫以加快處理速度。

> **Important**
>
> Git 複製選項不支援跨多個儲存庫的應用程式。如果您的應用程式需要來自多個儲存庫的原始碼，請將它們封裝為 zip 檔案，並改用 zip 上傳選項。

選項 2：Zip 檔案上傳

如果您未設定 CodeConnections，或偏好直接上傳原始碼，您可以上傳 zip 檔案。

將原始碼上傳為 zip 檔案

1. 出現提示時，為每個應用程式上傳一個 zip 檔案。您可以將檔案拖曳至聊天，或使用附件按鈕。
2. 每個 zip 檔案都應包含一個應用程式的原始程式碼。
3. 個別檔案不得超過 1 GB，且所有上傳的總大小不得超過 8 GB。

選用：設定私有相依性

如果您的應用程式依賴來自私有登錄檔的套件，您可以在此步驟期間設定私有相依性來源。 AWS Transform 支援下列私有相依性類型：

- AWS CodeArtifact 儲存庫 — 設定在 AWS CodeArtifact 中託管的 Maven、PyPI 或 npm 儲存庫。 AWS 轉換會顯示帳戶中的可用儲存庫清單，供您選擇。
- 私有 Amazon ECR 基礎映像 — 如果您的 Dockerfiles 使用私有 Amazon ECR 儲存庫的基礎映像，請提供儲存庫詳細資訊，以便建置環境可以提取這些映像。

當您設定私有相依性時， AWS Transform 會提示您連線到託管這些資源 AWS 帳戶 的 。只有在您使用私有相依性時，才需要此連接器組態。

確認容器化偏好設定

原始碼可用後， AWS Transform 會詢問您是否擁有容器化應如何完成的特定指示。您可以選擇性地指定：

- 是否要產生新的 Dockerfile 或重複使用現有的 Dockerfile。
- 是處理單一儲存庫中的特定服務，還是處理所有服務。
- 容器化程序的任何其他偏好設定。

預設值為：

1. 使用 Amazon Linux 2023 基礎映像 (`public.ecr.aws/amazonlinux/amazonlinux:latest`)。
2. 處理儲存庫中的所有應用程式。
3. 如果有的話，請重複使用現有的 Dockerfile，並視需要進行細微修改。

您可以確認 以繼續預設值，或提供特定指示。

步驟 3：容器化

在此步驟中， AWS Transform AI 代理程式會分析您的應用程式原始碼並產生 Docker 成品。 AWS Transform 會檢查應用程式的結構、相依性和執行時間需求，以產生適當的 Dockerfile 和相關的組態檔案。

容器化期間會發生什麼情況

容器化代理程式會執行下列任務：

1. 原始程式碼分析： AWS Transform 會檢查應用程式的專案檔案、相依性、建置組態和執行時間需求。 AWS 轉換也會取代硬式編碼值 （例如資料庫 IP 地址或 DNS 名稱）、識別環境變數、偵測磁碟區，以及嘗試將日誌重新導向至標準輸出。
2. Dockerfile 產生 — 根據分析， AWS Transform 會產生專為您的應用程式量身打造的 Dockerfile。
3. 容器映像建置和測試 — AWS 轉換會建置容器映像並執行測試，以驗證 Dockerfile 是否產生運作中的映像。如果建置失敗， AWS 轉換會自動在 Dockerfile 上反覆運算。
4. 安全性分析： AWS Transform 會掃描產生的成品是否有硬式編碼值，例如登入資料、API 金鑰或其他敏感資料，並標記任何問題清單供您檢閱。

如果您提供多個儲存庫或具有多個服務的單一儲存庫，則 會平行處理每個服務。

支援的應用程式類型

AWS 轉換支援容器化下列應用程式類型：

- .NET 7 和更新版本 — 針對在 7 版或更新版本上執行的 .NET 應用程式最佳化容器化。
- 一般應用程式 — 使用任何語言或架構建置的應用程式容器化，包括 Java、Python、Node.js、Go 等。
- 不支援的應用程式 — 不支援 Windows、Xcode 或任何專屬建置環境。

您需要執行的事項

此步驟會自動執行。 AWS Transform 會在分析和容器化每個應用程式時顯示進度更新。如果 AWS 轉換遇到問題，可能會要求您釐清或提供其他資訊。

容器化完成時， AWS Transform 會移至檢閱產生的成品的下一個步驟。輸出會儲存在成品存放區中。

步驟 4：檢閱 Docker 成品和程式碼變更

在此步驟中，您將檢閱容器化期間所產生 AWS 轉換的 Docker 成品和程式碼變更。

檢閱 Git 儲存庫的變更

如果您從 Git 儲存庫提供原始碼， AWS Transform 會將容器化變更遞交到每個儲存庫中的新分支。如果您有多個儲存庫， AWS Transform 會將所有變更顯示為批次以供合併檢閱。

檢閱和核准變更

1. 檢閱 AWS Transform 提供的程式碼差異連結。每個 diff 會顯示已新增或修改的所有檔案，包括 Dockerfiles、組態檔案和任何原始程式碼變更。
2. 當 AWS 轉換顯示核准對話方塊時，核准或拒絕變更。對於多個儲存庫，您可以核准單一批次操作中的所有變更。
3. 如果您核准， AWS Transform 會將變更推送到儲存庫中的新分支。
4. 確認您已準備好繼續進行下一個步驟。

檢閱 zip 上傳的變更

如果您上傳原始程式碼做為 zip 檔案， AWS Transform 會提供容器化成品的下載連結。下載並檢閱成品，其中包括產生的 Dockerfile 和任何原始程式碼修改。

請求變更

如果產生的成品需要修改，您可以提供 AWS 轉換的意見回饋，以更新的指示重新啟動容器化步驟，並產生新的成品供您檢閱。

步驟 5：發佈映像

在此步驟中， AWS Transform 會將您的容器映像發佈至 Amazon Elastic Container Registry。如果您尚未設定 Amazon ECR 存取， AWS Transform 會在此時提示您提供 Amazon ECR 儲存庫的詳細資訊。

發佈期間會發生什麼情況

AWS 轉換會為每個容器映像執行下列任務：

1. 連接器組態 — 如果您尚未設定 Amazon ECR 存取， AWS Transform 會顯示連接器表單，您可以在其中提供 Amazon ECR 儲存庫 ARN 並連線至您的 AWS 帳戶。
2. 核准請求 — AWS 轉換會顯示要發佈的映像清單，並請求您的核准。您可以核准或拒絕發佈操作。
3. 映像推送 — 核准後， AWS Transform 會使用 將容器映像發佈到您的 Amazon ECR 儲存庫。如果您有多個 服務， AWS Transform 會在單一批次操作中發佈所有映像。
4. 漏洞掃描 — Amazon ECR 會自動掃描發佈的映像是否有已知漏洞。 AWS 轉換會報告掃描結果。如需更全面的分析，請啟用 AWS ECR 增強型掃描和 AWS GuardDuty 執行期監控。

> **Note**
>
> 影像發佈會使用 以非同步方式執行。如果您的工作階段在發佈期間中斷， AWS Transform 會在您重新連線時自動復原操作。

您需要執行的事項

- 檢閱要發佈的映像清單。

- 核准或拒絕發佈操作。如果您拒絕， AWS Transform 會略過影像發佈，而且您可以繼續進行下一個步驟，而無需發佈影像。
- 在發佈完成後檢閱漏洞掃描結果。

發佈之後， AWS Transform 會提供用於基礎設施部署步驟的映像 URIs。

步驟 6：產生基礎設施做為程式碼

在此步驟中， AWS Transform 會產生部署容器化應用程式的 AWS 基礎設施範本。您可以選擇 Amazon Elastic Kubernetes Service 和 Amazon Elastic Container Service 作為目標平台。

Amazon Elastic Kubernetes Service (Kubernetes)

如果您選擇 Amazon EKS， AWS Transform 會為您的應用程式產生具有 Kubernetes 資訊清單的 Helm Chart。產生的範本包括：

- 部署和服務
- 傳入規則
- ConfigMaps 和 SecretProviderClass 資源
- 服務帳戶
- 持久性磁碟區宣告 (EBS 和 EFS)
- Route 53 DNS 記錄
- 運作狀態檢查組態

選用：CloudWatch 記錄

AWS 轉換會詢問您是否要為 Amazon EKS 部署包含 CloudWatch 記錄。如果您選擇加入， AWS Transform 會產生 Fluent Bit DaemonSet 組態，收集 Pod 日誌並將其傳送至 CloudWatch Logs。

如果您選擇 CloudWatch 記錄，您的叢集管理員必須在部署之前完成下列先決條件：

1. 在叢集中建立`amazon-cloudwatch`命名空間。
2. 使用 CloudWatch Logs 寫入許可為 Fluent Bit 服務帳戶建立 IAM 角色。在部署期間，系統會提示您輸入角色 ARN。

Amazon Elastic Container Service (Terraform)

如果您選擇 Amazon ECS， AWS Transform 會產生 Terraform 模組來部署您的應用程式。產生的範本包括：

- ECS 叢集
- 具有任務定義的 ECS 服務
- 具有存取記錄的 Application Load Balancer
- 適用於持久性儲存的 Amazon EFS
- 用於服務探索的私有託管區域
- 運作狀態檢查組態

自動化驗證和安全性掃描

AWS 轉換會自動驗證產生的基礎設施範本，然後再提供給您。驗證包括：

- 對於 Terraform： `terraform fmt`和 `terraform validate`檢查語法和組態正確性。
- 對於 Helm：驗證圖表，以確認產生的資訊清單格式正確。
- 使用 Checkov 進行安全性掃描，以識別所產生基礎設施程式碼中的潛在安全性錯誤設定。

AWS 轉換會報告任何驗證問題，並在繼續之前解決這些問題。

在沒有發佈映像的情況下產生 IaC

即使您未在上一個步驟中發佈容器映像，也可以產生基礎設施範本。產生的範本使用預留位置映像 URIs，您可以在稍後使用實際映像位置進行更新。

您需要執行的事項

產生基礎設施範本

1. 出現提示時，請選擇您的目標平台：Amazon EKS 或 Amazon ECS。
2. 如果您選擇 Amazon EKS， AWS Transform 會詢問是否包含 CloudWatch 記錄。回應是或否。
3. 如果出現提示，請提供應用程式的運作狀態檢查端點詳細資訊 （例如`/health`路徑）。
4. AWS 轉換會產生並驗證基礎設施範本。此步驟會自動執行， AWS 轉換會顯示進度更新，包括任何驗證或安全掃描結果。

5. AWS 轉換呈現範本時，請檢閱產生的範本。

步驟 7：部署測試基礎設施

在此步驟中， AWS Transform 部署測試基礎設施，讓您可以在生產切換之前驗證容器化應用程式。

測試部署期間會發生什麼情況

AWS 轉換會將上一個步驟中產生的基礎設施範本部署到 AWS 帳戶。對於 Amazon EKS 部署，這會使用 Helm。對於 Amazon ECS 部署，這會使用 Terraform。

部署之前， AWS Transform 提供基礎設施值表單，您可以在其中設定部署參數，例如資源名稱、複本計數和環境特定設定。 AWS Transform 也會產生部署預覽，顯示要建立哪些資源，因此您可以在核准之前檢閱變更。

您需要執行的事項

部署和驗證測試基礎設施

1. 使用您的部署組態完成基礎設施值表單。表單包含叢集名稱、命名空間、複本計數和其他環境特定設定等參數。
2. 檢閱顯示將建立或修改之資源的部署預覽。
3. AWS 轉換請求時核准基礎設施部署。
4. 等待部署完成。 AWS Transform 會顯示部署結果。
5. 測試您部署的應用程式，以確認其在容器中正確執行，以及基礎設施符合您的需求。
6. 告知 AWS Transform 您對部署是否滿意，還是想要修改基礎設施並重新部署。

在基礎設施上反覆運算

如果您需要修改基礎設施範本，您可以上傳更新的範本並重新部署：

1. 告知 AWS Transform 您想要修改 IaC。
2. 上傳包含修改後基礎設施範本的 zip 檔案。
3. AWS 轉換會取代範本並執行增量更新 （套用 Terraform 或 Helm 升級）。
4. 檢閱更新的部署結果。

您可以重複此週期，直到您對部署感到滿意為止。

工作階段復原

基礎設施部署會使用 以非同步方式執行。如果您的工作階段在部署期間中斷， AWS Transform 會在您重新連線時自動復原操作，並顯示部署結果。

步驟 8：清除測試基礎設施

完成驗證後， AWS Transform 會縮減測試基礎設施，以避免不必要的成本。

您需要執行的事項

清除測試基礎設施

1. AWS 轉換會通知您測試基礎設施將會遭到破壞。
2. AWS 轉換請求時核准銷毀操作。
3. 等待清除完成。移除所有測試資源後 AWS ，Transform 會顯示結果。

對於 Amazon ECS 部署，此步驟會移除測試部署期間建立的所有資源，包括運算資源、負載平衡器、儲存和聯網元件。

對於 Amazon EKS 部署，清理的範圍會依特定專案的標籤而定。只會移除為此容器化工作流程加上標籤的資源。在同一 Amazon EKS 叢集上執行的其他工作負載不會受到影響。

步驟 9：部署切換基礎設施

在此最終步驟中， AWS Transform 會部署最終基礎設施以供生產使用。切換部署使用您在測試部署步驟期間驗證的相同基礎設施範本。

您需要執行的事項

部署切換基礎設施

1. 使用您的生產部署組態完成基礎設施值表單。您可以從測試部署調整參數，或使用相同的值。
2. 檢閱顯示將建立之生產資源的部署預覽。
3. AWS 轉換請求時核准生產部署。

4. 等待部署完成。 AWS Transform 會顯示切換部署結果。
5. 確認您的應用程式在生產環境中正確執行。

> **Important**
>
> 與您的團隊一起檢閱產生的基礎設施組態，以確保它們符合您組織的安全性、合規性和業務需求。雖然 AWS Transform 提供自動化組態建議，但您有責任驗證和調整設定以符合您的需求，然後再繼續進行切換部署。

工作階段復原

生產部署會使用 以非同步方式執行。如果您的工作階段在部署期間中斷， AWS Transform 會在您重新連線時自動復原操作，並顯示部署結果。

大型主機應用程式的現代化

AWS 轉換旨在加速傳統大型主機應用程式的現代化。它協調大型主機程式碼庫的分析、產生文件、擷取商業邏輯、分解單體結構、轉換舊版程式碼，以及在需要時使用人工輸入 (HITL) 管理整體旅程。用於現代化和遷移大型主機應用程式的 AWS 轉換功能可讓您更快速地現代化關鍵大型主機應用程式，同時在整個轉換過程中保留業務關鍵邏輯。

主題

- 功能和主要功能
- 高階演練
- 循環中的人類 (HITL)
- 大型主機應用程式轉換支援的檔案類型
- 適用於 AWS Transform 主機的支援區域和配額
- 大型主機現代化旅程的高階概觀
- 大型主機應用程式的轉換
- 重構後建置和部署現代化應用程式

功能和主要功能

AWS Transform 為大型主機現代化提供下列功能：

- 支援使用相關聯的 JCL （工作控制語言）、CICS （客戶資訊控制系統） 交易、BMS （基本映射支援） 畫面、Db2 資料庫和 VSAM （虛擬儲存存取方法） 資料檔案，以 COBOL （常見業務導向語言） 和 PL/I （程式設計語言一） 撰寫的 z/OS 大型主機應用程式現代化。
- 支援重構具有 PSAM （簡報服務存取方法）、日文字元集和 NDB （網路資料庫） 資料檔案的 Fujitsu GS21 大型主機應用程式。
- 執行目標驅動推理、分析、分解、規劃、文件產生和程式碼重構。
- 自動將 COBOL 型大型主機工作負載重構為現代化的雲端最佳化 Java 應用程式。
- 協調並與執行分析、文件、分解、規劃和程式碼重構的基礎工具無縫整合。
- 提供ready-to-use基礎設施即程式碼 (IaC) 範本，協助您為現代化大型主機應用程式設定雲端環境。

高階演練

以下是 AWS 轉換的高階演練，用於現代化和遷移大型主機應用程式。

1. 使用 AWS 轉換開始聊天，然後輸入目標。
2. 根據您的目標， AWS Transform 會提議現代化計劃，將高階目標分解為中繼步驟。
3. 根據您提供的目標， AWS Transform 可以：
   - 評估並重新建構程式碼庫
   - 根據目標建立自訂任務

在此過程中， AWS Transform 可能會向您請求資訊以執行任務。

> **Note**
>
> 如需大型主機重構功能 AWS 轉換的詳細資訊，請參閱「大型主機重構 AWS 轉換」文件中的建立專案。

循環中的人類 (HITL)

在整個大型主機應用程式的轉換過程中，您可以透過轉換 Web 體驗來監控 AWS 轉換任務的進度和狀態。

AWS 在下列案例中，轉換會收集其他資訊：

- 需要其他資訊來執行任務時。
- 當中繼成品需要核准時（例如，網域分解或波規劃）。
- 當發生無法自動解決 AWS 轉換的問題時。

大型主機應用程式轉換支援的檔案類型

z/OS 支援的檔案類型包括：

- COBOL 成品和相關 CPY（手冊）
- PL/I 來源檔案
- JCL（工作控制語言）和 JCL 程序 (PROC)

- CICS 系統定義 (CSD)
- 基本映射支援 (Basic Mapping Support)
- Db2 資料庫
- VSAM （虛擬儲存存取方法）
- IMS TM （交易管理員）

Fujitsu GS21 支援的檔案類型包括：

- PSAM （簡報服務存取方法）
- ADL (AIM 定義語言）
- NDB （網路資料庫）

如需 Fujitsu GS21 的詳細資訊，請參閱《 AWS 大型主機轉換遷移指南》中的這些主題：

- GS21
- 擷取和重播 - GS21 終端機
- Mainframe、AS400、Open VMS 和 GS21

適用於 AWS Transform 主機的支援區域和配額

如需支援區域的清單，請參閱 支援的 區域 AWS Transform。

> **Note**
>
> 您的資料可能會在與使用 AWS 轉換的 區域不同的 區域中進行處理。如需跨區域處理的資訊，請參閱 the section called “跨區域處理”。

如需配額限制，請參閱 配額。

大型主機現代化旅程的高階概觀

將大型主機應用程式現代化為 AWS 通常分為四個階段：(a) 評估、(b) 調動、(c) 遷移和現代化，以及 (d) 操作、最佳化和創新。每個階段都會進一步詳細說明目標和相關活動，以支援您的現代化旅程。

階段

- 階段 1：評估
- 階段 2：調動
- 階段 3：遷移和現代化
- 階段 4：操作、最佳化和創新

階段 1：評估

目標：了解您的現代化準備程度，並制定初始現代化計劃。

透過 AWS 轉換，您可以評估大型主機應用程式、基礎設施和操作，以判斷適合您業務需求的現代化方法。

> **Note**
>
> 每個階段都包含一份清單，列出您可以在現代化大型主機應用程式時執行的所有可能活動。您可以略過一些不符合使用案例或目標的活動。

活動

- 從有關現代化的非正式對話開始，並透過在聊天室中找到合適的人員來獲得機會資格
- 判斷機會資格
- 使用應用程式相依性映射計劃和應用程式架構進行初次呼叫簡報
- 確定包含遷移期間基礎設施成本、遷移人力、後製成本、專案持續時間的 ROM （大致數量順序）
- 快速產品組合偵測：
  - 執行模式和工具指導評估
  - 執行原始程式碼分析
  - 識別概念驗證 (POC) 候選者
- 建立技術啟用訓練：
  - 沉浸天數
  - 具有一般主題的研討會
- 為大型大型主機現代化專案或新 AWS 客戶建立遷移整備度評估 (MRA) 報告
- 建立 Mobilize 階段的工作陳述式

階段 2：調動

目標：透過成功的概念驗證或試行現代化來建立基礎並驗證方法。

透過調動階段，您可以建立必要的架構、工具和程序，以支援大規模大型主機現代化。

活動

- 使用試行和識別的 POC 啟動現代化計劃：
  - 分析試行方案並設定程式碼以進行現代化
  - 建置和測試試行現代化資料
  - 交付結果並檢閱試行方案，為更大的資料現代化建立詳細的解決方案
- 對於 平台：
  - 建立安全、合規和監控計畫
  - 使用 AWS 大型主機登陸區域和帳戶結構設定登陸區域環境
  - 確定架構基礎設施、應用程式、整合等
- 考慮人員和程序：
  - Cloud Center of Excellence 是很好的資源
  - 操作模型
- 為不同的應用程式案例建立全面的產品組合分析：
  - 包含高階文件的全面探索
  - 分解計畫（適用於所有應用程式）
  - 所有應用程式的模式和工具指引
  - 提出初始現代化和遷移計劃
- 考量試行、平台、人員和程序，以及全方位的產品組合分析，建立詳細的解決方案
- 判斷商業案例
- 為下一個階段的工作陳述式，使用解決方案完成成功的試行

階段 3：遷移和現代化

目標：在計劃的時間軸和預算內完成現代化和遷移。

在此階段，您可以將大型主機應用程式和資料遷移至 並進行現代化 AWS。

活動

- 將資源配置到生產就緒的應用程式程式碼
- 使用現有文件或採訪主題專家 (SMEs) 來檢閱和分析設計
- 定義測試案例
- 使用適當的執行時間、資料庫和第三方軟體來設定現代化環境
- 遷移和現代化原始程式碼和資料：
  - 您可以根據應用程式程式碼庫中的業務網域反覆現代化應用程式
  - 視需要擴展現代化環境，以支援現代化工作負載
- 建立 CI/CD （持續整合、持續交付） 管道
- 遷移選取的工作負載以啟動現代化。
- 傳輸應用程式並視需要調整環境擴展：
  - 您可以根據需求向上或向下擴展環境
  - 透過執行程式碼健全度測試來現代化工作套件
  - 視需要重新同步原始程式碼
- 執行全面測試並驗證遷移：
  - 收集初始狀態資料
  - 在大型主機上記錄測試案例
  - 階段環境、應用程式和資料
  - 在雲端上執行測試案例
  - 比較來源和目標測試結果
  - 建置自動化測試案例執行管道
  - 產生 KPIs和報告
- 驗證您的資料以進行生產設定
- 透過以下方式驗證您的進度：
  - 執行整合和系統測試
  - 執行效能測試
  - 執行使用者接受度測試
  - 執行 HA/DR 測試
- 使用應用程式擁有者定義推展計畫，並建立訓練和知識轉移的計畫
- 考慮切換並執行生產切換

- 建立對後製活動的持續支援，例如應用程式函數的操作、監控、功能規劃和保證

階段 4：操作、最佳化和創新

目標：支援現代化應用程式的卓越營運和持續改進。

現代化之後，您可以最佳化應用程式的效能、安全性和成本，同時利用 AWS 服務進行創新。

活動

- 監控應用程式：
  - 效能指標
  - 安全實務
  - 合規準則
  - 成本
- 記錄詳細資訊
- 管理應用程式操作：
  - 基礎設施管理
  - 交易和任務管理
  - 執行期環境支援
- 應用程式最佳化和現代化
- 應用程式開發和維護：
  - 編碼 IDE
  - 建置
  - 整合
  - 測試
  - 部署

大型主機應用程式的轉換

AWS Transform 可加速大型主機現代化應用程式的轉換。本主題說明可用的功能。

主題

- 先決條件：在 S3 中準備專案輸入

- 大型主機來源成品集合
- 登入並建立任務
- 追蹤轉換進度
- 設定連接器
- 評估和重新構想任務計畫
- 重新構想任務計畫
- 自訂任務計畫

先決條件：在 S3 中準備專案輸入

AWS 轉換能夠處理複雜的大型主機程式碼庫。若要使用程式碼庫，請確定您的 S3 位置擁有所有資產。

關鍵專案輸入：

- 原始程式碼：您必須將大型主機原始程式碼檔案上傳至 S3。這包括 COBOL 程式、JCL 指令碼、複製手冊和任何其他相關的來源檔案。
- 資料檔案：如果您有大型主機應用程式使用的任何 VSAM 檔案或其他資料檔案，則需要將這些檔案上傳至 S3。
- 組態檔案：包含您大型主機環境特有的組態檔案。

其他專案輸入

- 系統管理設施 (SMF) 記錄：如果適用，請將 SMF 記錄上傳到存放原始碼的 S3 儲存貯體中的新資料夾，這些記錄應該是 .zip 檔案格式。
- 格式化：對於技術文件產生，您可以利用選用的組態檔案來產生符合所需格式和標準的 PDF 文件，包括標頭、頁尾、標誌和自訂資訊。
- 詞彙表： AWS Transform AWS Transform 利用自動化與生成式 AI 進行文件產生和業務規則擷取。在 zip 檔案的根目錄中包含包含重要縮寫和術語相關資訊的詞彙表 CSV 檔案，將有助於改善產生的文件品質。
- 測試資料：如果可用，請上傳可用於驗證現代化應用程式的測試資料集。此資料應存放在存放來源碼的 S3 儲存貯體中的新資料夾中。

您可以在此處找到專案輸入的詳細資訊。

大型主機來源成品集合

本主題概述了收集大型主機原始程式碼和相關成品的程序，以支援使用 AWS Transform 的大型主機現代化計畫。正確收集和準備來源成品對於成功分析、遷移規劃和實作至關重要。

原始程式碼庫存

應用程式原始碼類型

支援下列應用程式原始碼類型：

- COBOL 程式
- JCL 指令碼
- 組裝器程式
- PL/I 程式
- CICS 交易
- 自然程式
- REXX 指令碼
- Easytrieve 程式
- 複製手冊和 包含
- Proc 程式庫

資料庫資產

支援下列資料庫資產：

- DB2 DCLGEN 和 DDL 指令碼
- IMS 資料庫定義 (PSBs和 DBDs)
- VSAM 檔案定義
- 實體和邏輯資料庫結構描述
- 資料庫程序和觸發條件

原始程式碼副檔名

如果您不確定延伸模組，請將它保留為空白或 .txt，且 AWS Transform 會為您分類。

下表列出大型主機來源成品的常見副檔名。

大型主機原始碼副檔名

語言/類型	常見延伸模組	說明
COBOL	.cbl、.cob、.cobol	COBOL 來源程式
JCL	.jcl	任務控制語言指令碼
組裝器	.asm	組合語言程式
PL/I	.pl1	PL/I 語言程式
CICS 定義	.csd	CICS 系統定義 (CSD)
自然	.nat	自然程式
REXX	.rex、.rexx	REXX 指令碼
Easytrieve	.ezt	Easytrieve 報告程式
複製手冊	.cpy	COBOL 複製手冊
BMS	.bms	基本映射支援 (BMS)
PL/I 複製手冊	.pl1_copy	PL/I 複製手冊
Db2 DCLGEN	.dcl	Db2 宣告產生器
Db2 定義	.sql、.ddl	Db2 資料庫定義
IMS 定義	.ims	IMS 資源定義資料集 (IMS 階段 1)
MFS	.mfs	IMSMFS （訊息格式服務）
PSB	.psb	IMS PSB （程式規格區塊）
DBD	.dbd	IMS 資料庫定義
JCL 處理	.prc、.proc	JCL 程序程式庫
JCL 包括	.inc	JCL 包含檔案

語言/類型	常見延伸模組	說明
巨集	.mac	組裝器巨集
控制卡	.ctl	JCL 公用程式控制卡

收集方法

原始程式碼擷取

使用安全 FTP 用戶端 (WinSCP/FileZilla) 從大型主機 PDS 程式庫中擷取互動式原始程式碼。

DB2 結構描述擷取

DB2 LUW (Linux、UNIX 和 Windows) 用戶端軟體包含 db2look公用程式做為其安裝套件的一部分。db2look 公用程式會從 DB2 資料庫擷取 DDL （資料定義語言） 陳述式。

執行以下命令：

```
db2look -d DATABASE_NAME -i userid -w password -a -e -m -l -x -f -createdb -printdbcfg
 -o DATABASE_NAME.sql
```

下列清單說明參數：

- `-d` *`DATABASE_NAME`*：指定要從中擷取結構描述的資料庫名稱
- `-i` *`userid`*：資料庫身分驗證的使用者 ID
- `-w` *`password`*：資料庫身分驗證的密碼
- `-a`：擷取授權資訊 （授與）
- `-e`：擷取所有資料庫物件 （資料表、檢視、索引等）
- `-m`：擷取統計資料和實體特性
- `-l`：擷取資料表和資料欄註解
- `-x`：擷取說明資料表
- `-f`：格式化輸出以提高可讀性
- `-createdb`：包括資料庫建立陳述式
- `-printdbcfg`：包括資料庫組態參數

- `-o DATABASE_NAME.sql`：指定輸出檔案名稱

從大型主機擷取目錄資訊

IDCAMS 中的 LISTCAT 命令是一種公用程式，用於擷取大型主機上資料集的目錄資訊。這在大型主機現代化專案期間非常有用，可清查資料集並了解其特性。

```
//LSTCATJ JOB 'LISTCAT',CLASS=A,MSGCLASS=X,NOTIFY=&SYSUID
//*
//STEP1 EXEC PGM=IDCAMS
//*
//SYSPRINT DD DSN=AWS.M2.CATALOG.LIST,
//            DISP=(NEW,CATLG,DELETE),
//            SPACE=(CYL,(1,1),RLSE),
//            DCB=(RECFM=FBA,LRECL=133,BLKSIZE=0)
//*
//SYSIN DD *
  LISTCAT ENT('AWS.M2.CARDDEMO.*') ALL
  LISTCAT ENT('SYS1.*') ALL
/*
```

擷取 CICS 定義

IBM 提供的 DFHCSDUP 公用程式可以從 CICS 系統定義 (CSD) 檔案擷取 CICS 資源定義。

使用下列 JCL 從 DFHCSD 卸載現有定義：

```
//CSDEXTJ JOB 'EXTRACT CSD',CLASS=A,MSGCLASS=X,NOTIFY=&SYSUID
//*
//STEP1 EXEC PGM=DFHCSDUP,REGION=0M,
//          PARM='CSD(READONLY),PAGESIZE(60),NOCOMPAT'
//*
//STEPLIB  DD DSN=your-hlq.SDFHLOAD,DISP=SHR
//DFHCSD   DD DSN=your-hlq.DFHCSD,DISP=SHR
//*
//CBDOUT   DD DSN=your-hlq.CSD,
//            DISP=(NEW,CATLG,DELETE),
//            SPACE=(CYL,(1,1),RLSE),
//            DCB=(RECFM=FB,LRECL=80,BLKSIZE=0)
//SYSPRINT DD SYSOUT=*
//SYSIN DD *
  EXTRACT GROUP(cics-group) USERPROGRAM(DFH0CBDC) OBJECTS
```

```
/*
```

擷取 IMS 定義

若要擷取 IMS 定義，您可以使用 DFSURDD0 公用程式產生 IMS 交易檔案。此公用程式會建立階段 1 巨集陳述式，可用於遷移。目前僅支援 IMS 階段 1。

使用下列 JCL 擷取 IMS 定義：

```
//IMSEXTJ JOB 'IMS STAGE 1',CLASS=A,MSGCLASS=X,NOTIFY=&SYSUID
//*
//STEP1 EXEC PGM=DFSURDD0,MEMLIMIT=12G
//*
//STEPLIB  DD DISP=SHR,DSN=your-hlq.SDFSRESL
//*
//RDDSDSN DD DISP=SHR,DSN=your-rdds
//*
//SYSOUT   DD DSN=your-hlq.STAGE1.IMS,
//            DISP=(NEW,CATLG,DELETE),
//            SPACE=(CYL,(1,1),RLSE),
//            DCB=(RECFM=FB,LRECL=80,BLKSIZE=0)
//SYSPRINT DD SYSOUT=*
//SYSIN DD *
  OUTPUT=MAC
/*
```

擷取 CA-7 排程器資訊

CA-7 任務排程資訊包含在 LJOB 報告中。使用 LJOB 公用程式搭配 LIST=NODD 參數來產生大型主機的報告。報告必須具有.ca7副檔名。每個報告在資料欄 1 中都必須有 ANSI 換行控制字元。您可以在用來執行 LJOB 公用程式的 JCL 中指定 DCB=RECFM=FBA（或 FA），在資料欄 1 中建立包含換行控制字元的報告。

例如：LJOB,JOB=ZBN*,LIST=ALL

如需詳細資訊，請參閱 Broadcom 文件。

擷取 SMF 資料

System Management Facility (SMF) 記錄提供 AWS Transform 用來分析批次任務和 CICS 交易用量的活動指標。支援下列 SMF 記錄類型：14、15、30（子類型 5)、64、102、110（子類型 1 搭配資料類別 1、3 和 4)。

SMF 記錄的格式需求：

- 必須包含記錄類型 30 和 110 （至少）
- 必須是包含 RDW (Record Descriptor Word) 位元組的原始二進位 EBCDIC 格式
- 必須以下列其中一種方式提供：
  - 高達 600 MB 的檔案，以 .zip 格式壓縮
  - 最多 5 GB 的檔案，以 .tar.gz 或 .gz 格式壓縮
- 必須與 Amazon S3 中的原始程式碼存放在不同的資料夾中

提供至少 13 個月的 SMF 記錄，以擷取較短時間範圍可能遺漏的年度批次週期和季節性模式。

選項 1：擷取和排序 SMF 記錄

使用下列範例 JCL 來擷取和排序 SMF 記錄：

```
//SMFEXTR  JOB (ACCT),'EXTRACT SMF',CLASS=A,
//             MSGCLASS=X,NOTIFY=&SYSUID
//*--------------------------------------------------------------------*
//* SMF RECORD EXTRACTION TEMPLATE
//* CUSTOMIZE: Job card, dataset names, date range, record types
//*--------------------------------------------------------------------*
//*
//* STEP 1: EXTRACT SMF RECORDS
//*
//EXTRACT  EXEC PGM=IFASMFDP
//SYSPRINT DD SYSOUT=*
//*
//* INPUT: Specify your SMF datasets (MAN files or GDG)
//*
//DUMPIN   DD DISP=SHR,DSN=SYS1.MAN1
//         DD DISP=SHR,DSN=SYS1.MAN2
//         DD DISP=SHR,DSN=SYS1.MAN3
//*
//* OUTPUT: Extracted SMF records
//*
//DUMPOUT  DD DSN=your.hlq.SMF.EXTRACT,
//            DISP=(NEW,CATLG,DELETE),
//            UNIT=SYSDA,
//            SPACE=(CYL,(500,100),RLSE),
//            DCB=(RECFM=VBS,LRECL=32760,BLKSIZE=27998)
//*
```

```
//* CONTROL CARDS
//*
//SYSIN    DD *
  INDD(DUMPIN,OPTIONS(DUMP))
  OUTDD(DUMPOUT,TYPE(14,15,30,110))
  DATE(yyyy/ddd,yyyy/ddd)
  START(0000)
  END(2359)
/*
//*
//* STEP 2: SORT EXTRACTED RECORDS (OPTIONAL)
//*
//SORT     EXEC PGM=SORT
//SORTIN   DD DISP=SHR,DSN=your.hlq.SMF.EXTRACT
//SORTOUT  DD DSN=your.hlq.SMF.SORTED,
//            DISP=(NEW,CATLG,DELETE),
//            UNIT=SYSDA,
//            SPACE=(CYL,(500,100),RLSE),
//            DCB=(RECFM=VBS,LRECL=32760)
//SORTWK01 DD UNIT=SYSDA,SPACE=(CYL,(50))
//SORTWK02 DD UNIT=SYSDA,SPACE=(CYL,(50))
//SORTWK03 DD UNIT=SYSDA,SPACE=(CYL,(50))
//SYSOUT   DD SYSOUT=*
//SYSPRINT DD SYSOUT=*
//SYSIN    DD *
  SORT FIELDS=(11,4,CH,A,7,4,CH,A,15,4,CH,A),EQUALS
/*
```

在上述 JCL 中自訂下列值：

1. 工作卡：更新帳戶、類別和訊息類別
2. DUMPIN：指向您的 SMF 資料集
3. DUMPOUT：指定輸出資料集名稱和 HLQ
4. TYPE：選取記錄類型 (14、15、30、110 或其他）
5. 日期：格式 yyyy/ddd （例如 2026/055、2026/056)
6. SPACE：根據預期的資料量調整
7. 如果不需要，請移除 SORT 步驟

選項 2：使用 DFSORT 擷取 SMF 資料

您可以使用 DFSORT 來合併和報告歷史 SMF 資料。如果您依日或週將 SMF 記錄存放在 GDG 中，這會很有幫助。下列任務使用 DFSORT 從 SORTIN 檔案合併 SMF 記錄，並根據 INCLUDE COND 參數中指定的記錄進行篩選。

```
//EXTRSMF JOB 'EXTRACT SMF RECORDS',CLASS=S,MSGCLASS=H,
// MSGLEVEL=(1,1),REGION=0M,NOTIFY=&SYSUID,TIME=1440
//SORTJES2 EXEC PGM=SORT,REGION=0M
//SYSOUT DD SYSOUT=*
//SORTMSG DD SYSOUT=*
//SORTIN DD DISP=SHR,DSN=your.hlq.SMF.EXTRACT
//SORTOUT DD DSN=your.hlq.SMF.OUTPUT,
// DISP=(MOD,CATLG,DELETE),
// DCB=(BUFNO=20,
// RECFM=VBS,LRECL=32760,BLKSIZE=27998),
// SPACE=(CYL,(1400,900),RLSE)
//SORTWK1 DD UNIT=SYSDA,SPACE=(CYL,(30,50))
//SORTWK2 DD UNIT=SYSDA,SPACE=(CYL,(30,50))
//SORTWK3 DD UNIT=SYSDA,SPACE=(CYL,(30,50))
//SORTWK4 DD UNIT=SYSDA,SPACE=(CYL,(30,50))
//SYSIN DD *
OPTION COPY
INCLUDE COND=(6,1,BI,EQ,X'0E',OR,6,1,BI,EQ,X'0F',OR,
6,1,BI,EQ,X'1E',OR,6,1,BI,EQ,X'40',OR,
6,1,BI,EQ,X'50',OR,6,1,BI,EQ,X'59',OR,
6,1,BI,EQ,X'5C',OR,6,1,BI,EQ,X'65',OR,
6,1,BI,EQ,X'66',OR,6,1,BI,EQ,X'6E')
```

若要在保留 RDW 資料的同時下載資料，您可以使用 FTP 伺服器來接收解壓縮的檔案。確保以二進位格式傳輸資料，並使用 RDW 選項，以便將 RDW 包含在資料傳輸中。下列任務顯示傳輸此檔案的 FTP 任務範例。

```
//EXTRSMF JOB 'EXTRACT SMF RECORDS',CLASS=A,MSGCLASS=H,
// MSGLEVEL=(1,1),REGION=0M,NOTIFY=&SYSUID,TIME=1440
//STEP1 EXEC PGM=FTP,REGION=2048K
//SYSIN DD *
10.10.10.10
userid
password
type i
LOCSITE RDW
```

```
put 'your.hlq.SMF.OUTPUT' SMFREQS.SMF
quit
```

上傳 SCRT 報告

您也可以將子容量報告工具 (SCRT) 報告上傳至 AWS 轉換。

應用程式庫存上傳

收集所有成品之後，請完成下列步驟：

1. 依成品類型將檔案整理成子資料夾（例如 /cobol、/jcl、/copybooks、/db2、/ims、/cics、/ca7)。
2. 將頂層資料夾壓縮為單一 .zip 檔案。
3. 將 .zip 檔案上傳至連接到 AWS 轉換工作區的 Amazon S3 儲存貯體。

> **Note**
>
> SMF 記錄必須放置在與 Amazon S3 儲存貯體中原始碼不同的資料夾中，且必須是 .tar.gz 或 .gz 格式。

如需將 Amazon S3 儲存貯體連線至 AWS 轉換的詳細說明，請參閱 the section called “設定連接器”。

登入並建立任務

若要登入 AWS 轉換 Web 體驗，請遵循文件 AWS 轉換入門區段中的所有指示。

若要建立和啟動任務：請遵循啟動專案中的步驟。

建立工作區：命名並描述將存放任務、協作者和相關聯成品的工作區。

建立任務：從預先設定的任務計畫中選取 以建立任務，或從支援的 功能清單中選取 以根據您的目標自訂任務計畫。

> **Important**
>
> AWS 如果您沒有適當的許可，轉換會拒絕您的操作。例如，參與者無法取消大型主機應用程式的任務轉換或刪除任務。只有管理員可以執行這些函數。

建立任務時，您可以從以下功能中選取 ，但啟動步驟始終是必要的，因為它是專案原始碼的位置。在工作區中設定的第一個任務中，您必須設定 Amazon S3 儲存貯體的連接器。

追蹤轉換進度

您可以透過兩種方式追蹤整個程序的轉型進度：

- Worklog – 這提供 AWS Transform 所採取動作的詳細日誌，以及人工輸入請求，以及您對這些請求的回應。
- 儀表板 – 這可提供大型主機應用程式轉換的高階摘要。它顯示轉換的任務數量、套用的轉換，以及完成大型主機應用程式轉換的預估時間的指標。您也可以查看每個步驟的詳細資訊，包括各檔案類型的程式碼行、各檔案類型產生的文件、分解的程式碼，以及遷移計畫。

設定連接器

AWS 轉換會使用連接器來存取您帳戶中大型主機現代化函數所需的資源。連接器會自動設定您在工作區中執行的第一個任務。根據您選擇的任務計劃， AWS Transform 會引導您建立連接器。

大型主機重新構想連接器

大型主機重新構想連接器適用於執行評估和重新構想工作流程的任務。它使用 S3 儲存貯體來存取和存放轉換資源，以及使用 Amazon Neptune 叢集來存放擷取的成品。Neptune 叢集可做為統一的知識圖表，存放任務的所有擷取成品，而知識圖表會回答 AWS 轉換聊天介面中的所有問題。

在 VPC 中部署 Amazon Neptune 叢集，其中 AWS Transform 可以建立彈性網路介面 ENIs)。這些是允許 AWS Transform 安全地與 VPC 中的 Neptune 通訊的網路連線，以載入資料並查詢您的知識圖表。

AWS CloudFormation

建議使用下列 CloudFormation 範本來建立大型主機重新構想連接器所需的資源。執行 CloudFormation 範本時，請使用您計劃用於連接器的相同 S3 儲存貯體。如需使用 CloudFormation 範本的詳細資訊，請參閱使用範本。

若要下載 CloudFormation 範本，請選擇 neptune-kg-setup.yaml。

範本接受下列參數：

- BucketName – 必要。Neptune 大量載入器存取的 S3 儲存貯體名稱。您必須使用您計劃在 AWS 轉換連接器中使用的相同 S3 儲存貯體。

- KmsKeyId – 選用。Neptune 加密的 KMS 金鑰。接受金鑰 ID、ARN、別名名稱或別名 ARN。如果省略，則預設為 AWS 受管金鑰。

當您設定連接器時，請提供下列詳細資訊：

- S3 儲存貯體 ARN
- Neptune 叢集 ARN
- Neptune 叢集資源 ID
- 應用程式子網路 IDs
- 應用程式安全群組 ID
- Neptune S3 大量載入器角色 ARN

> **Important**
>
> CloudFormation 範本的輸出索引標籤包含您在設定連接器時需要提供給 AWS Transform 的詳細資訊。

自訂組態

如果您偏好使用現有的 VPC 或其他工具來建立必要的基礎設施，您的環境必須符合下列要求：

Neptune 叢集

- 引擎版本 1.4.5.1 或更新版本的 Amazon Neptune Serverless
  - IAM 身分驗證已啟用
  - 啟用儲存加密 (AWS 受管金鑰或客戶受管 KMS 金鑰）
- 無伺服器擴展組態（建議：1–128 NCUs)
- （建議）第二個可用區域中的僅供讀取複本，可提供高可用性並改善讀取效能

聯網

- 啟用 DNS 支援和 DNS 主機名稱的 VPC
- 不同可用區域中至少有兩個子網路。 AWS Transform 會在這些子網路中建立 ENIs，以存取 Neptune 叢集，而 Neptune 叢集可以位於相同的子網路或專用子網路中。將子網路大小調整為 /20，以容納 VPC 端點和應用程式 ENIs。

- 透過 VPC 介面端點 (AWS PrivateLink) 從子網路到下列 AWS 服務的網路連線：
  - AWS Transform Agents API – 協調大型主機現代化任務
  - Amazon Bedrock 執行期 – 調用基礎模型進行分析和推理
  - Amazon Relational Database Service (Amazon RDS) – Neptune 叢集管理
  - Amazon Elastic Compute Cloud (Amazon EC2) – ENIs的管理
  - Amazon CloudWatch – AWS 轉換可觀測性的指標
- 連接至與子網路相關聯路由表的 S3 閘道端點。 AWS Transform 使用此端點將資料從 S3 儲存貯體載入 Neptune 叢集。

Security groups (安全群組)

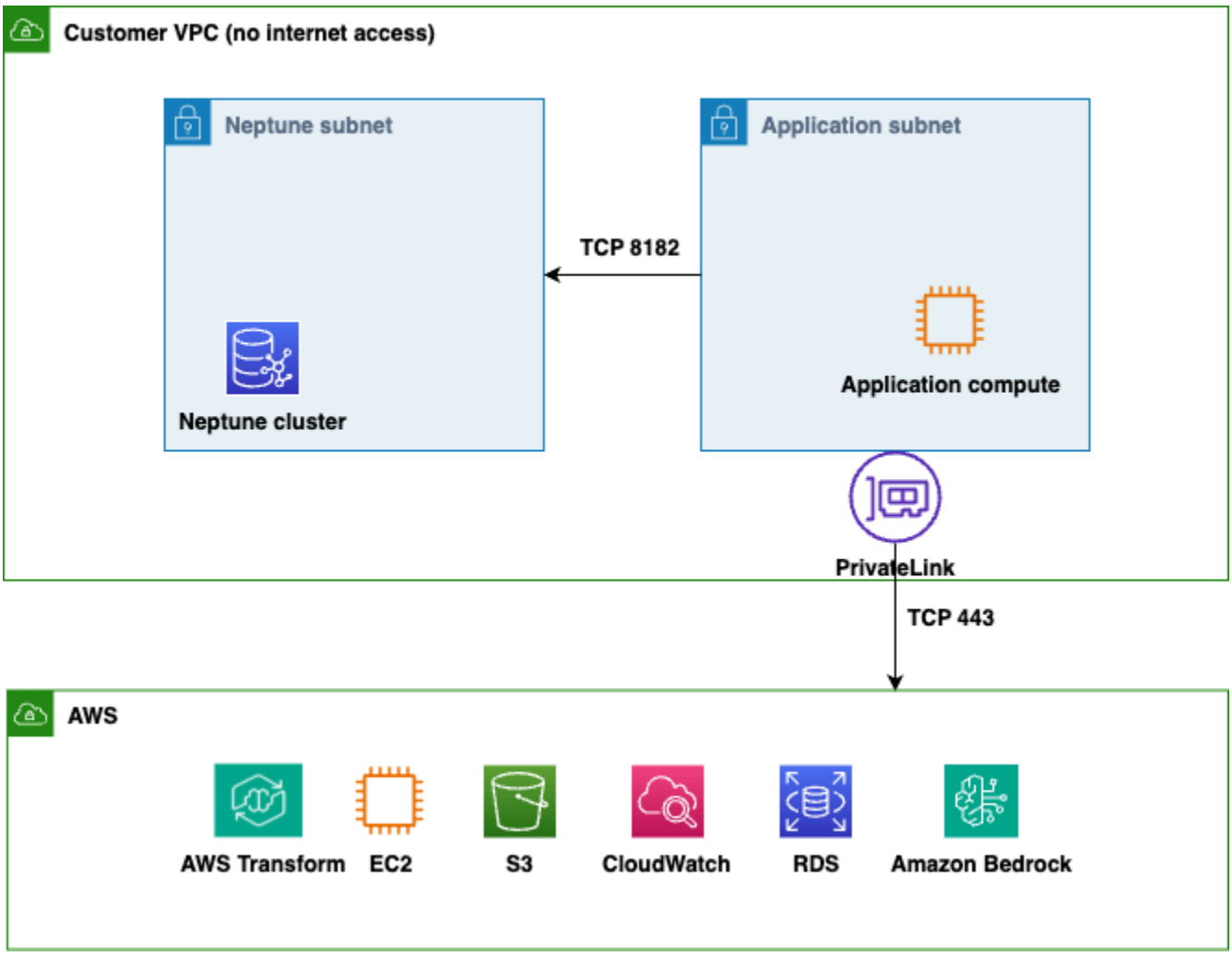
安全群組會連接到 ENIs，而非子網路。即使 AWS 轉換 ENIs和 Neptune 位於相同的子網路中，個別的安全群組也會控制它們之間的存取。

- 安全群組 （連接至 AWS Transform 建立ENIs)，允許：
  - 將 TCP 8182 傳出至 Neptune 安全群組
  - 用於連接 VPC 端點的傳出 TCP 443
- 安全群組 （連接至 Neptune 叢集），允許：
  - 從應用程式安全群組傳入 TCP 8182
- VPC 端點安全群組 （連接至介面端點 ENIs)，允許：
  - 從應用程式安全群組傳入 TCP 443

IAM

- 具有 信任政策的 IAM 角色`rds.amazonaws.com`，可授予 S3 儲存貯體`s3:GetBucketLocation`上的 `s3:ListBucket`、 `s3:GetObject`和
- 此角色必須與 Neptune 叢集相關聯，才能大量載入知識圖表資料

下圖顯示建議的架構。



S3 連接器

對於具有自訂計劃的任務， AWS Transform 可以使用 S3 連接器。S3 連接器使用 S3 儲存貯體來存取和存放轉換資源，以及用於索引輸出的 S3 向量儲存貯體。

> **Important**
>
> 您的資料會儲存在工作區的 AWS 轉換成品存放區中，並僅用於執行任務。

S3 向量儲存貯體的選用組態。

在可使用 S3 向量儲存貯體的區域中， AWS Transform 會將任務輸出的可搜尋向量編碼存放在您的帳戶中的此 S3 向量儲存貯體中，以提供 AI 支援的搜尋和聊天體驗。資料不會用於此任務之外，也不會

用於訓練模型。若要啟用此功能，您必須建立並提供 S3 向量儲存貯體。 AWS Transform 會自動建立並連接具有寫入此儲存貯體所需許可的角色。

S3 儲存貯體 CORS 許可

設定連接器後，請將下列 CORS 政策新增至 S3 儲存貯體，以便您可以直接在 AWS 轉換主控台中檢視和比較成品。如果未正確設定此政策，則可能無法使用 AWS 轉換的內嵌檢視或檔案比較功能。

```
[
    {
        "AllowedHeaders": [],
        "AllowedMethods": [
            "GET"
        ],
        "AllowedOrigins": [
              "https://*.transform.eu-central-1.on.aws",
              "https://*.transform.ap-south-1.on.aws",
              "https://*.transform.ap-northeast-1.on.aws",
              "https://*.transform.ap-northeast-2.on.aws",
              "https://*.transform.ap-southeast-2.on.aws",
              "https://*.transform.ca-central-1.on.aws",
              "https://*.transform.eu-west-2.on.aws",
              "https://*.transform.us-east-1.on.aws",
              "https://*.transform.sa-east-1.on.aws"
        ],
        "ExposeHeaders": [],
        "MaxAgeSeconds": 0
    }
]
```

評估和重新構想任務計畫

評估和重新構想任務計畫是用於現代化大型主機應用程式的預先定義工作流程。它會引導您完成兩個階段：評估您的程式碼庫以識別業務函數，並重新構想您選取的函數。若要改為選擇個別功能，請使用自訂任務計劃。

評估

大型主機現代化旅程通常從評估程式碼庫開始，以識別內容並了解關係和相依性。在此評估之後，您可以開始分解並選取要現代化之來源碼的部分。分解的界限取決於業務職能。

商業函數目錄會將您的程式碼庫分解為離散的商業函數，這些函數是以決定性資料路徑為基礎，從頭到尾映射每個商業函數。資料路徑是資料需要的路由，從業務觸發到大型主機程式碼中的最終寫入。系統不會將分析限制為單一進入點，而是跨越批次任務、CICS 交易及其共用資料存放區，以識別一致的業務工作單位。

業務職能是從業務觸發條件開始，並以可衡量的業務成果結束的工作內文。 AWS Transform 提供業務線可以採取動作的業務職能目錄，讓企業能夠先做出有關要現代化項目的明智決策。

使用商業函數評估程式碼庫以現代化的優勢：

- 全方位可見性 – 了解批次任務、線上交易和資料存放區如何為您的業務連接到有意義的 函數。
- 可行界限 – 每個已識別的業務職能都是獨立的單位，您的line-of-business利益相關者可以檢閱並排定現代化工作的優先順序。
- 從程式碼到規格的一致性 – 定義商業函數的相同程式碼區塊用於產生其規格，無需翻譯層，也不需要調校。
- 縮短探索時間 – 自動化偵測以系統化、可重複的分析取代幾個月的手動部落知識訪談。

透過聊天提供的評估結果

透過聊天提供的評估結果包括業務職能清單，包括資料路徑的數量、每個職能在批次和 CICS 交易方面的範圍，以及業務描述。您會收到在 Amazon S3 儲存貯體中產生成品的連結，您也可以透過聊天存取這些成品。提供兩種成品：業務職能詳細資訊和業務職能摘要。

- 商業函數摘要 – 提供商業函數的清單，以及程式碼中元素正在執行之函數的自然語言描述。
- 商業函數詳細資訊 – 提供互動式圖形，描述來源碼之間的關係。

若要與圖形互動，請選取 元素以顯示其其他詳細資訊，或開啟 元素來查詢其詳細資訊。在每個頁面中，都有該層級的所有元素摘要，以及要與 互動並進一步了解每個元件的圖形界面，包括下列項目：

- 業務職能 – 描述哪些業務職能互相連接，並提供每個業務職能的概觀。當您選取業務函數時，會提供下列資訊：
  - 資料路徑的數量
  - 程式碼的行數
  - 業務描述：業務功能的概觀，以自然語言描述程式碼中的元素正在執行哪些功能。
  - 介面：詳細說明業務職能中的資料元素的關聯方式 （例如交換或寫入）。

- 業務職能詳細資訊 – 描述單一業務職能中跨資料路徑的連線，可讓您深入了解業務職能的組成。當您選取 元素時，您會看到該元素如何跨業務函數連線，以及下列詳細資訊：
  - 資料存放區：資料存放區的寫入器和讀取器。
  - 其他元素：相關資料路徑的概觀，以自然語言描述資料路徑中處理的動作和結果、程式清單，以及讀者和寫入者。
- 資料路徑 – 描述一個資料路徑的詳細資訊，以及資料路徑中的元素彼此之間的關聯。
  - 描述：資料路徑的概觀，以自然語言描述資料路徑中處理的動作和結果。
  - 資料路徑的內容：
    - 進入點
    - 讀取
    - 寫入
    - 程式

透過聊天，您可以查詢輸出以了解每個業務職能中包含的元素，並透過業務職能圖表探索界限。

在您識別現代化邊界之後，聊天會提示您選取要重新構想的業務函數。您可以選擇單一業務職能或多個業務職能。 AWS Transform 會將選取的界限和必要的評估輸出傳送至重新構想流程，以繼續現代化旅程。

完成第一次現代化後，您可以使用聊天功能選取要現代化的額外商業功能集。

重新構想

在重新構想階段，您可以選擇評估識別的一或多個業務職能，並準備進行現代化。這會觸發業務邏輯擷取，然後為選取的業務函數產生需求。產生的要求是轉送工程的主要輸入，將傳統系統理解轉換為現代化應用程式必須提供的精確規格。

擷取商業邏輯

選取一或多個業務職能之後， AWS Transform 會開始為選取的業務職能產生業務邏輯。擷取完成後，AWS Transform 會將結果以 JSON 格式存放在 Amazon S3 儲存貯體中，以供下游使用。您可以監控擷取進度，並直接在 AWS 轉換主控台中檢閱任何問題。

檢閱商業邏輯擷取結果

1. 在左側導覽窗格中，選擇擷取業務邏輯步驟將其展開。
2. 從步驟詳細資訊中檢視下列項目：

- S3 儲存貯體連結：擷取的業務邏輯結果以 JSON 格式儲存的位置。
- 問題：業務邏輯擷取程序期間遇到的任何問題清單。

如果在擷取期間遇到任何檔案問題，每個受影響的檔案會顯示下列詳細資訊：

- 檔案名稱：遇到問題的檔案名稱。
- 檔案類型：檔案類型（例如 COBOL 或 JCL)。
- 檔案路徑：應用程式內檔案的位置。
- 狀態：檔案擷取的目前狀態。
- 詳細資訊：所遇到問題的描述。

> **Note**
>
> 擷取步驟完成後， AWS Transform 會自動開始產生需求。在此程序開始之前，不會提示您輸入任何其他輸入。

產生需求

業務邏輯擷取完成後，產生需求代理程式會使用擷取的成品（程式碼分析、資料分析、業務規則），並產生現代化需求。這些要求是與技術無關的正式功能規格，並包含可測試的接受條件。 AWS Transform 會為您選取的每個業務函數產生一個`requirements.md`檔案，並將輸出存放在 Amazon S3 儲存貯體中。若要檢視輸出的 Amazon S3 位置，請選擇產生需求步驟。

每個`requirements.md`檔案會組織為下列部分：

- 標題 – 為業務函數及其代表的工作流程命名。
- 全域先決條件 – 在處理之前和期間在整個工作流程中必須保持 true 的條件。可設定的值會顯示為參數預留位置。
- 已編號的工作流程區段 – 每個區段代表業務職能的分散階段。每個區段都包含下列項目：
  - 將目標陳述為角色、該角色想要採取的動作，以及結果的使用者案例。
  - EARS (Easy Approach to Requirements Syntax) 格式中的需求清單，每個格式都有唯一的識別符。

> **Note**
>
> 選取第二組商業函數會重新啟動新選取函數的重新構想步驟。然後，主控台只會顯示新選擇的結果，因此不會再顯示先前業務職能中業務規則的任何問題，以及存放業務邏輯和要求的輸出的 Amazon S3 連結。您先前的輸出不會遺失。您仍然可以從成品索引標籤或 Amazon S3 儲存貯體中存取它們。

轉換成品之間的可追蹤性

AWS 轉換可在整個評估和重新構想工作流程中產生的成品之間維持可追蹤性。可追蹤性可讓您追蹤每個需求到解壓縮的業務規則，或直接追蹤到產生要求的原始原始原始原始程式碼。

您可以使用 `traceability.yaml` 檔案來檢視每個業務職能的所有可追蹤性詳細資訊。它描述了每個業務規則如何映射到要求。

如需互動式可追蹤性，您可以在 VS Code 和 Open VSX 相容編輯器中使用 IDE 外掛程式。如需詳細資訊，請參閱開發人員工具。

重新構想任務計畫

對於您已為現代化設定範圍且已準備好重新構想的應用程式，您可以執行獨立的重新構想任務。任務會分析您的程式碼和資料、擷取商業邏輯、識別商業網域，以及為每個商業網域產生現代化需求。

自訂任務計畫

自訂任務計畫可讓您選取要執行的功能，以建置自己的現代化工作流程。它可讓您完全控制包含哪些功能。根據您的現代化目標，從下列功能中進行選擇。有些功能取決於先執行的其他功能。例如，大多數其他功能都需要程式碼分析。

分析程式碼

與 AWS Transform 共用 Amazon S3 儲存貯體路徑後，它會分析每個檔案的程式碼，其中包含檔案名稱、檔案類型、程式碼行及其路徑等詳細資訊。

> **Note**
>
> 您可以透過任務或工作區層級的成品索引標籤下載分析程式碼結果。在任務層級前往左側導覽選單中的「Artifacts」選項，開啟「結果」資料夾，或在工作區層級尋找任務名稱，並開啟

「結果」資料夾。這將下載 zip 檔案，其中包含手動分類工作流程的分類檔案、資產清單、相依性 JSON 檔案，以及遺失檔案的清單。

在任務計畫中，選取左側導覽窗格中的分析程式碼以檢視結果。您可以透過多種方式檢視程式碼分析結果：

- 清單檢視 – 您要為大型主機轉換的 Amazon S3 儲存貯體中的所有檔案
- 檔案類型檢視 – Amazon S3 儲存貯體中每個檔案類型顯示的所有檔案。如需支援的檔案類型清單，請參閱支援的檔案。
- 資料夾檢視 – 在資料夾結構中顯示的 Amazon S3 儲存貯體中的所有檔案。

在檔案結果中， AWS Transform 會根據您選擇的檔案檢視提供下列資訊：

- 名稱
- 檔案類型
- 程式碼總行數
- 檔案路徑
- 註解行
- 空行
- 有效的程式碼行
- 檔案數目
- Cyclomatic Complexity - Cyclomatic complexity 代表透過程式原始碼的線性獨立路徑數量。 AWS Transform 會顯示每個檔案的週期複雜性。

遺失檔案 – 大型主機現代化程式碼分析中遺失的檔案。理想情況下，這些檔案應新增為 Amazon S3 儲存貯體中來源輸入的一部分，且分析步驟應重新執行，以獲得更佳且一致的結果。

同名 – AWS Transform 提供您共用相同名稱的檔案清單，以及可能相同的特性 （例如程式碼行數）。它將無法一次比較任何兩個檔案的內容之間的差異。

重複IDs – 使用 Cobol 程式時，程式 ID 欄位可做為檔案的唯一識別符。此 ID 必須是唯一的，因為它用於在整個專案中呼叫程式。不過，有些專案可能有不同名稱但程式 ID 相同的 COBOL 檔案。在評估期間取得這些檔案的清單，有助於了解所有程式之間的相依性。

> **Note**
>
> 這是 COBOL 程式碼和檔案特有的。

當您的程式具有重複IDs 時，建議您變更這些檔案的程式 IDs，以擁有 COBOL 程式碼中每個檔案的唯一識別符。然後，您可以重新執行任務，以取得更準確且全面的程式碼分析結果。

透過解決重複IDs，您可以：

- 改善程式碼清晰度和可維護性
- 減少程式呼叫中的潛在衝突
- 提升相依性映射的準確性
- 簡化未來的現代化工作

Codebase 問題 – 在程式碼庫中偵測到的潛在問題，您應該先解決這些問題，然後再繼續現代化專案。這些問題可能包括缺少與程式碼中相關聯陳述式或不支援連結的參考。

更新分類 – 透過手動重新分類，您可以透過上傳具有新分類的 JSON 檔案，使用大量更新功能重新分類檔案。

> **Important**
>
> 這僅適用於 UNKNOWN和 TXT 檔案。

重新分類後， AWS Transform 將：

1. 更新分類結果
2. 使用新的檔案類型重新執行相依性分析
3. 重新整理所有受影響的分析結果

> **Note**
>
> 您只能在初始分析迴圈完成後重新分類檔案。

內嵌檢視器和檔案比較

內嵌檢視器是大型主機 AWS 轉換功能中的一項功能，可提供兩個關鍵視覺化功能：

- 檔案檢視：從任務檢視所選舊版檔案的內容
- 檔案比較：side-by-side比較兩個舊版檔案的內容

輸入檔案檢視

若要在分析程式碼步驟中檢視您的檔案

- 在檢視程式碼分析結果下，使用清單中的核取方塊選取檔案。

  選擇檢視動作按鈕（選取 1 個項目時啟用）。

  檔案內容會在檔案檢視元件的畫面上呈現。

檔案比較

若要比較分析程式碼步驟中的檔案

1. 在檢視程式碼分析結果下，使用清單中的核取方塊選取兩個檔案。
2. 選擇比較動作按鈕（僅在選取 2 個項目時啟用）。
3. 檔案將在檔案比較元件中side-by-side顯示。

> **Note**
>
> 您無法選取兩個以上的檔案來比較檔案。

> **Important**
>
> 如果內嵌檢視器或檔案比較發生問題，請確定 S3 儲存貯體已正確設定。如需 S3 儲存貯體 CORS 政策的詳細資訊，請參閱 the section called “S3 儲存貯體 CORS 許可”。

資料分析

AWS 轉換提供資料分析，以協助了解資料關係和元素對大型主機現代化專案的影響。提供的兩個輸出為：

- 資料歷程：透過映射資料來源、任務和程式之間的關係，追蹤資料生命週期
- 資料字典：做為記錄舊版資料元素結構中繼資料的儲存庫

完成分析時，每個輸出都會有兩個索引標籤，然後針對資料歷程和字典提供以下所述的多個檢視。

> **Note**
>
> 當您請求資料分析時， AWS Transform 會執行程式碼分析，這是執行資料分析的必要項目。

資料沿襲

AWS 轉換會根據需要跨要現代化之程式碼庫了解的資料關係，提供多個檢視。資料譜系中可用的四個資料表檢視包括：

- 資料集：此檢視提供全面的影響分析，包括操作追蹤，以協助區分讀取、寫入、更新和刪除
- Db2 資料表：提供與 Db2 資料表和操作相關的影響分析
- Program-to-data：識別哪些 COBOL 程式參考每個資料集
- JCL-to-data的關係：識別哪些 JCL 指令碼參考每個資料集

摘要提供資料來源的概觀，以及其與程式和 JCLs的關係，以及有關如何利用資料來源的摘要資訊，以及在程式碼庫中找到的總操作。

資料字典

了解程式碼庫中存在之資料來源內的資料元素，是了解各種資料來源如何相依的下一個步驟。資料字典是一種資料目錄，提供具有商業語言描述的欄位層級中繼資料，以準確進行轉換映射。

- COBOL 資料結構：跨代碼庫中存在的 COBOL 複本和 INLINE 參考提供欄位資訊，包括欄位屬性和業務定義
- Db2 資料表：跨程式碼庫中存在的 Db2 資料表提供資料欄和資料表屬性，包括主索引鍵和外部索引鍵、結構描述和索引資訊，以及資料類型

選取資料來源，然後利用資料歷程或資料字典按鈕，以深入了解資料來源與資料元素之間的關係，即可取得資料歷程與字典之間的關係。資料譜系和字典之間的導覽提供整合的資料可見性與資料譜系，提供「什麼」 - 結構和意義，以及「哪裡」 - 用量和關係。

活動指標分析

活動指標分析可讓您分析類型 14、15、30、64、102 和 110 的系統管理設施 (SMF) 記錄。此分析可讓您深入了解如何在大型主機應用程式中使用 元素。它可協助淘汰未使用的程式碼，或決定現代化應用程式的目標架構。如果您在任務中包含活動指標分析，完成程式碼分析步驟會先提供更豐富的 SMF 輸出，但這不是必要的。

> **Note**
>
> 當您協商大型主機現代化的任務計畫時，完成程式碼分析和分解步驟會先提供更豐富的輸出。

加入 SMF 記錄進行分析

您必須在 Amazon S3 儲存貯體中提供 SMF 記錄位置，做為 SMF 分析的初始步驟。提供至少 13 個月的記錄，以擷取較短時間範圍可能遺漏的年度事件。雖然建議使用 13 個月，但任何具有可偵測 SMF 記錄的時間範圍都會產生分析結果。

您的 SMF 擷取必須符合下列格式要求：

- 包括類型 14、15、30 （ 子類型 5)、64、102 和 110。
- 使用 EBCDIC 格式的原始二進位檔案。
- 包含 RDW 位元組。

提供 Amazon S3 儲存貯體中 SMF 記錄的連結，確保記錄位於與原始程式碼分開的資料夾中。格式選項包括壓縮的 .zip （ 最多 600 MB) 或 .tar.gz （ 最多 5 GB)。如果您提供未偵測到 SMF 記錄的資料夾連結，您會收到錯誤訊息，而且沒有完成分析。

分析輸出

分析輸出包含兩個元件，取決於記錄類型：表格式檢視和 .csv 輸出 （ 可在 Amazon S3 儲存貯體中使用 ）。在 AWS 轉換中，顯示類型 30 和 110 的輸出。透過 Amazon S3 儲存貯體中的成品，您可以探索其他記錄類型的分析。在使用者介面中， 標頭會顯示所提供記錄的時間範圍，讓您可以識別任何遺失的金鑰日期。例如，如果您的記錄跨越 5 月 1 日至 10 月 31 日，但不包括感恩節後的忙碌一天，您可以看到金鑰記錄遺失。Web 應用程式中的時間戳記會反映系統的時區和 SMF 記錄。

Amazon S3 中可用的成品可提供所提供記錄中任何記錄類型的分析。

表格式檢視

表格式檢視僅適用於 SMF 30 和 110，包含批次任務和 CICS 交易最多三個主要元件：

- 摘要 – 提供關鍵任務和交易。
- 批次任務/CICS 交易分析 – 提供跨任務和交易的彙總分析。
- 程式碼分析比較（僅限批次）– 在 SMF 分析之前執行程式碼分析步驟時提供比較資料。

探索摘要提供三個任務和交易群組，可協助您快速識別項目以進行更深入的分析。

批次任務和 CICS 交易分析提供跨任務和交易的彙總分析。分析結果中的某些資料欄預設為隱藏。選擇齒輪圖示以顯示其他欄位。

交易金鑰會為 CICS 交易產生唯一的資料彙總，將四個欄位合併為單一金鑰值：

- 交易 ID
- 程式名稱
- SysPlex ID
- SysID

您可以依完整索引鍵或依分析輸出中索引鍵的任何元件進行搜尋。

程式碼分析比較會反白顯示 SMF 記錄或分析程式碼步驟中找到的任務，但不會同時出現在兩者中。這會顯示在您的 SMF 記錄時間範圍內未執行或不存在於分析程式碼步驟的任務。只有當您在任務中的 SMF 分析之前執行程式碼分析步驟時，才能使用此輸出。

最佳實務

若要取得批次任務的完整輸出（類型 30)，請確定您的 JCL 檔案名稱符合任務名稱，以在程式碼分析比較中取得有意義的輸出。

產生技術文件

您可以為正在進行現代化的大型主機應用程式產生技術文件。透過分析程式碼， AWS Transform 可以自動建立應用程式的詳細文件，包括舊版系統中存在的程式邏輯、流程、整合和相依性的描述。本文件功能有助於彌補知識差距，讓您在將應用程式轉換為現代雲端架構時做出明智的決策。

> **Note**
>
> 當您請求產生技術文件時， AWS Transform 會執行程式碼分析，包括程式碼相依性分析，這是產生文件所需的。

產生技術文件

1. 在左側導覽窗格的產生技術文件下，選擇選取檔案並設定設定。
2. 選取您要為其產生文件的 Amazon S3 儲存貯體中的檔案，然後在協作索引標籤中設定設定。

> **Note**
>
> 選取的檔案應具有相同的編碼類型（亦即，全部位於相同的 CCSID - UTF8 或 ASCII 中）。否則，產生的技術文件可能會有空白欄位或區段。

3. 選擇文件詳細資訊層級：
   - 摘要 – 提供範圍內每個檔案的高階概觀。此外， 會提供每個檔案的單行摘要。
   - 詳細功能規格 – 提供大型主機應用程式轉換範圍內每個檔案的完整詳細資訊。有些詳細資訊包括邏輯和流程、相依性、輸入和輸出處理，以及各種交易詳細資訊。

> **Note**
>
> 只能為 COBOL 和 JCL 檔案產生文件。

4. 選擇繼續。
5. 一旦 AWS 轉換產生文件，請遵循 主控台中產生和儲存結果的 Amazon S3 儲存貯體路徑來檢閱文件結果。
6. 產生文件後，您也可以使用 AWS 轉換聊天來詢問有關所產生文件的問題，並決定後續步驟。

將使用者資訊新增至文件

```
ARTIFACT_ID.zip
### app/
    ### File1.CBL
    ### File2.JCL
```

```
    ### subFolder/
    #   # File3.CBL
### glossary.csv
### pdf_config.json
### header-logo.png
### footer-logo.png
# ...
```

選用檔案可以新增到 zip 檔案中，以協助改善產生的文件品質，並提供自訂的 PDF 封面。其中一些可以是：

- glossary.csv 檔案：您可以選擇在 S3 儲存貯體的 zip 檔案中提供和上傳選用的詞彙表。詞彙表採用 CSV 格式。此詞彙表有助於根據客戶詞彙建立具有相關描述的文件。範例`glossary.csv`檔案看起來像：

  ```
  LOL,Laugh out loud
  ASAP,As soon as possible
  WIP,Work in progress
  SWOT,"Strengths, Weaknesses, Opportunities and Threats"
  ```

- pdf_config.json：您可以利用此選用組態檔案來產生符合其公司格式和標準的 PDF 文件，包括標頭、頁尾、標誌和自訂資訊。範例`pdf_config.json`看起來像：

  ```
  {
      "header": {
      "text": "Acme Corporation Documentation",
      "logo": "header-logo.png"
    },
    "customSection": {
      "variables": [
        {
          "key": "business Unit",
          "value": "XYZ"
        },
        {
          "key": "application Name",
          "value": "ABC"
        },
        {
          "key": "xxxxxxxxxx",
          "value": "yyyyyyyyyyyy"
        },
  ```

```
      {
        "key": "urls",
        "value": [
          {
            "text": "Product Intranet Site",
            "url": "https://example.com/intranet"
          },
          {
            "text": "Compliance Policies",
            "url": "https://example.com/policies"
          }
        ]
      }
    ]
  },
  "footer": {
    "text": "This document is intended for internal use only. Do not distribute
 without permission.",
    "logo": "footer-logo.png",
    "pageNumber": true
  }
}
```

- 標頭：
  - 對於封面 PDF 檔案，預設文字將是專案名稱。
  - 對於每個程式 PDF 檔案，預設文字將是程式名稱。
  - 沒有預設標誌。如果未設定標頭標誌，則不會顯示任何標誌。
  - 字型大小和標誌大小應根據單字數或標誌檔案大小動態變更。
- 自訂區段：
  - 如果未設定自訂區段，則會從 PDF 中省略它。
  - 連結必須能夠按一下。
- 頁尾：
  - 頁尾沒有預設的文字或標誌。
  - 除非另有明確設定，否則頁面號碼預設會顯示在頁尾中。
  - 字型大小和標誌大小應根據單字數或標誌檔案大小動態變更。

產生文件內嵌檢視器

您可以在產生技術文件步驟中檢視 PDF 檔案。

檢視 PDF 檔案

1. 導覽至檢閱文件結果索引標籤。
2. 在列出產生的 PDF 的資料表中找到 PDFs。
3. 選取 rile，然後選取檢視或選取覆蓋在檔案名稱上的連結元素。

PDF 會在 AWS 轉換中開啟，並可選擇展開右上角的畫面。

> **Note**
>
> AWS 轉換也可讓您下載所產生技術文件的 PDF 版本 XML。

> **Important**
>
> 如果文件內嵌檢視器發生問題，請確定 S3 儲存貯體已正確設定。如需 S3 儲存貯體 CORS 政策的詳細資訊，請參閱 the section called “S3 儲存貯體 CORS 許可”。

擷取商業邏輯

您可以從正在進行現代化的大型主機應用程式中擷取基本業務邏輯。 AWS Transform 會自動分析您的程式碼，以識別和記錄關鍵業務元素，包括詳細程序流程，以及內嵌在應用程式中的業務邏輯。此功能可在現代化旅程中為多個利益相關者提供服務。業務分析師可以利用擷取的邏輯來建立精確的業務需求，並識別目前實作中的差距或不一致。開發人員無需廣泛的大型主機專業知識，就能快速了解複雜的舊版系統功能。

> **Note**
>
> 當您請求業務邏輯擷取時。 AWS Transform 會執行程式碼分析，包括程式碼相依性和進入點分析，這些分析是執行業務邏輯擷取所需的。

擷取商業邏輯

1. 在左側導覽窗格的擷取商業邏輯下，選擇設定設定。
2. 在協同合作索引標籤中，選取您要如何擷取商業邏輯：
   - 應用程式層級：產生所有業務職能、交易、批次任務和檔案的業務文件。這會選取應用程式中的所有檔案。
   - 檔案層級：僅針對您從檔案資料表中選取的檔案產生商業文件。

   > **Note**
   >
   > - 對於任一選項，您可以選取包含詳細的功能規格，以便 AWS 轉換包含所選檔案的控制流程和全面的業務規則。
   > - 選取的檔案應具有相同的編碼類型（亦即，全部都在相同的 CCSID - UTF8 或 ASCII 中）。否則，產生的文件可能會有空白欄位或區段。
   > - 只能為 COBOL 和 JCL 檔案產生文件。
   > - 對於應用程式層級，CICS 交易和批次任務所使用的程式會分組在一起，而所有其他程式則會分類為未指派。
3. 選擇繼續。
4. 一旦 AWS 轉換擷取商業邏輯，它會以 JSON 格式將結果存放在 Amazon S3 儲存貯體中，以便您可以線上檢視。

> **Note**
>
> 產生的業務規則檔案數目可能大於您的初始選擇。某些選取的檔案可能會觸發業務規則擷取，以包含其他相依檔案，這些檔案也會出現在結果表格中。

內嵌檢視擷取的業務文件

您可以在擷取業務規則步驟中檢視業務邏輯。若要這樣做，

1. 導覽至檢閱業務邏輯擷取結果。
2. 從資料表中選取您要檢視的文件，然後按一下檢視結果按鈕。

商業文件頁面會在新的瀏覽器索引標籤中開啟。

分解

您可以將程式碼分解為考量程式和元件之間相依性的網域。這有助於相關檔案和程式在相同網域中適當分組。它也有助於在分解過程中維護應用程式邏輯的完整性。

> **Note**
>
> 當您請求分解時， AWS Transform 會執行程式碼分析，包括執行分解所需的程式碼相依性分析。我們也建議您在分解之前執行商業邏輯擷取，以獲得更好的結果。

若要開始分解您的應用程式：

1. 從左側導覽窗格中選取分解程式碼。

   > **Note**
   >
   > 系統會自動為與網域無關的所有檔案建立未指派的網域。在初始導覽時，所有檔案都應與未指派相關聯，除非從應用程式層級商業邏輯擷取提出網域。

2. 透過動作功能表建立新網域，然後選擇建立網域。
3. 在建立網域中，提供網域名稱、選用描述，並將某些檔案標記為種子。
   - CICS 設定檔案 (CSD) 和排程器設定檔案 (SCL) 可用於自動種子偵測。
   - 您也可以將一個網域設定為常見元件。此網域中的檔案常見於多個網域。
4. 選擇建立。

   > **Note**
   >
   > 您可以建立多個網域，並以不同的檔案做為種子。

5. 確認所有網域和種子之後，請選擇分解。
6. AWS 轉換會檢查原始程式碼檔案，然後使用具有類似使用案例和高程式設計相依性的程式和資料集分解為網域。

   AWS 轉換可讓您以表格式和圖形檢視分解的網域做為相依性。圖形檢視有三個選項：

   - 網域檢視 – 可以檢視不同的網域如何以視覺化格式相互關聯。

- 相依性檢視 – 可以將每個網域中的所有檔案檢視為複雜的相依性圖表。如果新增至網域的節點未從相同網域中的種子接收資訊，則此節點會預測為未指派（節點未接收任何資訊）、中斷連線（子圖表中未接收種子資訊）或另一個網域（節點至少從該網域接收資訊）。
- 子圖檢視 - 使用者可以建立子圖以視覺化節點子集，以更清楚地了解節點集合的關係影響和界限。
  - 若要建立子圖，請選取一組節點，然後從工具列中選取擷取子圖選項
  - 除了您要合併的兩個子圖之外，還建立合併新的第三個子圖時，可以使用合併子圖。

> **Note**
>
> 如果您不喜歡目前的網域結構，請重複這些步驟來新增更多網域，或重新設定已使用不同種子集建立的網域。

7. 完成後，選擇繼續。

種子

種子是分解程式碼階段的基礎輸入。每個元件或檔案（例如 JCL、COBOL、Db2 資料表、CSD 和排程器檔案）只能指派為一個網域的種子，以確保分解程序期間的邊界清晰且一致性。

種子的識別取決於應用程式或產品組合的結構。在典型大型主機舊版應用程式中，種子通常可以透過遵守已建立的命名慣例、排程器中的批次層級分組，以及 CICS 系統中定義的交易層級分組來確定。此外，資料庫資料表也可以做為種子，為分解提供另一層結構。

匯入和/或更新相依性檔案

在分解期間，您可以上傳相依性的 JSON 檔案，以取代 AWS Transform 執行的相依性分析所產生的現有檔案。

匯出相依性函數可讓您下載分解步驟中產生的相依性 json 檔案。下載之後，您可以根據您的需求修改檔案。然後，您可以使用 AWS 轉換的上傳功能匯入相依性，這可讓您上傳相依性的新 JSON 檔案，以取代相依性分析產生的檔案。之後，分解步驟中的圖形將會更新。

匯出、修改和匯入相依性

1. 在檢視分解結果頁面上，選擇動作。
2. 在下拉式清單中，選擇其他動作下的更新相依性檔案選項。
3. 在更新相依性檔案模態中，

a. 下載從現有分析結果建立的相依性檔案 AWS 轉換。
b. 在下載的檔案中，根據您想要達成的目標修改相依性。
c. 修改後，使用上傳相依性檔案按鈕儲存和上傳此檔案。

> **Note**
>
> 唯一接受的檔案格式是 JSON 檔案。

4. 接著，選擇匯入。

AWS 轉換會匯入相依性檔案，並根據您的輸入建立新的相依性圖表。

匯入和/或更新網域

對於在分解步驟之前映射網域、種子和/或檔案關係的客戶，您可以透過動作功能表提供的匯入網域檔案函數上傳此網域定義。可以使用此函數的一些範例：

- 從另一個任務引入轉送分解
- 提供此映射的主題專家

匯入網域檔案後，使用者可以對網域定義執行分解，如果滿足，則可以儲存然後提交網域定義。

Parent/child/neighbor檔案

在相依性圖表中，程式透過不同類型的連線彼此關聯。了解這些關係可協助您在大型主機應用程式的轉換期間分析程式相依性。它也有助於了解網域的邊界。例如，如果您選取網域，然後選取父層級，則會顯示連接的節點。

父系關係 – 父系檔案呼叫或控制其他程式。父系位於階層中其相依程式的上方。您可以在一個層級或所有層級選取父系。

子系關係 – 子系檔案由父系程式呼叫或控制。子系位於檔案階層中父系下方。

鄰關係 – 鄰是相同階層層級的檔案。他們共用相同的父系程式，並且可能會直接彼此互動。

重新建構程式碼

Reforge 使用大型語言模型 (LLMs) 來改善重構程式碼的品質。初始 COBOL-to-Java 轉換會保留功能等效性，同時保留舊版系統中 COBOL 影響的資料結構和變數名稱。Reforge 會重組此程式碼，以遵循

現代 Java 實務和模式，將 COBOL 樣式的建構取代為原生 Java 集合和命名慣例。這可讓 Java 開發人員更易於讀取和維護程式碼。

> **Note**
>
> 重新建構的配額為：
>
> - 每個任務 3，000，000 行程式碼
> - 每位使用者每月 50，000，000 行程式碼

請依照下列步驟，在重構後重新強化程式碼：

1. 在左側導覽窗格中選擇重新編碼 Java 程式碼，然後選取設定程式碼重新編碼。
2. 將 S3 位置提供給壓縮的可建置來源專案，然後選擇繼續。使用此 zip 結構：

   ```
   input.zip
           ### PROJECT-pom
           ### PROJECT-entities
           ### PROJECT-service
           ### PROJECT-tools
           ### PROJECT-web (optional)
           ### pom.xml
   ```

   AWS Transform 會分析您的 zip 套件，以尋找 PROJECT-service 目錄中的檔案，以便提供可選取的類別清單，供您重新建構。這些類別的尾碼為 `ProcessImpl.java`。
3. 完成選取要重新建構的類別頁面，然後選擇繼續。追蹤 Worklog 標籤上的重新強化狀態。
4. 在檢視結果頁面上檢視已完成的重新建構的結果，其中會顯示每個類別的重新建構狀態。它也會指定在 S3 儲存貯體中尋找 Reforge 結果的位置。

AWS 轉換從您取得此輸入後，就會為您提供可下載的檔案，其中包含 Reforge 結果。

這是成功重新建構所產生的 zip 結構：

```
reforge.zip
### maven_project
### reforge.log
###tokenizer_map.json
```

- maven_project 包含強化來源碼。
  - 已重構但未成功完成編譯的檔案位於 `/src/main/resources/reforge/originalClassName.java.incomplete`，並命名為 `originalClassName.java.incomplete`。將這些檔案與原始版本的檔案進行比較，以選擇您要儲存的強化功能。
  - 提供給 AWS 轉換且已成功重構的來源檔案會備份至 ，`src/main/resources/reforge/originalClassName.java.original`並命名為 `originalClassName.java.original`。檔案的重構版本會取代提供給 AWS Transform 的來源檔案。

> **Note**
>
> 只有在強化程序成功時，才會將`originalClassName.java`檔案取代為強化檔案。否則，它們會保留原始內容。

- reforge.log 包含可用於診斷任務失敗的日誌，或在發生問題 AWS 時提供支援的日誌。
- tokenizer_map.json 包含權杖 IDs 與資料的映射，例如檔案路徑和類別/方法名稱，這些名稱會在日誌中權杖化，以保護隱私。您可以在發生問題時提供此檔案 AWS 以支援 。

規劃您的現代化應用程式測試

您可以根據擷取的程式碼屬性、任務複雜性和排程器路徑，為大型主機現代化應用程式建立和管理測試計畫。 AWS Transform 有助於排定要測試哪些任務的優先順序，並識別每個測試案例所需的特定成品。測試規劃程序分為三個主要階段：組態、範圍和檢閱。

建立測試計畫

1. 設定測試計畫設定
   a. 在左側導覽窗格的規劃測試下，選擇設定設定。
   b. （選用）為您的商業邏輯擷取 (BLE) 提供 S3 路徑。這些成品可增強測試計畫品質。如果沒有 BLE 成品，測試計畫中的某些欄位可能會保持不完整。
2. 定義測試計畫範圍
   a. 選取要包含在測試計畫中的進入點，例如批次任務。
   b. 根據多個屬性篩選和排序任務：
      - 商業函數（擷取自 BRE BLE)

- 網域（從分解階段）
- 檔案路徑和位置
- 自訂搜尋條件

c. 選取個別任務或整個群組進行測試。

d. 檢閱任務關係和相依性。

3. 檢閱和調整測試計畫

產生的測試計畫提供完整資訊，包括：

- 根據相依性偏好的執行順序
- 來自排程器的任務群組指派
- 複雜性分數，這是測試案例的彙總分數
- 商業網域關聯
- 循環複雜度指標
- 資料集和資料表相依性
- 程式碼指標行
- 商業函數映射

測試計畫自訂選項

您可以自訂您的測試計畫，以滿足特定需求。例如，您可以：

- 選取多個進入點以建立新的測試案例
- 合併現有的測試案例以結合相關功能
- 分割測試案例以進行更精細的測試
- 移除不必要的測試案例
- 新增或移除現有測試案例的進入點
- 修改測試案例描述和屬性
- 調整執行順序

詳細的測試案例資訊

每個測試案例都提供描述其內容和相關資料集或資料檔案的詳細資訊：

- 測試範圍的完整描述
- 包含的進入點完整清單
- 顯示複雜性和大小的彙總指標
- 商業規則和自動化測試案例指引
- 具有方向的資料集和資料表相依性（輸入/輸出）
- 互動式相依性圖表視覺化
- 執行先決條件和要求

資料管理功能

這些詳細資訊可協助您了解與測試案例相關的資料。您可以：

- 依輸入/輸出方向篩選資料集
- 識別測試執行所需的成品
- 追蹤測試案例之間的資料相依性
- 監控跨測試計畫的資料集用量

> **Note**
>
> AWS 轉換會自動分析排程器相依性，並指派複雜性分數，以協助排定測試工作的優先順序。較高的複雜性分數表示在測試過程中可能需要更徹底測試或隔離的任務。

業務規則和測試案例指引

AWS 轉換測試計畫會根據業務規則擷取，為您的測試案例計畫提供建議：

- 使用 LLM 自動處理業務規則
- 產生合成測試案例
- 特定商業案例的測試指引
- 規則和測試案例之間的可追蹤性

最終測試計畫會存放在指定的 S3 位置，並包含所有必要資訊，以有效執行您的測試策略。您可以匯出測試計劃，以與其他測試工具或文件系統整合。

> **Note**
>
> 提供綜合測試案例指引時，必須根據指引單獨建立實際的測試成品。測試計畫可做為測試策略的完整藍圖，但不會產生測試資料或執行指令碼。

測試案例建立規則 - 摘要

一般規則

- 測試案例以排程執行順序包含 1 到多個 JCLs
- 測試案例是從有效的支援排程器 (CA7 和 Control-M) 建立的
- 測試會執行 JCLs，而非排程器本身或排程任務
- 排程任務是唯一的，而且只會執行一個 JCL
- 一個 JCL 可由多個排程任務執行
- 一個 JCL 可以存在而不處於排程中

預設測試案例建立規則

- 如果測試案例中有單一 JCL：
  - JCL 不涉及排程
  - JCL 是由分散到多個分支的排程任務執行
  - 排程中的分支僅包含此 JCL
- 如果測試案例中有多個 JCL： 代表排程分支內的線性執行路徑序列
- 如果 JCL 正在進行不同的排程任務：JCL 會成為自己的個別測試案例
- 如果 JCL 正在進行收斂排程任務：JCL 可以啟動新的測試案例，但不會包含在先前的分支中
- 略過缺少JCLs 並繼續執行 （計劃未來增強功能，以在缺少 JCL 點時剪下測試案例）

使用者操作規則

- 建立測試案例：使用者從可用的 JCLs 選取
  - 如果排程執行分支序列中存在 JCLs則成功
  - 遵循排程執行順序
- 將 JCL 新增至測試案例：使用者從可用的 JCLs 選取

  - 如果測試案例的排程執行分支/路徑中可以存在 JCL，則成功
- 從測試案例移除 JCL：使用者可以從測試案例移除任何 JCL
  - 即使造成執行路徑差距，也允許
- 合併測試案例：使用者選取要合併的兩個測試案例
  - 如果 JCLs可以同時存在於相同的排程執行分支中，就會成功
  - 維護排程執行順序
- 分割測試案例：使用者在分割的測試案例中選取一個 JCL
  - 從分割點向前建立新的測試案例
  - 原始測試案例已修改，以排除超過分割點JCLs
- 刪除測試案例：使用者可以刪除任何建立的測試案例

> **Note**
>
> 您無法從不同的排程器分支/路徑建立、新增或合併測試案例。未來的增強計劃允許排程器中差異/彙整任務以外的操作。

產生測試資料收集指令碼

您可以產生 JCL 指令碼，根據上一個步驟中建立的測試計畫，從大型主機系統收集測試資料。 AWS Transform 會自動建立資料集、資料庫資料表和序列檔案的資料收集指令碼，以進行全面測試。資料收集程序分為四個主要階段：輸入組態、測試案例選擇、指令碼組態和指令碼產生。

產生測試資料收集指令碼

1. 提供測試計畫輸入
   a. 在左側導覽窗格的測試資料收集下，選擇提供測試計畫輸入。
   b. 從規劃現代化應用程式測試中，指定測試計畫 JSON 檔案的 S3 路徑。
   c. 如果在上一個任務步驟中產生測試計畫，則輸入欄位會預先填入。
   d. 您也可以指定適當的 S3 位置，從其他任務中選取測試計畫。
2. 選取資料收集的測試案例
   a. 檢閱測試計畫中測試案例的完整清單。
   b. 根據多個屬性篩選和排序測試案例：

- 商業函數和網域
- 資料庫資料表相依性
- 資料集需求
- 複雜性指標
- 自訂搜尋條件

c. 選取個別測試案例或使用大量選取選項。

d. 按一下一個測試案例以查看詳細資訊，以檢閱測試案例詳細資訊，包括進入點、指標和業務規則。

3. 設定資料收集指令碼

a. 下載範例範本和組態檔案以供參考。

- AWS Transform 提供 Db2 資料庫卸載、VSAM 檔案 REPRO 和循序資料集處理的範例範本，做為程序預期範本類型的指引。
- 標準可能因網站而異，因此預期客戶會修改或取代這些範本，以符合自己的標準。
- 這些修改後的範本需要上傳至測試資料收集可以處理它們的 S3 儲存貯體。

b. 提供變數組態檔案 (JSON 格式），其中包含：

- 使用者字首和環境特定的常數
- 資料庫組態參數
- 目的地端點設定和資料傳輸參數
- 使用者定義並用於 JCL 範本的其他必要參數

c. 上傳不同資料收集方法的 JCL 範本：

- Db2 範本：用於資料庫資料表卸載 （針對 BMC、IBM DSN 或其他卸載公用程式自訂）
- VSAM 範本：用於 VSAM 檔案處理 （通常使用 REPRO 公用程式）
- 循序資料集範本：用於處理循序資料集、分割資料集、GDGs等。

4. 檢閱和管理產生的指令碼

產生的指令碼提供全面的資料收集功能，包括：

- 分隔「之前」和「之後」測試執行資料收集的指令碼
- 依測試案例和資料類型排列的指令碼結構
- 指令碼會自動存放在 S3 儲存貯體中，以便輕鬆存取和傳輸

- 產生的 JCL 指令碼已準備好執行大型主機
- 變數替換是根據範本中定義的使用者組態

指令碼產生功能

產生的指令碼會根據您的範本和組態自動自訂：

- 範本型產生：使用您提供的 JCL 範本搭配變數替換
- 環境：納入您的特定大型主機組態
- 資料類型處理：為循序資料集、VSAM 檔案和資料庫資料表建立適當的指令碼
- 測試案例的集合：產生「之前」和「之後」的資料收集指令碼
- 循序資料集處理： AWS 提供的範例提供檔案傳輸函數，但可自訂為您站點可用的壓縮公用程式，或 Connect Direct 或受管檔案傳輸等公用程式。

資料收集策略

產生的指令碼支援全面的資料收集策略：

- 循序資料集收集：適用於 VSAM 和一般檔案的 REPRO 和複製公用程式
- 資料庫資料表卸載：可自訂的 Db2 卸載程序
- 循序資料集處理：可自訂循序資料集的後續處理，例如壓縮、受管檔案傳輸服務等。
- 相依性管理：根據測試案例定義協調集合

> **Note**
>
> AWS 轉換會根據您的範本和組態產生指令碼。在大型主機環境上執行之前，請檢閱所有產生的 JCL，以確保與您的特定系統組態和安全性需求相容。

範本自訂和最佳實務

ATX 測試資料收集提供靈活的範本自訂功能：

- 多重公用程式支援：針對不同的大型主機公用程式 (BMC、IBM、DSN) 調整範本
- 變數驅動組態：針對環境特定參數使用常數
- 可重複使用的範本：建立標準化範本以產生一致的指令碼

- 資料處理：納入組織特定的資料處理需求
- 安全整合：包含適當的安全與存取控制
- 效能最佳化：設定 以實現高效的資料收集和傳輸

產生的輸出結構

產生的指令碼會在 S3 儲存貯體中組織，結構如下：

- 測試案例組織：依相關測試案例分組的指令碼
- 收集時間：針對「之前」和「之後」資料收集分隔資料夾
- 資料類型分類：依循序資料集、資料庫資料表和傳輸整理的指令碼
- 中繼資料檔案：摘要資訊和執行指引
- Ready-to-transfer格式：針對直接大型主機部署格式化的 JCL

最終指令碼集合會存放在指定的 S3 位置，並包含所有必要的 JCL，以有效執行您的資料收集策略。您可以下載要傳輸至大型主機環境的指令碼，或與自動化部署程序整合。

> **Note**
>
> 產生完整的 JCL 指令碼時，必須在大型主機環境上執行實際執行。指令碼可做為ready-to-use資料收集工具，但需要適當的大型主機存取和執行許可。

測試自動化指令碼產生

您可以產生測試自動化指令碼，根據上一個步驟中建立的測試計畫，在現代化應用程式上執行測試案例。 AWS 轉換會自動建立全面的測試指令碼，利用從測試資料收集程序收集的資料。測試自動化指令碼產生程序包含三個主要階段：輸入組態、測試案例選擇和指令碼產生結果。

產生測試指令碼

1. 提供測試計畫輸入

   a. 在左側導覽窗格的測試自動化指令碼產生下，選擇提供測試計畫輸入。
   b. 從規劃現代化應用程式測試中，指定測試計畫 JSON 檔案的 S3 路徑。
   c. 如果在上一個任務步驟中產生測試計畫，則輸入欄位會預先填入。
   d. 您也可以指定適當的 S3 位置，從其他任務中選取測試計畫。

e. 系統會使用此測試計畫做為產生自動化指令碼的基礎。

2. 選取測試案例以產生指令碼

a. 檢閱測試計畫中測試案例的完整清單。

b. 根據多個屬性篩選和排序測試案例：

- 商業函數和網域
- 資料庫資料表相依性
- 資料集需求
- 複雜性指標
- 自訂搜尋條件

c. 選取個別測試案例，或使用大量選擇選項搭配全部勾選和全部取消勾選按鈕。

d. 按一下個別測試案例，檢閱測試案例詳細資訊，包括進入點、指標和業務規則。

選取的測試案例將產生自動化指令碼，以便在現代化應用程式上執行。

3. 檢閱和管理產生的測試自動化指令碼：

- 系統會顯示成功訊息，確認指令碼產生完成。
- 產生的測試指令碼會自動存放在您指定的 S3 儲存貯體位置。
- 使用各自的 S3 位置存取產生的測試指令碼的完整清單。
- 每個測試案例都有存放在個別 S3 位置的對應自動化指令碼。
- 指令碼已準備好在現代化應用程式環境中進行部署和執行。

測試自動化指令碼功能

產生的自動化指令碼提供全方位的測試功能：

- 現代化應用程式測試：指令碼專為在轉換的應用程式上執行測試案例而設計
- 資料整合：利用從先前測試資料收集步驟收集的測試資料，這些資料需要複製到每個測試案例的資料夾
- 自動化執行：指令碼可用來設定資料接收器、執行測試案例和比較結果，某些參數必須根據您的部署環境進行設定
- 組織化結構：指令碼是依 S3 儲存貯體中的測試案例系統化組織
- Ready-to-deploy的格式：指令碼已格式化，可直接部署到您的測試環境

產生的輸出結構

產生的測試自動化指令碼會在 S3 儲存貯體中組織，結構如下：

- 測試案例組織：每個測試案例都有儲存在個別 S3 資料夾中的專用指令碼
- 可立即執行的格式：指令碼經過格式化，以便在根據您的環境設定一些變數之後立即部署和執行
- 集中存取：所有指令碼都可以從單一 S3 儲存貯體位置存取，以便輕鬆管理

測試執行策略

產生的指令碼支援完整的測試執行工作流程：

- 環境設定：指令碼包含設定初始資料以執行測試的功能
- 資料準備：與測試案例資料收集步驟中收集的測試資料整合
- 測試案例執行：在現代化應用程式上自動執行個別測試案例
- 結果比較：用於比較測試結果和驗證應用程式行為的內建功能

> **Note**
>
> AWS 轉換會根據您的測試計畫和選取的測試案例產生測試自動化指令碼。指令碼專為在現代化應用程式環境中執行而設計，並利用上一個步驟中收集的測試資料。在部署之前檢閱所有產生的指令碼，以確保與您的特定應用程式組態和測試需求相容。

測試自動化的最佳實務

- 環境驗證：確保您的現代化應用程式環境在指令碼執行之前已正確設定
- 資料驗證：驗證收集階段所需的測試資料是否可用且可存取
- 指令碼自訂：根據您的特定測試需求，視需要檢閱和自訂產生的指令碼
- 執行監控：在測試指令碼執行期間實作適當的監控和記錄
- 結果分析：建立分析測試結果和識別應用程式問題的程序

測試自動化指令碼的最終集合提供完整的測試架構，以驗證您的現代化應用程式功能。指令碼可以整合到您的持續測試程序中，或在應用程式驗證工作流程中執行。

AWS 轉換中的部署功能

AWS 轉換透過提供ready-to-use基礎設施即程式碼 (IaC) 範本，協助您為現代化大型主機應用程式設定雲端環境。透過 AWS 轉換聊天介面，您可以存取預先建置的範本，以建立運算資源、資料庫、儲存和安全控制等基本元件。範本提供熱門格式 AWS Cloud Development Kit (AWS CDK)，包括 CloudFormation (CFN) 和 Terraform，讓您靈活部署基礎設施。

這些範本可做為建置區塊，減少為現代化大型主機應用程式設定環境所需的時間和專業知識。您可以自訂這些範本以符合您的需求，為您提供建置部署環境的基礎。

若要擷取 IaC 範本，請在 Infrastructure-as-Code 範本的 AWS 轉換聊天中詢問 ，以釐清您偏好的現代化模式 （例如大型主機重構 AWS 轉換）、您偏好的拓撲 （獨立與高可用性），以及您偏好的格式 (CloudFormation 與雲端開發套件與 Terraform)。

重構後建置和部署現代化應用程式

使用 AWS Transform 完成重構程序後，您可以建置和部署現代化 Java 應用程式。本指南會逐步引導您擷取現代化程式碼、設定您的環境，以及部署和測試您的應用程式。

> **Note**
>
> 除了此處提供的指引之外， AWS 轉換產生的程式碼套件還將包含設定 AWS 自動重構開發環境文件，提供使用開發人員執行期設定 IDE （整合式開發環境） 的說明。

主題

- 先決條件
- 步驟 1：擷取現代化程式碼
- 步驟 2：建置現代化應用程式
- 步驟 3：設定測試環境
- 步驟 4：部署現代化應用程式
- 步驟 5：測試現代化應用程式
- 其他範例

先決條件

開始之前，請確定您已：

- 使用 AWS Transform 成功完成重構任務。
- 存取您的現代化程式碼。
- 在開發機器上安裝和設定的建置軟體工具堆疊，例如 Apache Maven 或 Apache Tomcat。如需執行期版本控制的詳細資訊，請參閱AWS 轉換大型主機執行期版本備註。
- 安裝並設定 Amazon Corretto 或 Java 執行時間版本。如需安裝 Amazon Corretto 的詳細資訊，請參閱 Amazon Corretto 24。
- 視需要存取 以建立和設定 Runtime 元件的 Amazon Aurora PostgreSQL 資料庫。如需建立 Aurora PostgreSQL 資料庫的詳細資訊，請參閱使用 Amazon Aurora PostgreSQL。
- 將應用程式部署到您的執行期環境的管理存取權。
- 已檢閱AWS 大型主機執行期概念的轉換，了解使用 AWS 自動化重構解決方案進行現代化之應用程式的基本概念。

步驟 1：擷取現代化程式碼

擷取現代化程式碼

1. 下載並擷取產生的程式碼套件。
2. 開啟 `codebase/app-pom/pom.xml` 並記下所需的執行期引擎版本。例如 `<gapwalk.version>4.6.0</gapwalk.version>`。
3. 從下載的程式碼套件中找到設定 AWS 自動重構開發環境文件以供參考。

步驟 2：建置現代化應用程式

建置現代化應用程式

1. 從大型主機的 AWS 轉換工具箱存取執行期。
2. 在本機開發機器上下載並安裝適當的執行時間版本（在 中識別the section called “步驟 1：擷取現代化程式碼”）。

   > **Note**
   >
   > 如需在本機電腦上安裝執行時間相依性的其他資訊，請參閱「設定 AWS 自動重構開發環境」文件的第 3.1 節。

3. 開啟命令提示字元並導覽至應用程式的根目錄。

4. 若要為現代化應用程式建置可部署套件，請執行 Maven build 命令：

```
mvn package
```

如需現代化程式碼的基本組織詳細資訊，請參閱應用程式組織頁面。例如，對於包含前端 Web 應用程式的現代化應用程式，除了執行期元件之外，您可能至少預期下列可部署.war彙總：

- 服務專案：包含傳統商業邏輯現代化元素

```
<business-app>-service.*.war
```

- Web 專案：包含使用者界面相關元素的現代化

```
<business-app>-web.*.war
```

步驟 3：設定測試環境

設定您的測試環境

1. 設定您的現代化應用程式執行時間。如需詳細資訊，請參閱AWS Mainframe Modernization 《使用者指南》中的設定執行期組態一節。

> **Note**
>
> 如需執行時間元件特定組態範例， AWS 請參閱「設定自動重構開發環境」指南的第 5 節。

2. 為現代化應用程式準備輸入和輸出 (I/O) 資料集。現代化應用程式可能會處理循序 I/O 資料集、VSAM 資料集或其他項目。

> **Note**
>
> 如需範例，請參閱設定 AWS 自動重構開發環境的第 6 節。

3. 執行期環境 - 您可以使用現有的執行期環境或建立新的執行期環境。
   - 若要設定非受管執行期環境，請參閱設定非受管應用程式。
   - 若要設定受管執行期環境，請參閱設定受管應用程式。

設定測試環境後，您會移至部署現代化應用程式的下一個步驟。

步驟 4：部署現代化應用程式

在您建立和/或在 the section called “步驟 2：建置現代化應用程式”和 the section called “步驟 3：設定測試環境”區段中設定的執行時間中部署應用程式成品。

您可以使用下列連結找到部署現代化應用程式的其他指引：

- 在 Amazon EC2 上部署
- 在 Amazon ECS 和 Amazon EKS 上的容器上部署
- 建立 AWS Mainframe Modernization 應用程式

步驟 5：測試現代化應用程式

部署之後，

1. 檢閱可用的執行期 APIs，了解如何與現代化應用程式互動。
2. 測試您的應用程式，使其功能等效性與舊版應用程式保持一致。例如，請參閱《 AWS Mainframe Modernization 使用者指南》中的測試範例應用程式。

其他範例

如需使用 AWS Transform 現代化大型主機應用程式的特定範例，請參閱現代化 CardDemo 大型主機應用程式。

全堆疊 Windows 現代化

AWS 轉換提供完整堆疊的 Windows 現代化，包括 .NET 現代化和 SQL Server 現代化。

適用於 .NET 的 AWS Transform 代理程式可協助您將 .NET 應用程式現代化為與跨平台 .NET 相容。您可以使用 .NET Web 應用程式或 .NET IDE 來現代化 .NET。

AWS Transform for SQL Server 現代化是一項採用 AI 的服務，可將 Microsoft SQL Server 資料庫及其相關聯 .NET 應用程式的完整堆疊現代化自動化至 Amazon Aurora PostgreSQL。此服務協調從結構描述轉換、資料遷移和修改應用程式程式碼以符合新目標 PostgreSQL 的整個遷移旅程，透過自動化複雜且耗費大量人力的任務，讓您的團隊更具生產力。

主題

- 使用 AWS 轉換現代化 .NET
- SQL Server 現代化

使用 AWS 轉換現代化 .NET

適用於 .NET 的 AWS Transform 代理程式可協助您將 .NET 應用程式現代化為與跨平台 .NET 相容。此功能稱為 .NET 現代化。在 AWS 轉換AWS 轉換環境中，您可以建立 .NET 現代化轉換任務。

體驗

AWS 轉換提供多種體驗：

- Web 主控台：一次可大規模轉換最多 500 個儲存庫。
- Visual Studio IDE：開發人員主導的解決方案或專案轉換，以互動和反覆方式與客服人員搭配使用。建議用於中大型專案。

您可以在 Web 主控台和 IDE 之間自由切換，以處理轉換任務。

您也可以從其他 IDEs 和 AI 程式碼配套叫用 AWS 轉換：

- Kiro：使用 Transform for Kiro 電源從 Kiro AWS 轉換。
- 其他 AI 程式碼搭配：使用 Transform MCP 代理程式從您偏好的 AI 編碼助理 AWS 轉換。

功能和主要功能

- 從來源控制系統分析 .NET Framework 程式碼庫，其中包括私有 NuGet 支援、識別跨儲存庫相依性，以及提供分析報告。
- 將舊版 .NET Framework 應用程式自動轉換為跨平台 .NET、電子郵件通知和轉換摘要報告。
- 輕鬆與來源控制平台 (BitBucket、GitHub 和 GitLab) 整合，以擷取現有程式碼並將轉換後的程式碼遞交至新的分支。
- 透過單元測試驗證轉換的程式碼。

支援的版本和專案類型

AWS 轉換支援這些 .NET 版本的轉換：

- .NET Framework 3.5+
- .NET Core 3.1
- .NET 5.x+
- .NET 8

AWS 轉換可以轉換為這些目標 .NET 版本：

- .NET 8
- .NET 10

AWS 轉換支援轉換這些類型的專案 （僅限 C#)：

- 類別程式庫
- 主控台應用程式
- https：//ASP.NET：
  - 模型檢視控制器 (MVC)，包括前端 Razor 檢視
  - 單頁應用程式 (SPA) 後端 （業務邏輯層）
  - Web API
  - Web 表單
- 單元測試專案 (NUnit、xUnit 和 MSTest)
- Windows 通訊基金會 (WCF) 服務

- 具有第三方或私有 NuGet 套件所提供跨平台版本的專案。如果跨平台對等項目遺失或無法使用，AWS Transform for .NET 將嘗試盡最大努力進行轉換。

AWS 轉換也可以將下列專案類型轉換為現代 .NET。這是預覽功能，而且可能不會完全轉換為支援的專案類型。

- WinForms 桌面專案。
- WPF 桌面專案。
- Xamarin 行動專案。
- 以 VB.NET 撰寫的專案。

限制

如需 AWS 轉換配額和限制的詳細資訊，請參閱 AWS 轉換的配額。

AWS 轉換不會轉換下列項目：

- Blazor UI 元件
- 沒有核心相容程式庫的 Win32 DLLs
- 不包含任何解決方案的儲存庫。

AWS 轉換不會修改原始儲存庫分支，而且只能寫入轉換計劃中指定的個別目標分支。

人工介入

在將 .NET Framework 應用程式移植到跨平台 .NET 期間，您可能需要在下列情況下提供輸入或核准：

- 設定原始程式碼和許可的連接器
- 驗證提議的現代化計劃
- 上傳缺少的套件相依性做為 NuGets
- 檢閱並接受轉換後的程式碼

其他資訊

您可以使用 AWS Transform Web 應用程式或 AWS Toolkit for 來現代化 .NET 程式碼Visual Studio。

- 使用 AWS Transform Web 應用程式現代化您的 .NET 程式碼
- 在 IDE 中現代化 .NET
- .NET 轉換的最佳實務

使用 AWS Transform Web 應用程式現代化您的 .NET 程式碼

AWS Transform for .NET 是新的生成式 AI 驅動代理程式，旨在現代化舊版 .NET 應用程式。您可以使用 AWS Transform Web 應用程式或 Visual Studio AWS Toolkit 擴充功能來現代化舊版 .NET 程式碼。

若要使用 AWS 轉換 Web 應用程式來現代化 .NET 程式碼，請導覽至 Web 應用程式，並遵循以下詳細步驟：

1. 建立 AWS Transform .NET 任務計畫
2. 建立原始程式碼儲存庫連接器
3. 確認您的儲存庫以準備進行轉換
4. 解決套件相依性以準備轉換
5. 檢閱您的計劃以準備轉型
6. 轉換您的 .NET 程式碼

建立 AWS Transform .NET 任務計畫

建立工作區後，在任務索引標籤上，選取建立任務。然後，遵循聊天窗格中使用自然語言 AWS 轉換的提示。這些是建立 .NET 現代化任務的典型步驟。

1. AWS 轉換會詢問您要建立的轉換任務類型。在聊天中，輸入 .NET 現代化。
2. AWS 轉換會建議任務名稱，並詢問您是否要變更任務名稱。如果您想要變更任務名稱，請指示以自然語言 AWS 轉換，例如，將任務名稱變更為 ExampleCorpDotNet1。否則，您可以在聊天中接受建議的任務名稱。接受任務名稱後， AWS Transform 會在聊天視窗中通知您正在建立任務。
3. AWS 轉換會建立轉換任務。

AWS Transform .NET 任務計畫的元件

AWS 轉換 .NET 任務顯示有 5 個標籤，您可以從最左側的垂直圖示中選取：任務、儀表板、核准、成品和工作日誌。每個索引標籤都有一個左側窗格和中央聊天窗格。右側協作窗格有時可能會出現，以顯示其他詳細資訊並請求人工輸入。

任務（任務計劃）

此索引標籤會在左側窗格中顯示您的任務計畫。.NET 任務有 5 個步驟：

1. 取得要轉換的資源：在此階段，您會使用 AWS CodeConnections 建立程式碼儲存庫的連接器。根據您的儲存庫許可，程式碼儲存庫的管理員可能需要核准連接器，並授予儲存庫的 AWS 轉換存取權。
2. 探索用於轉換的資源：在此階段， AWS Transform 會在來源控制中探索儲存庫，然後選取部分或全部儲存庫進行評估。
3. 評估轉換的程式碼：系統會評估選取的儲存庫，而且您可以檢視評估報告。
4. 準備轉換：在此階段， AWS Transform 會通知您儲存庫中是否有任何相依性遺失。您可以上傳缺少的相依性或忽略它們。如果您不是儲存庫的管理員，則管理員可能需要核准最終轉換計劃。
5. 轉換：在此階段中， AWS 轉換會轉換您的儲存庫，並在轉換期間為您提供持續狀態，直到完成為止。您可以檢閱轉換報告，以了解變更的內容及其原因。

您可以查看每個步驟的狀態：

- 未啟動
- 等待使用者輸入
- 進行中
- 已完成

儀表板

儀表板索引標籤提供轉換的高階摘要。它會顯示轉換的任務數量、套用的轉換，以及完成轉換的預估時間的指標。儀表板下方是儲存庫及其狀態的資料表：進行中、失敗或成功。

核准

任務的核准請求會顯示在此索引標籤上並完成。

成品

Jjob 相關的成品會從此索引標籤上傳或下載。

工作日誌

AWS 轉換會在 Worklog 索引標籤中記錄其動作。Worklog 提供 AWS Transform 所採取動作的詳細日誌，以及人工輸入請求，以及您對這些請求的回應。

建立原始程式碼儲存庫連接器

在 之後建立 AWS Transform .NET 任務計畫，在任務索引標籤上， AWS 轉換視窗的左側窗格會列出轉換任務的階段。第一個階段是取得要轉換的資源。在此階段，您可以邀請協作者並連接原始程式碼儲存庫。 AWS 轉換視窗的右窗格是您指定詳細資訊的位置。

每個轉換任務只需要一個原始程式碼儲存庫連接器。 AWS 轉換代理程式使用此連接器，透過 AWS CodeConnections 從 GitHub、GitLab 或 Bitbucket 下載 .NET 程式碼庫。您必須在與 AWS 轉換任務相同的區域中設定 AWS CodeConnections。或者，您可以連線到 Amazon S3 中的原始碼，而不是原始碼儲存庫。

> **Note**
>
> 如果您有現有的原始碼儲存庫連接器， AWS Transform 會通知您。選取使用現有的連接器來使用此連接器。如果您不想使用現有的連接器，請參閱 刪除現有的連接器 之前的 新增連接器。每個任務只能有一個來源儲存庫連接器。

新增連接器

若要建立新的原始程式碼儲存庫連接器：

1. 輸入您想要用於 AWS CodeConnections 連接器的 AWS 帳號。
2. 如果您尚未為相同 AWS 帳戶設定 AWS CodeConnections，請設定 AWS CodeConnections。
3. 使用AWS 開發人員工具主控台建立 Bitbucket、GitHub、GitHub Enterprise Server、GitLab 或 AzureDevOps 儲存庫的連線。
4. 複製您建立之連線的 Amazon Resource Name (ARN)。
5. 返回 AWS 轉換，並貼上您建立之連線的 ARN。
6. 輸入連接器的名稱。

> **Note**
>
> 請勿在連接器名稱中輸入個人資訊。

7. 選取初始化連接器建立。
8. AWS 轉換會請求在與目前轉換任務相同的區域中，為您輸入的 AWS 帳戶建立連接器，並通知您在 AWS 管理主控台中的 AWS 管理員已準備好核准核准核准請求。選取複製驗證連結。

9. 如果您是 AWS 管理員，請登入 AWS 帳戶並前往驗證連結以核准連線請求。如果您不是 AWS 管理員，請提供驗證連結給您的 AWS 管理員。
10. 在 AWS 管理員核准連接器請求後，選取完成連接器以完成連接器建立程序。如果您想要使用不同的連接器，請選取重新啟動，以重新啟動連接器建立程序。

協作索引標籤也包含連接器的詳細資訊，其中包括：

- 狀態 -- 已核准或待核准
- AWS 帳戶 ID
- AWS 區域
- 連線 ARN

刪除現有的連接器

> **Note**
>
> 如果您有現有的原始碼儲存庫連接器， AWS Transform 會通知您。選取使用現有連接器或刪除並建立新的連接器。

如果您選擇刪除現有的原始碼儲存庫連線， AWS Transform 會在實際刪除連接器之前警告您。

1. 您可以用幾種方式刪除現有的連接器：
   a. 如果 AWS 轉換提示您，您可以選取刪除並建立新的連接器。
   b. 您也可以在提示中選取重新啟動。若要修改此連接器，您必須重新啟動。
2. AWS 轉換會警告您重新啟動將會刪除連接器。若要刪除連接器，請再次選取重新啟動。
3. AWS 轉換會再次提醒您，刪除連接器會移除與第三方儲存庫的連線，例如 Bitbucket、GitHub 和 GitLab。此外，如果刪除連接器，任何使用此連接器的 AWS 轉換任務都會失敗。若要確認刪除，請輸入 delete，然後選取 Delete。
4. 若要新增新的原始程式碼儲存庫連接器，請參閱 新增連接器。

連線至 Amazon S3 中的原始碼

您可以將 AWS Transform 連接到 Amazon S3 中的原始碼，作為連接原始碼儲存庫的替代方案。

S3 儲存貯體組織

原始原始原始程式碼和轉換後的程式碼存放在常見的 S3 儲存貯體中，如下所示。您必須在與 AWS 轉換任務相同的區域中設定 S3 儲存貯體。將原始碼上傳到儲存貯體，做為根層級的 zip 檔案。zip 檔案必須包含每個儲存庫的頂層資料夾。

在轉換期間， AWS Transform 會建立轉換輸出資料夾，並將轉換結果存放在該資料夾中。轉換會建立名為 transformed-code.zip 的 zip 檔案，其中包含轉換的程式碼。這包括程式碼差異報告檔案名稱 diff.txt，強調專案層級的檔案變更。

```
<customer-bucket>/
### source-code.zip
         ### repo 1
         ### repo 2
         ### ......
         ### repo n
### transform-output/
      ### transformed-code.zip
```

新增 S3 連接器

若要建立新的 S3 原始碼儲存庫連接器：

1. 在 AWS 主控台中，建立 S3 儲存貯體。
2. 將原始碼作為 zip 檔案上傳至 S3 儲存貯體。
3. 在 AWS 轉換 Web 應用程式中，啟動 .NET 轉換任務。在連接原始碼儲存庫步驟中，選取在 S3 儲存貯體中連接原始碼，然後選擇儲存。
4. 在下一頁中，輸入您的 S3 儲存貯體詳細資訊，然後選擇提交。
   a. 連接器名稱
   b. AWS 帳戶 ID
   c. S3 儲存貯體 Arn
   d. S3 儲存貯體加密金鑰 （選用）
5. 核准連接器：
   a. 在下一頁上，複製驗證連結。
   b. 讓核准者瀏覽至連結，以到達 AWS 轉換連接器建立請求頁面。
   c. 選擇 以建立新的角色或使用現有的角色。

d. 檢閱請求後，選擇儲存並核准以核准請求。

6. 指定 S3 zip 檔案位置：
   a. 在 AWS 轉換 Web 應用程式中，等待狀態顯示已核准。
   b. 在指定資產位置頁面上，以 格式輸入程式碼 zip 檔案的 S3 URL，`s3://bucket-name/zip-file-name`然後選擇傳送至 AWS 轉換。
   c. 任務會繼續進行探索步驟以繼續轉換。

刪除 S3 連接器

若要刪除現有的 S3 連接器：

1. 在 AWS 轉換 Web 應用程式中，選取右上角的管理連接器。
2. 在管理連接器視窗中，選取連接器。
3. 選擇 刪除。

確認您的儲存庫以準備進行轉換

在 之後建立原始程式碼儲存庫連接器，確認儲存庫是準備轉換的第一步。您可以：

- 檢閱和變更會影響計畫內容預設設定的變更。
- 檢閱探索的儲存庫，然後選取要評估哪些儲存庫以進行轉換。
- 檢閱儲存庫評估報告，並與 AWS Transform 討論其內容。
- 使用 AWS Transform 產生的計劃.
- 自訂轉換計劃 使用 Web 應用程式或下載 JSON 檔案、修改檔案，並將其上傳至 AWS Transform。

預設設定

在協同合作索引標籤的任務詳細資訊區段中，您可以設定下列項目：

在任務索引標籤的準備轉換 - 確認要轉換的儲存庫步驟中，您可以設定下列項目：

- 設定轉換後的程式碼寫入儲存庫的目標分支名稱。
- 設定目標 .NET 版本：
  - .NET 8：將所有專案轉換為 .NET 8
  - .NET 10：將所有專案轉換為 .NET 10

- 您可以更新預設任務設定，或保持原狀。其中包含：
  - 從轉換計畫中排除 .NET Standard 專案 預設會選取此設定。選取時， AWS Transform 會從轉換計畫中排除任何 .NET Standard 專案。如果您取消選取此設定，則會轉換 .NET Standard 專案，使它們不再與 .NET Framework 相容。
  - 檢查 NuGet 來源並取得 .NET 相容套件版本 允許 AWS 轉換搜尋並取得您要轉換之程式碼的 .NET 相容套件版本。

檢閱儲存庫評估報告

儲存庫評估報告提供 AWS Transform 偵測到之每個儲存庫的資訊表格式檢視。其中包含：

- 儲存庫擁有者
- 評估分支
- 解決方案數量
- 專案數量
- 程式碼行總數
- 偵測到的 .NET 版本
- 偵測到的專案類型
- Private Nuget Dependencies 的數量
- 公有 Nuget 相依性數目
- 轉換複雜性

若要下載 檔案：

1. 在工作區中，選取協同合作索引標籤。
2. 在選擇儲存庫窗格中，選取下載，然後選擇下載為 HTML 或下載為 JSON

有關儲存庫摘要報告的聊天

您的儲存庫摘要可能很長。使用聊天功能進一步了解其內容。當您在 Worklog 索引標籤上看到此訊息時，您的報告可供聊天使用：評估報告現在可在聊天中用於查詢。若要開啟聊天，請按一下 Web 主控台右下角的紫色六邊形圖示。以下是一些範例提示：

- 列出探索或評估的所有儲存庫。
- 在評估中發現了多少個 .NET 6 專案？

- 哪些專案的複雜性最高？

使用 AWS Transform 產生的計劃

您可以選擇使用從探索轉換成功機率較高的儲存庫所建立的轉換 AWS 計劃，其中包括上次修改的、根儲存庫和跨相依儲存庫。

AWS 轉換列出有關轉換計劃的一些高階詳細資訊，包括：

- 探索的儲存庫總數 此舊版 .NET 儲存庫數目是使用原始碼儲存庫連接器探索的 AWS 轉換。 AWS Transform 最多可以掃描每個任務中的 1，000 個儲存庫。如果您有更多要掃描或轉換的儲存庫，您可以建立多個轉換任務。
- 選取的儲存庫 為 AWS 轉換選取的舊版 .NET 儲存庫數量。
- 選取的相依性 所選儲存庫所需的相依性數量，其會自動偵測 AWS 轉換並新增至轉換計劃。

選取的儲存庫資料表會列出選取的儲存庫。您可以依名稱搜尋儲存庫、導覽至其他儲存庫頁面，以及下載列出所選儲存庫及其相依性的 JSON 格式檔案。您可以在此檢視中進行任何變更。

選取的儲存庫資料表會列出針對 AWS 轉換選取之儲存庫的下列詳細資訊：

- 儲存庫名稱
- 來源分支
- 上次修改的日期和時間
- 程式碼行 這可讓您查看是否接近配額限制。如需詳細資訊，請參閱AWS 轉換的配額。
- 相依儲存庫 您可以按一下相依儲存庫的數量，以檢視這些相依性的詳細資訊。

如果您對 AWS 轉換產生的轉換計劃感到滿意，請選取確認儲存庫。

如果您想要變更 AWS 轉換產生的轉換計劃，請選取 自訂轉換計劃。

自訂轉換計劃

如果您選擇不 使用 AWS Transform 產生的計劃，您可以使用下列其中一個選項來自訂要轉換的儲存庫清單：

1. 在選取的儲存庫資料表中選取儲存庫。
   a. 當您將儲存庫新增至計劃時， AWS Transform 會為您選取儲存庫的相依性，並自動將其新增至轉換計劃。

b. 您也可以取消選取資料表中的儲存庫。

2. 下載 AWS 轉換產生的儲存庫和分支 JSON 清單。

a. 選取下載，然後選取下載為 JSON。

b. 檢閱和修改 JSON。您可以移除您不想轉換的儲存庫或儲存庫中的解決方案。

c. 選取上傳自訂計劃來上傳修訂的 JSON。

d. 如果 JSON 上傳成功，選取的儲存庫資料表會顯示您所做的選擇。

3. 您可以選取顯示相依儲存庫，以顯示發現 AWS 的轉換是所選儲存庫相依性的儲存庫清單。

4. 如有需要，您可以重複這些步驟。當您對自訂計劃感到滿意時，請選取確認儲存庫。

解決套件相依性以準備轉換

在 之後確認您的儲存庫以準備進行轉換，如果 AWS Transform 發現缺少套件相依性，您必須完成此步驟。您可以執行 Windows PowerShell 指令碼，從與Visual Studio開發環境相同的裝置取得缺少的套件相依性，也可以手動擷取缺少的套件。然後，上傳遺失的套件。

有兩種方式可以更新缺少套件相依性：

- 使用成品連接器解決：透過專用 Connect 成品儲存庫 HITL 工作流程設定成品儲存庫 (ADO NuGet Connector) 來解決此問題，此工作流程會在未設定成品連接器且套件遺失時顯示。
- 更新遺失套件： AWS Transform 會在遺失套件相依性資料表中列出遺失的套件。您可以在搜尋方塊中依名稱搜尋遺失的套件。此資料表包含下列遺失套件的詳細資訊：
  - 名稱
  - 關聯的儲存庫
  - 架構版本狀態
  - 核心版本狀態

若要解決缺少的套件相依性，請上傳遺失的套件。

上傳遺失的套件

1. 如果您選擇，您可以下載 Windows PowerShell 協助程式指令碼，從Visual Studio開發環境中擷取缺少的套件相依性。或者，您可以手動找到遺失的套件。

   若要使用 Windows PowerShell 指令碼：

   a. 選取下載 Windows PowerShell 指令碼。

b. 在本機以作用中連線執行指令碼，連線至包含遺失套件相依性檔案的儲存庫。

c. 此指令碼可讓您將缺少的套件相依性下載到本機環境。

2. 指令碼會建立單一 zip 檔案供您上傳，其中包含一個封存中的所有相依性。您也可以為每個相依性上傳個別.nupkg或 zip 檔案。
3. 選取上傳套件檔案。
4. 在上傳相依性檔案模態中，選取選擇檔案，然後瀏覽至裝置上的壓縮遺失套件檔案位置。
5. 選取上傳。
6. AWS 轉換會驗證您上傳的檔案。在驗證期間，您無法進行任何更新。 AWS Transform 會在缺少套件相依性資料表上方報告驗證狀態。
7. AWS 轉換也會更新遺失套件相依性資料表中的狀態欄，從遺失更新為已解決。如果套件驗證失敗，其狀態會變成無效。對於無效檔案，請執行下列動作：

   a. 在遺失套件相依性表格中，使用核取方塊選取無效的套件。

   b. 選取移除上傳的檔案。

   c. 這會將其狀態變更回缺少。

8. 在您上傳遺失的套件並解決套件相依性之後，請選取繼續檢閱。

   如果您選取繼續檢閱而不解決缺少的套件相依性， AWS Transform 會詢問您是否要在沒有缺少套件的情況下啟動轉換任務。如果您選取忽略缺少的套件相依性， AWS Transform 將使用組件參考來轉換程式碼。繼續此動作可能會影響相關資源。

資料夾結構需求

對於 NuGet 上傳， AWS 轉換需要以下其中一項：

- 要放置在根層級.nuspec的檔案，用於手動上傳的套件，或
- 使用提供的 PowerShell 指令碼來產生正確的結構

版本比對需求

- Framework status： AWS Transform 會嘗試將 .csproj 檔案（原始程式碼）中指定的相依性版本與上傳的相依性版本進行比對。完全相符會導致成功狀態。
- 核心狀態： AWS Transform 預期上傳.nuspec檔案之相依性區段的核心版本規格。如果找到一個，則核心狀態為成功。

  範例格式：

```
<dependencies>
    <group targetFramework="net8.0" />
</dependencies>
```

常見版本包括：

- .NET 5.0 (net5.0)
- .NET 6.0 (net6.0)
- .NET 7.0 (net7.0)
- .NET 8.0 (net8.0)

檢閱您的計劃以準備轉型

在 確認您的儲存庫以準備進行轉換、 和 之後解決套件相依性以準備轉換， AWS 帳戶管理員必須檢閱轉換計劃，並在 AWS 轉換中核准轉換計劃。

AWS 轉換會顯示任務的儲存庫清單、相依儲存庫，以及為轉換選取的相依套件。

檢閱轉換計畫

AWS 轉換會顯示任務的儲存庫清單、相依儲存庫，以及為轉換選取的相依套件。

> **Note**
>
> AWS 每個轉換計劃最多可轉換 100 個相依性和儲存庫。

1. 如果您不是 AWS 帳戶管理員，請檢閱任務計畫，如果您接受，請選取傳送以進行核准。
2. 如果您是 AWS 帳戶管理員，您必須檢閱計劃，並在準備好時核准計劃以開始轉換。檢閱任務計畫後，請選取下列其中一項：
   a. 拒絕 如果任務是由非 AWS 帳戶管理員的使用者建立，我們建議您通知任務建立者重新啟動任務。
   b. 核准並開始轉換。

任務檢閱包含下列詳細資訊：

1. 任務摘要 這包括：

a. AWS 轉換將放置轉換程式碼的目標分支。

b. 目標 .NET 版本、.NET 8.0 或 .NET 10。

c. 任務設定：

i. 排除 .NET 標準專案

d. 為轉換選取的儲存庫數量

e. 相依儲存庫的數量

f. 私有 NuGet 套件的數量

g. 任務的總程式碼行數

2. 選取的儲存庫 這些是為轉換選取的儲存庫。它們必須是 MVC、Web、Windows Communication Foundation (WCF)、主控台、類別程式庫、UI 架構 - Razor 頁面或單元測試套件。此資料表包含下列資訊：

a. 名稱

b. 來源分支

c. 支援的專案

d. 程式碼行

e. 偵測到的專案

f. 專案已略過

g. 偵測到相依性

3. 新增的相依儲存庫 這些是為轉換新增的相依儲存庫。它們必須是 MVC、Web、Windows Communication Foundation (WCF)、主控台、類別程式庫、UI 架構 - Razor 頁面或單元測試套件。此資料表包含下列資訊：

a. 名稱

b. 需要

c. 來源分支

d. 支援的專案

e. 程式碼行

f. 偵測到的專案

g. 專案已略過

4. 相依套件 這些是為轉換新增的相依套件。它們必須是 MVC、Web、Windows Communication Foundation (WCF)、主控台、類別程式庫、UI 架構 - Razor 頁面或單元測試套件。此資料表包含下列資訊：

a. 名稱
b. 關聯的儲存庫
c. 架構版本狀態
d. 核心版本狀態

轉換您的 .NET 程式碼

AWS 帳戶管理員完成 後檢閱您的計劃以準備轉型，您可以在轉換任務的儀表板索引標籤上檢視轉換進度。

> **Note**
>
> 除了轉換儲存庫和相依性之外， AWS Transform 還可以執行完全轉換（零建置錯誤）的單位測試專案。 AWS Transform 在轉換之前無法存取單位測試結果，而且只能共用轉換後的結果。然後，您可以將轉換前的基準資料與轉換後結果進行比較，以了解任何潛在的差距。

在右上角，您可以看到任務狀態，其具有下列其中一個值：

- 等待使用者輸入
- 經過的時間
- 執行中

您也可以看到下列圖示：

- 停止轉換圖示
- 重新整理圖示
- 設定圖示

儀表板提供轉換的高階摘要。它會顯示轉換和套用轉換的任務數量指標，以及完成轉換的預估時間。

儀表板包括：

1. 轉換任務詳細資訊區段，列出轉換任務的預設設定和詳細資訊，包括：
   a. 目標分支目的地 若要轉換程式碼， AWS Transform 會在程式碼儲存庫中為轉換的程式碼建立新的分支。

b. 目標 .NET 版本、.NET 8.0 或 .NET 10

c. AWS 轉換任務 ID。

d. 任務設定：

i. 排除 .NET 標準專案

2. 轉換摘要區段包含：

a. 為轉換選取的儲存庫數量

b. 要轉換的專案數量

c. 這些儲存庫和專案中的程式碼總行數

轉換開始後，圓餅圖會顯示在儲存庫狀態、套件狀態和單位測試狀態區段中，以即時顯示進度。單元測試狀態會顯示 AWS 轉換在轉換後執行的儲存庫中單元測試的狀態，以測試轉換後的程式碼。 AWS 轉換會分享執行的測試結果，以及個別測試名稱，供客戶檢閱通過和失敗的單元測試清單。

> **Note**
>
> 儲存庫區段會列出 AWS Transform 建議或您為轉換選取的儲存庫。選取下載 JSON 以下載轉換計畫中的儲存庫、相依性和套件清單。

檢閱轉換報告

轉換任務完成後，您可以下載轉換報告：

- 轉換摘要報告：此報告提供 HTML 或 JSON 格式轉換的概觀。從儀表板索引標籤下載轉換摘要報告。選取下載，然後選擇下載為 HTML 或下載為 JSON。
- 轉換詳細資訊報告：此報告提供 HTML 格式轉換的深入資訊。從儀表板索引標籤下載轉換詳細資訊報告。在儲存庫清單中選取下載詳細報告連結，以下載詳細報告。

與 AWS 轉換討論轉換報告

您可以在完全處理儲存庫之後或轉換任務完成後，與 AWS 轉換討論轉換報告。Worklog 索引標籤會顯示可用於聊天的每個儲存庫的此訊息：儲存庫*repository_name*轉換詳細資訊現在可在聊天中用於查詢。當轉換任務完成時，會顯示此訊息：AWS 轉換轉換任務完成。

若要開啟聊天，請按一下 Web 主控台右下角的紫色六邊形圖示。

以下是一些範例提示：

- 哪些專案已成功轉換？
- 哪些專案已部分移植？
- 對repo_name儲存庫進行了哪些變更？
- project_name 專案中升級了哪些套件？

在 IDE 中現代化 .NET

AWS 轉換包含 AWS Toolkit for 中的互動式代理式 AI 助理Visual Studio。它可讓您透過直接在 IDE 中的對話step-by-step引導體驗來現代化應用程式。若要轉換 .NET 解決方案或專案， AWS 轉換代理程式會分析您的程式碼庫、決定移植應用程式所需的更新，並在轉換開始之前產生評估報告和轉換計劃。

IDE Visual Studio 體驗僅支援由 IAM Identity Center 進行身分驗證。如需詳細資訊，請參閱在 IAM Identity Center 中新增使用者。

IDE 體驗提供自動和互動式模式。使用自動模式進行全自動轉換，適用於夜間或長時間執行的任務。使用互動式模式與聊天中的客服人員一起工作，具有對轉換的高度可見性、可自訂的轉換計劃，以及每個專案的step-by-step檢閱。您可以反覆運算以精簡結果或變更方向，直到滿足為止。

當轉換任務處於作用中狀態時，您可以與三個視窗互動：

- 聊天視窗是您與轉換代理程式的主要互動點。使用聊天功能提出問題、討論選項、引導轉換，以及反覆執行。
- AWS 轉換任務計畫視窗會顯示進度步驟，您可以在其中下載或上傳成品或檢視程式碼變更差異。
- Worklog 視窗會以自然語言顯示轉換活動的日誌。

AWS 轉換會執行四個關鍵任務，將 .NET 應用程式移植到 Linux：

- 升級 .NET 和語言版本 – 將較舊的 .NET C# 程式碼升級至目前的 .NET 和語言版本。
- 從 .NET Framework 移轉至跨平台 .NET - 將專案和套件從 Windows 相依的 .NET Framework 移轉至與 Linux 相容的跨平台 .NET。
- 重寫程式碼以便與 Linux 相容 - 重構和重寫已棄用且效率不佳的程式碼元件。
- 產生 Linux 相容性整備報告 – 對於需要使用者介入才能在 Linux 上建置和執行程式碼的開放式任務，AWS Transform 會提供在轉換後設定應用程式所需的動作詳細報告。

如需 AWS Transform 如何執行 .NET 轉換的詳細資訊，請參閱 AWS 轉換如何現代化 .NET 應用程式。

若要使用從 IDE AWS 轉換來現代化 .NET Visual Studio 程式碼，請參閱下列內容：

- 使用 中的 AWS 轉換來現代化 .NET Visual Studio
- AWS 轉換如何現代化 .NET 應用程式
- IDE 中 .NET 轉換問題的故障診斷

配額

如需 IDE 中的 AWS 轉換 .NET 轉換配額，請參閱 AWS 轉換的配額。

使用 中的 AWS 轉換來現代化 .NET Visual Studio

完成以下步驟，將 Windows 型 .NET 應用程式移植到 Linux 相容跨平台 .NET 應用程式，並在 Visual Studio 2026 或 2022 年使用 AWS Transform。

步驟 1：事前準備

繼續之前，請確定您已從 Visual Studio Marketplace 下載並安裝 AWS Toolkit 擴充功能與 Amazon Q。檢閱 .NET 現代化的 AWS 轉換功能和限制，以確認您的程式碼可以轉換。

步驟 2：在 Visual Studio 中驗證

若要從 Toolkit for Visual Studio 連線至 AWS 您的帳戶，請開啟 AWS Toolkit 使用者介面 （連線 UI) 入門：

1. 從 Visual Studio 主功能表中，導覽至 Extensions > AWS Toolkit > 入門以開啟入門： AWS Toolkit 頁面。
2. 選取AWS 轉換身分驗證。
3. 選擇現有的設定檔或建立新的設定檔。建立新的設定檔時，請輸入設定檔的名稱和 AWS 轉換開始 URL，該 URL 會在管理員將您新增至 IAM Identity Center 後透過電子郵件傳送給您。
4. 選擇連線。依照提示登入，並透過 Web 瀏覽器授予存取許可。在 Visual Studio 中，您應該會看到與 IAM Identity Center 連線。
5. 登入後，系統會帶您前往AWS 轉換儀表板。您可以從此登陸頁面執行下列動作：
    - 選取 AWS 轉換設定檔 （區域）
    - 選取或建立工作區
    - 檢視轉換任務的狀態

步驟 3：轉換您的應用程式

若要轉換 .NET 解決方案或專案，請完成下列程序：

開始轉換

1. 在 Visual Studio 中開啟您要轉換的任何 C# 或 VB.NET 型解決方案或專案。
2. 從解決方案總管中，用滑鼠右鍵按一下要轉換的解決方案或專案，然後選擇具有 AWS 轉換的連接埠。
3. 隨即出現具有 AWS 轉換的連接埠對話方塊。
   a. 在選擇工作區下拉式清單中，建立工作區或選取現有的工作區。工作區可讓您的活動顯示在 AWS 轉換 Web 應用程式中，您可以在其中邀請協作者檢視和聊天轉換任務。
   b. 在選擇 .NET 目標下拉式功能表中，選擇您要升級的目標 .NET 版本。
   c. 針對轉換模式，選取自動進行全自動轉換，或選取互動式進行互動式轉換。
   d. 選擇開始以開始轉換。
4. 一旦轉換任務開始，即會顯示AWS 轉換任務計畫、聊天和工作日誌視窗。

評估和轉型計畫

1. AWS 轉換分析程式碼後，評估報告和轉換計劃會顯示在聊天中。在互動式模式中，聊天會暫停供您檢閱。如果您不想在聊天中檢閱，您可以使用這些替代方案：
   - 若要在程式碼編輯器中檢視評估或計劃，請在轉換任務計劃視窗中選擇顯示評估或顯示 AWS 轉換計劃。
   - 若要下載評估或計劃，請使用任務計劃視窗中的下載圖示。
2. 選擇性地修改轉換計劃。您可以與聊天討論計劃，例如探索其他選項。您可以在聊天中提供指示，或使用任務計畫視窗中的下載圖示上傳修訂後的轉換計畫，以進行計畫變更。您可以自由新增、移除或修改步驟。Chat 將透過修訂後的計劃，確認其了解您的指示。
3. 選擇性上傳轉向文件。在聊天視窗中，使用上傳圖示上傳指導文件，例如應用程式規格、組織技術堆疊偏好設定和慣例，或編碼範例。上傳指導文件之後，請在聊天視窗中描述它，以提供客服人員內容。
4. 一旦您對計劃感到滿意，請在聊天中提供核准，轉換就會開始。
5. 在互動式模式中，您可以將檢查點設定為在轉換專案以供檢閱後停止。任務計畫視窗中轉換程式碼下的步驟會有圓形檢查點圖示。所有專案預設都會啟用檢查點。使用核取方塊來清除或設定檢查點。

轉換和檢查點檢閱

1. AWS 轉換會開始轉換您的程式碼。您可以在轉換任務計畫視窗中監控 AWS 轉換步驟的進度。任務計畫視窗會顯示預估的剩餘時間上限和您的任務 ID。
2. 隨著專案轉換，摘要會顯示在聊天中，並套用程式碼變更。
3. 在互動式模式中，到達檢查點時，客服人員會暫停，讓您可以檢閱結果。在任務計畫視窗中，您會看到暫停步驟的檢視結果按鈕，您可以在其中檢閱程式碼差異。檢閱變更後，您可以在聊天中要求進一步變更，或在 中自行變更程式碼Visual Studio。
4. 您可以在檢查點視需要反覆執行。當您滿意時，指示聊天繼續，它將繼續進行下一個專案。

轉換結束

1. 轉換專案後，.NET 代理程式會在 中觸發本機建置Visual Studio，以確認程式碼在本機電腦上成功建置。如果有錯誤，它將可解決問題。
2. 轉換完成後，可能需要額外的步驟，例如 AWS 轉換無法執行的轉換任務，或是 Linux 相容性所需的變更。後續步驟 Markdown 檔案 (NextSteps.md) 可供下載，您可以將其做為 AI 程式碼配套的提示。使用任務計畫視窗的下載圖示按鈕來下載 NextSteps.md。
3. 您可以繼續在聊天中互動，以提出問題或請求其他變更。
4. 當您準備好結束轉換工作時，請告訴聊天。

AWS 轉換如何現代化 .NET 應用程式

如需 .NET 轉換搭配 AWS 轉換運作方式的詳細資訊，請參閱下列各節。

分析您的應用程式並產生轉換計畫

在轉換開始之前， AWS Transform 會在本機建置您的程式碼，以確認其可建置並正確設定以進行轉換。如果程式碼未建置， AWS Transform 將提示是否繼續轉換。 AWS Transform 接著會將程式碼上傳至安全且加密的建置環境 AWS，分析您的程式碼庫，並決定必要的更新以移植您的應用程式

在此分析期間， AWS Transform 會將您的 .NET 解決方案或專案劃分為程式碼群組。程式碼群組是專案及其所有相依性，這些會共同產生可建置的程式碼單位，例如動態連結程式庫 (DLL) 或可執行檔。即使您未選取要轉換的所有專案相依性， AWS Transform 也會決定建置所選專案所需的相依性，並加以轉換，以便轉換的應用程式可建置並可供使用。

分析程式碼後， AWS Transform 會產生一個轉換計劃，概述其將要進行的建議變更，包括程式碼群組清單及其將轉換的相依性。

轉換應用程式

若要開始轉換， AWS Transform 會在安全建置環境中再次建置您的程式碼，以驗證其是否可以遠端建置。 AWS Transform 接著會開始移植您的應用程式。它會從下而上進行，從最低層級相依性開始。如果 AWS 轉換遇到移植相依性的問題，則會停止轉換，並提供導致錯誤的原因資訊。

轉換包括對應用程式進行下列更新：

- 將過時的 C# 程式碼版本取代為與 Linux 相容的 C# 版本
- 將 .NET Framework 升級到跨平台 .NET，包括：
  - 識別並反覆取代套件、程式庫和 API
  - 升級和取代 NuGet 套件和 API
  - 轉換為跨平台執行時期
  - 設定中介軟體並更新執行時期組態
  - 取代私有或第三方套件
  - 處理 IIS 和 WCF 元件
  - 對建置錯誤進行偵錯
- 重寫程式碼使其與 Linux 相容，包括重構和重寫已棄用且效率不佳的程式碼，以移植現有程式碼

檢閱轉換報告並接受變更

轉換完成後， AWS Transform 會提供轉換報告，其中包含針對應用程式所提議更新的相關資訊，包括變更的檔案數目、更新的套件，以及變更APIs。它會標記任何未成功的轉換，包括受影響的檔案或部分檔案，以及在嘗試建置期間遇到的錯誤。您也可以使用建置日誌檢視建置摘要，以進一步了解所做的變更。

轉換報告也提供 Linux 移植狀態，指出是否需要額外的使用者輸入，才能使應用程式 Linux 相容。如果程式碼群組中的任何項目需要您輸入，您可以下載 Linux 整備報告，其中包含 AWS Transform 在建置時無法解決的 Windows 特定考量。如果任何程式碼群組或檔案需要輸入，請檢閱報告以取得仍需要進行何種變更的詳細資訊，並取得如何更新程式碼的建議 (如適用)。您必須先手動進行這些變更，才能在 Linux 上執行您的應用程式。

您可以先檢閱提議的變更 AWS 轉換在 diff 檢視中所做的變更，再接受它們做為檔案的就地更新。更新您的檔案並解決 Linux 整備報告中的任何項目後，您的應用程式就可在跨平台 .NET 上執行。

您可以下載後續步驟 Markdown 檔案，其中包含使用 AWS Transform 或 AI 程式碼配套繼續轉換的提示。若要下載檔案，請選擇報告右上角的下載後續步驟按鈕。

IDE 中 .NET 轉換問題的故障診斷

使用下列各節來疑難排解 IDE 中具有轉換的 .NET AWS 轉換的常見問題。

如何知道任務是否正在進行？

您應該會在 Worklog 視窗中看到一般活動。如果 AWS 轉換在AWS 轉換任務計畫視窗中的步驟上似乎花費很長的時間，您可以檢查任務是否在輸出日誌中仍處於作用中狀態。如果產生診斷訊息，表示任務仍為作用中。

若要檢查輸出，請選擇 中的輸出索引標籤Visual Studio。在顯示輸出來源：功能表中，選擇 Amazon Q 語言用戶端。

下列螢幕擷取畫面顯示 AWS Transform 在轉換期間產生的輸出範例。



為什麼未選取某些專案進行轉換？

AWS 轉換只能轉換支援的 .NET 專案類型。如需轉換 .NET 專案支援的專案類型和其他先決條件的清單，請參閱 步驟 1：事前準備。

如果我的專案或解決方案未轉換，如何取得支援？

如果您無法自行疑難排解問題，您可以聯絡 支援 或 AWS 帳戶 您的團隊提交支援案例。

若要取得支援，請提供轉換任務 ID，以便 AWS 可以調查失敗的任務。若要尋找轉換任務 ID，請選擇 中的輸出索引標籤Visual Studio。在顯示輸出來源：功能表中，選擇 Amazon Q 語言用戶端。

如何防止防火牆干擾轉換任務？

如果您的組織使用防火牆，可能會干擾 中的轉換Visual Studio。您可以在 Node.js 中暫時停用安全檢查，以進行故障診斷或測試阻止轉換執行的因素。

環境變數 `NODE_TLS_REJECT_UNAUTHORIZED` 可控制重要的安全檢查。將 `NODE_TLS_REJECT_UNAUTHORIZED` 設為「0」會停用 Node.js 的拒絕未經授權的 TLS/SSL 憑證。這表示：

- 將接受自我簽署憑證

- 將允許過期的憑證
- 將允許主機名稱不相符的憑證
- 將忽略任何其他憑證驗證錯誤

如果您的代理使用自我憑證，您可以設定下列環境變數，而不要停用 NODE_TLS_REJECT_UNAUTHORIZED：

```
NODE_OPTIONS = –use-openssl-ca
NODE_EXTRA_CA_CERTS = Path/To/Corporate/Certs
```

否則，您必須指定代理使用的 CA 憑證，才能停用 NODE_TLS_REJECT_UNAUTHORIZED。

若要在 Windows 上停用 NODE_TLS_REJECT_UNAUTHORIZED：

1. 開啟「開始」功能表並搜尋環境變數。
2. 選擇編輯系統環境變數。
3. 在系統屬性視窗中，選擇環境變數。
4. 在系統變數下，選擇新增。
5. 將變數名稱設為 NODE_TLS_REJECT_UNAUTHORIZED，並將變數值設為 0。
6. 選擇確定以儲存變更。
7. 重新啟動 Visual Studio。

移植 UI layer 程式碼

AWS 轉換可以將 ASP.NET 網站的 UI 層移植到與 ASP.NET Core 相容的 UI 架構，該架構可在 Linux 上執行。可使用下列轉換：

- MVC Razor UI 移植
- Blazor UI 移植的 Web 表單

MVC Razor UI 移植

具有 Razor Views UI 的 ASP.NET MVC 專案可以移植到 ASP.NET Core 上的 MVC Razor Views，並保留在相同的 UI 架構上。雖然 Razor 檢視在 ASP.NET 和 ASP.NET Core 之間類似，但有一些差異需要移轉程式碼變更：

- ASP.NET MVC Razor Views 使用 System.Web.Mvc 命名空間，並與 .NET Framework 密切相關。
- ASP.NET Core Razor Views 是模組化的，以 Microsoft.AspNetCore.Mvc, 為基礎，具有改善的相依性注入。
- ASP.NET Core 具有新功能，包括標籤協助程式和檢視元件。

AWS 轉換會在 Razor Views 中偵測並移植常見的不相容元件和建構。

Blazor UI 移植的 Web 表單

ASP.NET Web Forms UI 在 ASP.NET Core 上沒有對應項目。 AWS Transform 可以將 Web Forms UI layer 程式碼移植到 ASP.NET Core 上的 Blazor Server。目標 UI 架構的 UI layer 程式碼會重寫。

若要啟用或停用 Web 表單至 Blazor UI 移植，請檢查或清除將 UI ASP.NET Web 表單轉換為 Blazor 任務設定。

轉換詳細資訊

您的 Web Forms 專案會轉換為具有伺服器端託管的 Blazor 專案。下列專案和檔案變更會在轉換期間進行：

檔案轉換映射

從	到	說明
.aspx、.ascx	*.razor	.aspx 頁面和 .ascx 自訂控制項會變成 .razor 檔案
Web.config	appsettings.json	Web.config 設定會變成 appsettings.json 設定
Global.asax	Program.cs	Global.asax 程式碼會變成 Program.cs 程式碼
*.master	*layout.razor	主檔案成為 layout.razor 檔案

轉換後專案結構

轉換後，轉換的檔案會位於下列專案位置：

- 元件資料夾：所有修剪器元件 (*.razor) 都放置在與專案的 .csproj 檔案在相同層級建立的元件資料夾中。

- 頁面映射：Web Forms 頁面 (*.aspx) 會轉換為 Components/Pages 資料夾結構。
- 控制項映射：Web Forms 控制項 (*.ascx) 會直接放置在元件資料夾下方。

限制和不支援的功能

目前不支援下列功能。如果您的工作負載使用這些功能，則需要在轉換後手動移植該程式碼，或使用 AI 程式碼配套進行移植。

- .svc 檔案 （ 服務檔案 ）
- .ashx 檔案 （ 一般處理常式檔案 ）
- 服務參考和 Web 參考 (reference.map、https：//reference.cs、.wsdl 檔案)
- 相同專案中 .aspx (Web 表單 ） 檔案和 .cshtml (Razor) 檔案的混合
- AWS Transform for .NET 尚未支援的專案類型相依性
- 第三方供應商 UI 程式庫/控制項
- 網站專案

僅支援 Web 應用程式專案 （ 包含 .csproj 檔案 ）。若要將網站專案轉換為 Web 應用程式專案，請參閱 Microsoft 指引將網站專案轉換為 Web 應用程式專案。

轉換報告

.NET 轉換任務完成後，即可取得這些轉換報告：

- 轉換摘要報告
- 轉換詳細資訊報告

轉換摘要報告

轉換任務完成後，即可在 Web 主控台中使用轉換摘要報告。從儀表板索引標籤下載轉換摘要報告。選取下載轉換摘要報告，然後選擇下載為 HTML 或下載為 JSON。

轉換摘要報告提供轉換的概觀，以及每個已轉換儲存庫的特定資訊，包括：

- 任務詳細資訊
  - 轉換任務概觀
  - 轉換結果概觀

    - 檔案概觀
- 儲存庫清單，以及針對每個儲存庫：
    - 儲存庫名稱概觀
    - 解決方案轉換摘要
    - 專案詳細資訊，包括狀態、類型、.NET 版本、程式碼總行、程式碼轉換行和已變更的檔案

轉換詳細資訊報告

轉換任務完成後，轉換詳細資訊報告可供 Web 主控台和 IDE 使用者使用。

- Web 主控台使用者：每個轉換的儲存庫都可以使用詳細資訊報告。在儀表板索引標籤上，使用儲存庫清單中的下載詳細報告連結來下載詳細報告。
- IDE 使用者：使用下載圖示從轉換AWS 任務計劃視窗下載轉換報告。

轉換詳細資訊報告是互動式 HTML 報告。它包含有關轉換的深入資訊，包括檔案變更的原因和可操作的錯誤詳細資訊。資訊會依下列階層排列：

- 任務資訊
- 對於每個解決方案：
    - 解決方案轉換摘要
    - 轉換概觀
    - 專案
    - 對於每個專案：
        - 專案摘要
        - 組建錯誤摘要
        - NuGet 套件變更
        - 檔案變更
        - 組建錯誤
    - 單位測試結果
    - Linux 就緒狀態報告

如需範例轉換詳細資訊報告區段的逐步解說，請參閱部落格文章宣布適用於 .NET 的 AWS 轉換詳細轉換報告。

.NET 轉換的最佳實務

請遵循本指南，透過 AWS Transform 獲得更好的 .NET 現代化成果。這些最佳實務適用於 .NET 對話式 AI 助理，目前可用於 Visual Studio IDE。

主題

- 轉換之前
- 評估和規劃
- 以互動或自主方式轉換
- 驗證和定案

轉換之前

在開始 .NET 轉換任務之前，請檢閱下列建議。

使用 .NET 對話式 AI 助理

使用新的 .NET 代理程式以取得最佳轉換結果。對話式 AI 助理可透過 AWS Toolkit for Visual Studio 供 Visual Studio使用。它也可透過 AWS 轉換和 AWS 轉換 MCP 代理程式的Kiro強大功能，供 Kiro 或其他 IDEs 使用。Web 主控台尚未提供新的 .NET 代理程式。

如果目標不是 .NET 轉換為 .NET，請使用其他工具

AWS 適用於 .NET 的轉換適用於 .NET Framework 到 .NET 程式碼現代化，以及 .NET 升級到更新版本。它不適用於包含非 的轉換。NET 語言，例如 Java 或非 。NET 架構，例如 React。它也不會提供應用程式架構重構。針對這些類型的現代化使用AWS 轉換自訂 或 Kiro 。

使用穩定的 版本Visual Studio，最好是 VS2026

使用 的 GA 版本Visual Studio而非預覽版或內部人員版本，以避免預覽軟體的複雜性。 AWS Toolkit 可與 Visual Studio 2026 或 2022 搭配使用。建議使用 VS2026，因為它在減少記憶體耗用量的情況下表現更好。

使用最新的 AWS Toolkit for Visual Studio

請繼續使用最新版本的 AWS Toolkit forVisual Studio，以取得錯誤修正和功能更新。您可以在延伸項目 > 管理延伸項目 > 安裝中檢查您的工具組版本和升級。

在 IDE Visual Studio 中處理中等或更高複雜性的專案

IDE 體驗為您提供最深入的轉換檢視，您可以在轉換專案時與 .NET 代理程式搭配使用。對於中、高或關鍵複雜性專案，請使用 IDE 而非 Web 主控台。

擁有驗證計畫

決定如何在轉換後驗證應用程式的正確性。轉換後，您需要確認它在執行時的行為和外觀正確，以及安全控制、商業邏輯和資料儲存都完好無損。是否將手動和/或使用測試自動化執行驗證？ 如果您的解決方案包含單元測試， AWS Transform 會為您移植它們並執行它們，而結果會出現在轉換報告中。

提供NuGet私有套件相依性

如果您的解決方案取決於私有套件，請確保本機機器上有可用的套件，以便 IDE 和 AWS 轉換可以找到它們。

指定套件替換或詢問客服人員建議

對於沒有現代 .NET 版本的套件，您可以自訂轉換計劃以指定預期的套件替換，或向客服人員尋求建議。

在您確定不想再進行任何變更之前，請勿結束您的任務

轉換完成後，如果您想要其他變更，請勿立即結束任務。在您表示轉換之前，轉換不會完成。您可以在標記任務完成之前請求變更。

轉換之後，請遞交給 AI 程式碼合作夥伴，以完成您的應用程式

預期 會將 AWS Transform 與 AI 程式碼搭配組合，例如 Kiro。常見的模式是先使用 AWS Transform for .NET 進行轉換，然後交給 AI 程式碼夥伴以完成應用程式。該最終工作可能包括識別和更正執行時間錯誤、行為問題和 UX 樣式。

在現代化旅程中，將 AWS Transform 視為快速旅程，帶您朝目標邁進很長路，並將 AI 程式碼合作夥伴視為本機旅程，帶您前往最終目的地。

為了協助從 AWS 轉換到 AI 程式碼夥伴交接， AWS Transform 會在轉換結束時提供 HTML 轉換報告和後續步驟標記文件。

評估和規劃

開始轉換任務後， AWS Transform 會分析您的程式碼，並產生評估報告和轉換計劃。使用下列最佳實務，以充分利用此階段。

檢閱評估並提出問題以設定您的期望

仔細檢閱評估問題清單，以了解哪些專案難以轉換，以及原因為何。代理程式會呈現具有複雜度層級（低、中、高、關鍵）的專案，並說明其為何具有該評分。

提出問題，以進一步了解具有挑戰性的領域。例如：

- 詢問客服人員在專案轉換或使用案例中的可信度。
- 詢問客服人員，AI 程式碼配套可能需要哪些轉換後任務。

檢閱計劃並與客服人員討論選項

代理程式提供轉換計劃供您檢閱。您可以討論和修改此計劃。首先了解您的選項。詢問客服人員計劃的任何部分有哪些替代方案。

例如，轉換計畫可能會提議將 WCF 服務轉換為 ASP.NET Web APIs。不過，您的組織偏好使用 WCF。您向客服人員詢問選項，並了解替代方法是將其轉換為 CoreWCF。

上傳指導文件，為您的組織量身打造計劃

建立原始轉型計畫時，不了解組織的需求和偏好設定。您可以通知代理程式組織慣例、應用程式規格、偏好的技術堆疊和偏好的編碼模式範例。

上傳指導文件之後，請加以解釋，以提供客服人員內容。透過轉向文件的其他資訊，客服人員可以根據組織喜歡的運作方式，準備量身打造的計劃。

自由自訂計劃

.NET 代理程式具有彈性，您可以在 .NET 到 .NET 轉換的網域內自由自訂轉換計劃。您可以在聊天中要求計劃變更，或者如果您願意，也可以使用 Markdown 檔案。檢閱和精簡計畫，直到滿足為止。

如果需要由多個利益相關者檢閱計劃，您可以將計劃下載為 Markdown 檔案、共用，然後上傳自訂計劃。

例如，您檢閱轉換計畫，並決定要將類別程式庫專案轉換為 .NET Standard，而不是 .NET 10。在聊天中，您說：「修改計畫，將所有類別程式庫轉換為 .NET Standard 2.0」，客服人員會為您提供修訂後的計畫。

以互動或自主方式轉換

Visual Studio IDE 體驗提供自主和互動式模式，以控制轉換期間的互動程度。

使用互動式和自主模式來控制互動程度

您可以在開始轉換時選取 模式，而且您可以隨時透過聊天視窗頂端的下拉式清單進行變更。

- 使用自動模式進行全自動轉換，適用於夜間或長時間執行的任務。您仍然有機會檢閱結果，並在任務結束時要求變更。
- 在整個轉型過程中，使用互動式模式與客服人員一起聊天，搭配可自訂的轉型計畫、對轉型詳細資訊的高度可見性，以及每個專案的step-by-step審查。您可以反覆運算以精簡結果或變更方向，直到滿足為止。

您可以結合 模式。例如，以互動式模式開始檢閱和調整轉換計劃，然後切換到自動模式以自動轉換專案。

請客服人員解釋程式碼變更

如果您看到不了解的程式碼變更，請要求客服人員解釋。

使用檢查點在專案停止檢閱或變更

在互動式模式中，核准計畫後，您可以為每個專案設定或清除檢查點。轉換具有檢查點的專案時，轉換後的程式碼會套用至 IDE 中的專案，而客服人員會暫停供您檢閱。您可以檢閱結果，如果不喜歡這些結果，您可以要求更多變更。

在檢查點停止時，您可以：

- 檢閱聊天中顯示的結果，並在聊天中提出問題。例如：「為什麼要變更檔案 X 中的密碼編譯 API？」
- 在 AWS 轉換任務計畫視窗中，選擇專案的檢視結果按鈕來檢視程式碼變更。
- 透過要求其他變更來精簡轉換。例如：「將此變更為使用記錄器 X」或「將此變更為使用套件 X，而非套件 Y」。
- 重試轉換，使用不同的指示進行轉換。例如：「將此類別程式庫變更為目標 .NET Standard 而非 .NET 10」或「重試此轉換並將目標從 Blazor 變更為 MVC Razor Pages」。
- 在 IDE 中進行您自己的程式碼變更。
- 告知客服人員繼續前往下一個專案檢查點。

反覆運算直到滿足

現代化本質上是反覆的，您可以預期 代理程式會反覆進行。您可以在專案檢查點進行變更，也可以在轉換結束時進行變更。視需要反覆執行，直到您滿意為止。在您表示之前，轉換不會完成。

在檢查點停止時，與客服人員一起編寫程式碼

您可以在使用 代理程式時自行變更程式碼。在檢查點停止時，您可以在 中編輯程式碼檔案Visual Studio。當您指示代理程式繼續執行時，您的變更將會同步。

驗證和定案

轉換完成後，請驗證轉換的應用程式，並將其定案以供生產使用。

檢閱轉換報告和後續步驟，以了解完成的項目和剩餘項目

檢閱 HTML 轉換報告以了解已執行的操作。檢閱後續步驟的 Markdown 檔案，以了解仍保留哪些任務。請客服人員釐清任何不清楚的內容。

使用 AI 程式碼配套來驗證、偵錯和完成您的應用程式

檢閱轉換的應用程式是否正確。使用 AI 程式碼搭配，例如 Kiro 來解決問題。

驗證單位測試

如果您的解決方案包含單元測試專案 (NUnit、 或 MSTest)xUnit， AWS Transform 會將它們移植到現代 .NET 並為您執行測試。檢查 HTML 轉換報告以取得單位測試結果。使用 AI 程式碼配套修正失敗測試。

驗證應用程式功能

執行您的應用程式並確認其功能與原始應用程式相符。請注意功能問題和執行時間錯誤。使用 AI 程式碼配套進行更正。

驗證應用程式 UI

執行您的應用程式並確認其看起來和行為與原始應用程式相似，包括導覽和路由。如果您的應用程式沒有樣式，可能是 .css 檔案不在正確的位置。使用 AI 程式碼配套進行更正。

SQL Server 現代化

AWS Transform for SQL Server Modernization 是一項採用 AI 的服務，可將 Microsoft SQL Server 資料庫及其相關聯 .NET 應用程式的完整堆疊現代化自動化為 Amazon Aurora PostgreSQL。 AWS Transform 現在會使用代理互動式體驗，將採用 AWS DMS 技術的 SQL Server 儲存物件和程式碼物

件（存放程序）轉換。此服務協調從結構描述轉換、資料遷移和修改應用程式程式碼以符合新目標 PostgreSQL 的整個遷移旅程，透過自動化複雜且耗費大量人力的任務，讓您的團隊更具生產力。

支援的 區域

AWS 美國東部（維吉尼亞北部）- us-east-1 提供 SQL Server 轉換

跨區域使用：對於不支援區域中的資料庫，您可以將資料庫複製到支援的區域進行轉換，然後將結果部署回目標區域。

功能和主要功能

資料庫轉換

- 結構描述轉換：自動將 SQL Server 結構描述轉換為 Aurora PostgreSQL，包括資料表、檢視、索引、限制條件和關係
- 預存程序轉換：以 AI 增強的準確性將 T-SQL 預存程序轉換為 PL/pgSQL
- 資料遷移：使用 AWS Database Migration Service (DMS) 透過完整性驗證遷移資料
- 資料庫物件：支援觸發、函數、檢視、計算資料欄和身分資料欄
- 驗證：自動化資料完整性驗證和參考完整性檢查

應用程式轉換

- 實體架構轉換：更新 PostgreSQL 的實體架構 6.3-6.5 和 EF Core 1.0-10.0 組態
- ADO.NET 轉換：將 ADO.NET 資料存取碼從 SQL Server 轉換為 PostgreSQL 供應商。
- 連線字串更新：自動將所有資料庫連線字串更新至新的目標 PostgreSQL 資料庫
- 資料庫提供者變更：將 SQL Server 提供者取代為 Npgsql (PostgreSQL 提供者）
- ORM 組態更新：修改資料類型映射、身分資料欄和資料庫特定的組態

協調與驗證

- 以波為基礎的現代化：將大型資產組織成邏輯遷移階段
- 相依性映射：識別應用程式和資料庫之間的關係
- Human-in-the-loop (HITL) 檢查點：在關鍵階段提供審核和核准閘道
- 自動化驗證：測試結構描述相容性、資料完整性和應用程式功能

- CI/CD 整合：與現有的開發管道整合

部署

- Amazon ECS 和 Amazon EC2 部署：具有自動擴展支援的自動化容器化部署
- Infrastructure-as-code產生：建立 CloudFormation 或 AWS CDK 範本
- 自動化部署驗證：使用運作狀態檢查來驗證成功的部署
- 回復功能：發生問題時支援回復程序

支援的版本和專案類型

SQL Server 版本

AWS 轉換支援下列 SQL Server 版本：

SQL Server 版本	支援狀態
SQL Server 2022	支援
SQL Server 2019	支援
SQL Server 2017	支援
SQL Server 2016	支援
SQL Server 2014	支援
SQL Server 2012	支援
SQL Server 2008 R2	支援

> **Note**
>
> 支援所有 SQL Server 版本 (Express、Standard、Enterprise)。SQL Server 可在 AWS (Amazon RDS for SQL Server 或 Amazon EC2 上的 SQL Server) 上託管，或在 外部託管 AWS。

.NET 版本

.NET 版本	支援狀態
.NET 10	支援
.NET 8	支援
.NET 7	支援
.NET 6 （核心）	支援
.NET Framework 4.x 及更早版本	不支援

> **Important**
>
> 不支援舊版 .NET Framework 4.x 和舊版。如果您的應用程式使用 .NET Framework，您必須先使用 AWS Transform for .NET 現代化升級至 .NET Core 6+，才能使用 SQL Server 轉換功能。

實體架構版本

架構	支援的版本
實體架構 6	6.3、6.4、6.5
實體架構核心	1.0 到 10.0
ADO.NET	所有版本 (GA)

原始程式碼儲存庫

AWS 轉換支援下列原始程式碼平台：

- GitHub 和 GitHub Enterprise Server
- GitLab.com 和 GitLab 自我管理

- Bitbucket 雲端和 Bitbucket 資料中心
- Azure DevOps 和 Azure DevOps 伺服器
- Amazon S3

目標資料庫

AWS 支援最新 Aurora 功能和最佳化的轉換目標為 Amazon Aurora PostgreSQL (PostgreSQL 15+ 相容）。

技術需求

資料庫需求

- Microsoft SQL Server 2008 R2 至 2022 版
- 託管於 AWS (Amazon RDS for SQL Server 或 Amazon EC2 上的 SQL Server) 或託管於 外部的 SQL Server AWS
- 對於 AWS託管的資料庫，資料庫和 AWS 轉換必須位於相同的 AWS 區域。
- 對於託管於 外部的資料庫 AWS，需要與 AWS Transform 服務的網路連線。
- 具有 VIEW DEFINITION 和 VIEW DATABASE STATE 許可的資料庫使用者
- 僅使用可列印 ASCII 字元的資料庫密碼 （不包括 '/'、'@'、"" 和空格）
- 包含來源 SQL Server 的 VPC 必須在至少 2 個不同的可用區域中具有子網路 (DMS 複寫子網路群組需要）

應用程式需求

- .NET 6、7、8 或 10 應用程式
- 實體架構 6.3-6.5 或實體架構核心 1.0-10.0，或 https：//ADO.NET
- 原始程式碼中可探索的資料庫連線
- 應用程式已成功建置和執行
- 支援的儲存庫平台中的原始程式碼

AWS 帳戶需求

- AWS 具有管理員存取權的帳戶
- IAM Identity Center 已啟用

- 已建立必要的服務角色（請參閱下列設定指示）
- 具有適當網路組態的 VPC

資料處理和儲存

處理位置

- 結構描述處理發生在 VPC 內的 DMS 執行個體中
- 資料遷移是選用的，可以視需要排除
- 轉換成品存放在 AWS 轉換服務區域中

存放的成品

下列項目存放在服務區域中：

- 代理程式日誌
- 評估結果
- SQL 結構描述檔案
- DMS 輸出成品

> **Important**
>
> 資料常駐的重要：即使選擇退出資料遷移，中繼資料和處理成品也會存放在服務區域中。這對具有嚴格資料落地要求的組織來說很重要。

成品管理

- 使用您自己的 KMS 金鑰進行加密的客戶選項
- 為所有成品定義的 TTL time-to-live期間
- 您可以下載成品以進行離線儲存

現代化任務入門

在 AWS 轉換中建立 SQL Server 現代化任務且代理程式啟動後，代理程式會詢問您希望 AWS 轉換如何存取來源 SQL Server 結構描述。您對此第一則訊息的回應會決定在剩餘的任務中執行哪些工作流程。選擇下列其中一項：

- 連線至資料庫： AWS Transform 會直接連線至您執行中的 SQL Server。當資料庫的即時網路連線可用且您希望 AWS Transform 遷移真實資料時，請選擇此選項。
- 上傳 DDL 檔案 — 您可以使用提供的指令碼擷取結構描述定義 (DDL) 檔案，並將其上傳至 AWS 轉換。當無法使用或不想要直接資料庫連線時，請選擇此選項。不需要即時連線，也不會遷移真實資料。

這兩個工作流程都以 Amazon Aurora PostgreSQL 為目標，並共用與此頁面其他部分相同的支援版本、限制和資料處理行為。選擇符合您環境的工作流程。

> **Note**
>
> 當您選擇連線至資料庫時，線上工作流程會開始。當您選擇上傳 DDL 檔案時，離線工作流程就會開始。

連線至資料庫（線上工作流程）

在此工作流程中， AWS Transform 會直接連線至來源 SQL Server，並使用 AWS Database Migration Service (DMS) 將結構描述轉換，並將資料遷移至 Amazon Aurora PostgreSQL。這是即時資料庫連線可用時的標準end-to-end工作流程。

工作流程會繼續進行下列階段：

1. 先決條件 — AWS Transform 確認 DMS 先決條件已就緒 (IAM 角色、秘密和來源資料庫的網路存取）。
2. 連線 — 您提供連線詳細資訊，而 AWS 轉換會建立與來源資料庫的連線。
3. 驗證 - AWS 轉換會驗證連線能力和許可。
4. 探索和評估： AWS 轉換會探索伺服器上的資料庫，由您選擇要現代化哪些資料庫，而 AWS 轉換會評估資料庫。
5. 每個資料庫轉換 — 對於每個選取的資料庫， AWS Transform 會佈建 Aurora PostgreSQL 目標、轉換結構描述，以及遷移資料。選擇遷移真實資料、產生合成資料或略過資料遷移。

6. 程式碼評估和轉換（選用）— 如果來源程式碼儲存庫已連線， AWS Transform 會評估和轉換相關聯的 .NET 應用程式。
7. 部署（選用）— AWS Transform 部署轉換的應用程式。

> **Note**
>
> 此工作流程會使用 DMS AWS 遷移您的真實資料。開始之前，請確定網路和 IAM 先決條件已滿足。請參閱上一節中的技術需求。

SQL Server 需求

資料庫需求

外部託管資料庫

AWS 支援在 外部託管的資料庫。若要使用外部託管資料庫，您必須確保資料庫與 AWS Transform 服務之間的網路連線。

SSIS 工作負載

- 限制：不支援 SQL Server Integration Services (SSIS) 轉換。
- 解決方法：使用 AWS Glue 或其他 ETL 服務進行 SSIS 遷移。

連結伺服器

- 限制：透過連結伺服器的外部資料庫連線需要人工組態。
- 解決方法：遷移後重新設定連結的伺服器，或使用資料庫連結或應用程式層級整合等替代方法。

複雜的 T-SQL 模式

- 限制：某些進階 T-SQL 模式可能需要人工介入。
- 解決方法：使用 Amazon Kiro CLI 進行複雜的 SQL 轉換。 AWS Transform 會標記這些轉換，以便在轉換過程中檢閱。

應用程式需求

舊版 .NET Framework

- 限制：不支援 .NET Framework 4.x 和舊版。
- 解決方法：先使用 AWS Transform for .NET 升級至 .NET Core 6+，然後使用 SQL Server 轉換。

實體架構版本

- 限制：僅支援實體架構 6.3-6.5 和 EF Core 1.0-10.0。
- 解決方法：在轉換之前升級至支援的實體架構版本。

VB.NET 應用程式

- 限制：不支援 VB.NET。
- 解決方法：轉換為 C# 或使用 AWS 轉換自訂從 VB.NET 轉換為 C#。

跨資料庫相依性

- 限制：當資料庫結構描述跨多個資料庫互動時的挑戰。
- 解決方法：遷移前檢閱和重構跨資料庫查詢。請考慮合併資料庫或使用 PostgreSQL 結構描述。
- 影響：對於複雜的跨資料庫案例，可能需要人工介入。

儲存庫資料庫耦合

- 限制：當單一儲存庫提供多個資料庫時的挑戰。
- 解決方法：考慮儲存庫重組或分階段遷移方法。
- 影響：可能需要對以波為基礎的遷移進行額外規劃。

基礎設施需求

每個任務的單一帳戶/區域

- 限制：每個轉換任務都以一個 AWS 帳戶和區域為目標。
- 解決方法：為多帳戶或多區域部署建立多個轉換任務。

部署目標

- 限制：支援 Amazon ECS 和 Amazon EC2 部署。

儲存庫需求

Private NuGet 套件

- 限制：私有 NuGet 套件需要額外的組態。
- 解決方法：在開始任務之前，在轉換設定中設定私有 NuGet 饋送。

SQL Server 設定

在 SQL Server 環境中執行這些步驟，以啟用 AWS 轉換現代化。

資料庫設定和組態

步驟 1：建立具有必要許可的資料庫使用者

建立具有必要許可的 AWS Transform 專用資料庫使用者。如果您已經有 DMS 結構描述轉換使用者，則可以重複使用它。

連線至 SQL Server 執行個體並執行下列命令：

```
-- Create the login in master database
USE master;
CREATE LOGIN [atx_user] WITH PASSWORD = 'YourStrongPassword123!';

-- Switch to your application database
USE [YourDatabaseName];
CREATE USER [atx_user] FOR LOGIN [atx_user];

-- Grant required permissions
GRANT VIEW DEFINITION TO [atx_user];
GRANT VIEW DATABASE STATE TO [atx_user];
ALTER ROLE [db_datareader] ADD MEMBER [atx_user];

-- Grant master database permissions
USE master;
GRANT VIEW SERVER STATE TO [atx_user];
GRANT VIEW ANY DEFINITION TO [atx_user];
```

> **Note**
>
> 針對您要現代化的每個資料庫，重複資料庫特定的命令 (USE、CREATE USER、GRANT)。

db_datareader 角色僅適用於資料遷移，而不只是結構描述轉換。

- db_datareader 角色會授予資料庫中所有資料表的讀取存取權
- 只有在執行資料遷移時，才需要此角色。
- 僅針對結構描述轉換（沒有資料遷移），不需要 db_datareader 角色
- 其他許可 (VIEW DEFINITION、VIEW DATABASE STATE 等）足以轉換結構描述

步驟 2：在 AWS Secrets Manager 中存放登入資料

將您的資料庫登入資料安全地存放在 AWS Secrets Manager 中。如果您已為 DMS 建立秘密，請略過此步驟。

1. 在主控台中導覽至 AWS Secrets Manager
2. 選擇儲存新的秘密
3. 設定秘密：
   - 秘密類型：其他資料庫的登入資料
   - 資料庫：Microsoft SQL Server
   - 使用者名稱：atx_user（或您選擇的使用者名稱）
   - 密碼：您建立的密碼
   - 伺服器名稱：您的 SQL Server 端點
   - 資料庫名稱：您的資料庫名稱
   - 連接埠：1433（或您的自訂連接埠）
4. 選擇下一步
5. 輸入秘密名稱：atx-db-modernization-sqlserver
6. 新增必要的標籤（這些標籤為必要標籤）：
   - 金鑰：專案、值：atx-db-modernization
   - 金鑰：擁有者、值：資料庫連接器
7. 從剩餘的畫面選擇下一步
8. 選擇存放區

9. 請注意要用於下一個步驟的秘密 ARN

> **Important**
>
> 資料庫密碼只能使用可列印的 ASCII 字元，不包括 '/'、'@'、"" 和空格。排程刪除的秘密可能會導致轉換失敗。

步驟 3：建立必要的 DMS 角色

AWS 轉換需要 DMS 操作的特定 IAM 角色。使用以下 CloudFormation 範本部署這些角色。

> **Note**
>
> 如果 AWS 您的帳戶已有現有的 DMS 相關角色，請修改此範本以重複使用這些資源，而不是建立重複項目。

使用下列內容建立名為 dms-roles.yaml 的檔案：

```
AWSTemplateFormatVersion: '2010-09-09'
Description: 'DMS Service Roles for AWS Transform SQL Server Modernization'

Resources:
  DMSCloudWatchLogsRole:
    Type: AWS::IAM::Role
    Properties:
      RoleName: dms-cloudwatch-logs-role
      AssumeRolePolicyDocument:
        Version: '2012-10-17'
        Statement:
          - Effect: Allow
            Principal:
              Service:
                - dms.amazonaws.com
                - schema-conversion.dms.amazonaws.com
            Action: sts:AssumeRole
      ManagedPolicyArns:
        - arn:aws:iam::aws:policy/service-role/AmazonDMSCloudWatchLogsRole

  DMSS3AccessRole:
```

```
    Type: AWS::IAM::Role
    Properties:
      RoleName: dms-s3-access-role
      AssumeRolePolicyDocument:
        Version: '2012-10-17'
        Statement:
          - Effect: Allow
            Principal:
              Service:
                - dms.amazonaws.com
                - schema-conversion.dms.amazonaws.com
            Action: sts:AssumeRole
      Policies:
        - PolicyName: S3TaggedAccess
          PolicyDocument:
            Version: '2012-10-17'
            Statement:
              - Effect: Allow
                Action:
                  - s3:GetBucketLocation
                  - s3:GetBucketVersioning
                  - s3:PutObject
                  - s3:PutBucketVersioning
                  - s3:GetObject
                  - s3:GetObjectVersion
                  - s3:ListBucket
                  - s3:DeleteObject
                Resource: arn:aws:s3:::atx-db-modernization-*
                Condition:
                  StringEquals:
                    aws:ResourceAccount: !Ref AWS::AccountId

  DMSSecretsManagerRole:
    Type: AWS::IAM::Role
    Properties:
      RoleName: dms-secrets-manager-role
      AssumeRolePolicyDocument:
        Version: '2012-10-17'
        Statement:
          - Effect: Allow
            Principal:
              Service:
                - dms.amazonaws.com
                - schema-conversion.dms.amazonaws.com
```

```
            Action: sts:AssumeRole
      Policies:
        - PolicyName: SecretsManagerTaggedAccess
          PolicyDocument:
            Version: '2012-10-17'
            Statement:
              - Effect: Allow
                Action:
                  - secretsmanager:GetSecretValue
                  - secretsmanager:DescribeSecret
                Resource: '*'
                Condition:
                  StringEquals:
                    secretsmanager:ResourceTag/Project: atx-db-modernization
                    secretsmanager:ResourceTag/Owner: database-connector

  DMSVPCRole:
    Type: AWS::IAM::Role
    Properties:
      RoleName: dms-vpc-role
      AssumeRolePolicyDocument:
        Version: '2012-10-17'
        Statement:
          - Effect: Allow
            Principal:
              Service:
                - dms.amazonaws.com
                - schema-conversion.dms.amazonaws.com
            Action: sts:AssumeRole
      ManagedPolicyArns:
        - arn:aws:iam::aws:policy/service-role/AmazonDMSVPCManagementRole

  DMSServerlessRole:
    Type: AWS::IAM::ServiceLinkedRole
    Properties:
      AWSServiceName: dms.amazonaws.com
      Description: 'Service Linked Role for AWS DMS Serverless'

Outputs:
  DMSCloudWatchLogsRoleArn:
    Description: ARN of the DMS CloudWatch Logs Role
    Value: !GetAtt DMSCloudWatchLogsRole.Arn
  DMSS3AccessRoleArn:
    Description: ARN of the DMS S3 Access Role
```

```
    Value: !GetAtt DMSS3AccessRole.Arn
  DMSSecretsManagerRoleArn:
    Description: ARN of the DMS Secrets Manager Role
    Value: !GetAtt DMSSecretsManagerRole.Arn
  DMSVPCRoleArn:
    Description: ARN of the DMS VPC Role
    Value: !GetAtt DMSVPCRole.Arn
    Export:
      Name: !Sub ${AWS::StackName}-VPCRole

  DMSServerlessRoleArn:
    Description: ARN of the DMS Serverless Role
    Value: !Sub 'arn:aws:iam::${AWS::AccountId}:role/aws-service-role/
dms.amazonaws.com/AWSServiceRoleForDMSServerless'
    Export:
      Name: !Sub ${AWS::StackName}-ServerlessRole
```

使用 CLI 部署 CloudFormation AWS 堆疊：

```
aws cloudformation create-stack \
  --stack-name dms-roles \
  --template-body file://dms-roles.yaml \
  --capabilities CAPABILITY_NAMED_IAM \
  --region us-east-1
```

或使用 AWS 主控台部署：

1. 在 AWS 主控台中導覽至 CloudFormation
2. 選擇建立堆疊
3. 選取上傳範本檔案
4. 上傳 dms-roles.yaml 檔案
5. 輸入堆疊名稱：dms-roles
6. 確認 IAM 功能
7. 選擇建立堆疊

步驟 4：設定網路安全

確保 AWS Transform、SQL Server 資料庫和其他 AWS 服務之間的網路連線正常。

安全群組組態（建議的方法）

建議方法：使用安全群組型存取控制，而非 IP 型規則。這可提供更好的安全性、更輕鬆的管理，並與 AWS Transform 的架構無縫搭配運作。

為什麼要使用安全群組型存取控制？

- DMS 結構描述轉換會在 VPC 中建立彈性網路界面 (ENIs)
- 您的資料庫不需要公開存取
- AWS 轉換不會公開私有 IP 地址，使得 IP 型規則複雜
- 安全群組參考會在資源擴展時提供動態的自動更新

設定 SQL Server 安全群組

在 AWS 轉換中設定 DMS 結構描述轉換執行個體描述檔時，您可以指定 DMS SC 執行個體的安全群組。您的資料庫安全群組應允許來自此 DMS SC 安全群組的傳入流量。

Step-by-step組態：

1. 識別 DMS 結構描述轉換安全群組：
   - 這是在 AWS Transform 中建立執行個體描述檔時所指定
   - 請注意安全群組 ID（例如 sg-0123456789abcdef0)
2. 更新您的 SQL Server 安全群組傳入規則：
   - 類型：自訂 TCP
   - 連接埠：1433（或您的自訂 SQL Server 連接埠）
   - 來源：DMS 結構描述轉換安全群組 ID
   - 描述：「允許 DMS 結構描述轉換存取」
3. 對於 Aurora PostgreSQL 目標（建立後）：
   - 類型：PostgreSQL
   - 連接埠：5432（或您的自訂 PostgreSQL 連接埠）
   - 來源：DMS 結構描述轉換安全群組 ID
   - 描述：「允許 DMS 結構描述轉換存取」

> **Important**
>
> 對於最低權限安全模型很重要：如果您的組織使用預設封鎖所有流量的「最低權限」安全模型，您必須明確允許從 DMS 結構描述轉換安全群組到資料庫連接埠的傳入流量。請勿將連接埠 1433 開啟至所有來源或 IP 範圍。

必要的 AWS 服務連線

確保您的 VPC 可以與下列人員通訊：

- AWS 轉換服務端點
- AWS DMS 端點
- Aurora PostgreSQL 端點
- 用於成品儲存的 S3 端點
- AWS Secrets Manager 端點
- AWS CodeConnections 端點

VPC 端點：針對私有網路，設定所需 AWS 服務的 VPC 端點，以避免網際網路閘道相依性。

外部託管資料庫的需求

如果您的 SQL Server 資料庫託管在 外部 AWS，請確保符合下列先決條件，然後在開始現代化之前完成設定步驟。

先決條件

- 具有 VPC AWS 的帳戶
- VPC 與外部資料庫之間的網路連線。如需設定網路連線的詳細資訊，請參閱 AWS DMS 《使用者指南》中的設定網路連線。

設定步驟

1. 在 AWS Secrets Manager 中使用外部資料庫的連線詳細資訊建立秘密。如需詳細資訊，請參閱the section called “步驟 2：在 AWS Secrets Manager 中存放登入資料”。
2. 出現提示時，請提供 VPC ID 和安全群組 ID 以連線至外部資料庫。 AWS Transform 會提示您輸入此資訊，因為無法在 AWS 帳戶中解析秘密中的資料庫主機名稱。

AWS 轉換設定

存取 AWS 轉換主控台並啟動新的現代化專案，開始您的現代化旅程。此步驟會建立您的工作區，並為完整堆疊轉換設定基礎組態。

要完成的動作：

- 在 AWS 管理主控台中導覽至 AWS 轉換服務
- 從服務選項中選取 Microsoft Modernization
- 選擇建立新的現代化專案
- 提供專案名稱和描述
- 選取您的目標 AWS 區域（必須符合您的 SQL Server 位置）
- 檢閱並確認專案設定

> **Note**
>
> 最佳實務：使用包含應用程式名稱和目標環境（例如 'CustomerPortal-Production-Modernization') 的描述性專案名稱，在多波案例中輕鬆識別專案。

建立 SQL Server 現代化任務

連接資料庫和原始程式碼儲存庫

設定資料庫連接器

透過設定資料庫連接器，建立與 SQL Server 資料庫的安全連線。連接器會執行環境分析、相依性探索，並讓 AWS Transform 存取資料庫結構描述和中繼資料，以進行評估和轉換。

要完成的動作：

- 從設定精靈中選取設定資料庫連接器
- 選擇連線方法：新連線或現有連線
- 提供 SQL Server 連線詳細資訊（端點、連接埠、資料庫名稱）
- 設定身分驗證和測試連線
- 檢閱探索到的資料庫並確認選取

> **Note**
>
> 網路連線：確保您的 SQL Server 安全群組和 NACLs 允許來自 AWS 轉換服務端點的傳入連線。

連接原始程式碼儲存庫

啟用 AWS 轉換以存取您的 .NET 應用程式原始碼。 AWS 轉換支援三種提供原始碼的方法：個人存取字符 (PAT) 連接器 （ 建議 ）、 AWS CodeConnections 或 Amazon S3。此整合可讓服務分析您的應用程式程式碼、識別資料庫相依性，以及執行自動化程式碼轉換以實現 PostgreSQL 相容性。

要完成的動作：

- 導覽至連線來源碼儲存庫區段
- 選擇您的身分驗證方法：PAT Connector （ 建議 ）、AWS CodeConnections 或 Amazon S3
- 選取包含 .NET 應用程式的儲存庫
- 指定用於分析的分支 （ 通常是主要/主要或開發 ）
- 驗證儲存庫存取和程式碼結構

> **Note**
>
> 儲存庫探索： AWS Transform 會自動掃描您的儲存庫，以識別 .NET 專案、實體架構組態、資料庫連線字串和 SQL 相依性。

> **Note**
>
> 安全備註： AWS Transform 只需要對儲存庫的讀取存取權，並為轉換的程式碼建立新的功能分支。您的主要分支保持不變。

循環中的人類

AWS 轉換使用human-in-the-loop(HITL) 機制來確保品質，並允許您檢閱和核准重要的轉換決策。下列檢查點需要您注意：

Wave 計劃審核和核准

您檢閱的內容：提議的遷移波紋，包括將哪些資料庫和應用程式分組在一起，以及波紋順序。

您可以：

- 核准波動計畫
- 透過在波之間移動資料庫來自訂波
- 修改波動序列
- 分割或合併波

核准後， AWS Transform 會繼續進行結構描述轉換。

結構描述轉換檢閱

您檢閱的內容：轉換的資料庫物件，包括資料表、預存程序、函數和觸發。動作項目會反白顯示需要注意的物件。

您可以：

- 接受轉換後的程式碼
- 修改轉換後的程式碼
- 轉換後人工檢閱的旗標
- 檢視原始程式碼和轉換程式碼的side-by-side比較

核准後會發生的情況： AWS Transform 會將結構描述套用至 Aurora PostgreSQL，並繼續資料遷移（如果已設定）。

應用程式程式碼檢閱

您檢閱的內容：所有應用程式碼變更，包括實體架構組態、連線字串、資料存取碼和預存程序呼叫。

您可以：

- 接受每個檔案的變更
- 修改轉換的程式碼
- 拒絕變更（不建議）
- 為您的團隊新增評論

- 下載轉換後的程式碼以供本機檢閱

核准後會發生什麼情況： AWS Transform 會將變更遞交至儲存庫中的新分支，並繼續驗證。

驗證結果檢閱

您檢閱的內容：自動化驗證結果，包括結構描述相容性、資料完整性檢查和應用程式建置狀態。

您可以：

- 檢閱通過的測試
- 調查失敗的測試
- 地址警告
- 繼續部署或返回以修正問題

核准後會發生什麼： AWS Transform 準備部署到您的目標環境。

部署核准

您檢閱的內容：部署組態，包括infrastructure-as-code範本、ECS 服務組態和部署設定。

您可以：

- 檢閱和自訂部署設定
- 核准部署以繼續
- 額外測試的延遲部署
- 下載基礎設施程式碼以供檢閱

核准後， AWS Transform 會將您的現代化應用程式和資料庫部署到目標環境。

評估和波動規劃

設定登陸區域

設定要部署現代化應用程式的目標基礎設施環境。登陸區域設定包括 Aurora PostgreSQL 佈建、聯網組態和參考部署組態。

要完成的動作：

- 從組態功能表中選取設定登陸區域
- 設定 Aurora PostgreSQL 目標（版本、執行個體類別、異地同步備份）
- 設定網路和安全性設定 (VPC、子網路、安全群組）

> **Note**
>
> 成本考量：Aurora PostgreSQL 執行個體會產生持續成本。考慮將 Aurora Serverless v2 用於開發/測試環境。

評估

對資料庫結構描述、應用程式程式碼和相依性進行全面分析。評估階段提供轉換複雜性評分、識別潛在挑戰，並產生詳細報告。

要完成的動作：

- 選取儲存庫分支以進行程式碼分析
- 選取用於轉換的儲存庫和資料庫
- 檢閱評估結果和複雜性評分
- 使用工作量預測產生評估報告
- 匯出報告以供利益相關者檢閱和核准

> **Note**
>
> Assessment Insights：評估提供結構描述物件、預存程序、應用程式相依性的詳細分析，並估計所需的人工介入程度。

波規劃

根據轉型複雜性、業務優先順序和應用程式相依性，將您的現代化組織為可管理的波浪。 AWS Transform 會產生您可以自訂的智慧型波浪建議。

要完成的動作：

- 檢閱 AI 產生的 Wave 計畫和建議

- 根據業務優先順序自訂 Wave 組態
- 驗證應用程式和資料庫之間的相依性
- 使用對話界面完成 Wave 計劃
- 設定波動執行優先順序並指派責任

> **Note**
>
> 採用 AI 技術的建議：您可以透過自然語言與 AI 互動，以調整建議：「將 CustomerDB 移至 Wave 1」或「將這兩個應用程式組合成同一波」。

> **Note**
>
> 最佳實務：從包含 1-2 個低複雜度資料庫的試行波開始，以建立程序並建立團隊的可信度。

每一波的資料遷移

每一波的結構描述轉換

使用 AI 增強的轉換功能，將 SQL Server 資料庫結構描述轉換為 PostgreSQL 相容對等項目。此程序會轉換資料表、預存程序、函數、觸發程序和其他資料庫物件。

要完成的動作：

- 提供結構描述轉換目標並設定偏好設定
- 使用 DMS 結構描述轉換服務執行自動轉換
- 檢閱轉換結果並識別人工介入項目
- 透過 HITL 提示處理手動介入
- 驗證人工更正，並視需要重新執行轉換

> **Note**
>
> 常見的手動介入：連結的伺服器、使用者定義的類型、進階 T-SQL 模式和廠商特定的 SQL 功能通常需要人工檢閱和更正。

每一波的資料遷移

使用 AWS Database Migration Service (AWS DMS) 整合，將資料從 SQL Server 傳輸到 Aurora PostgreSQL。在生產資料遷移或合成資料產生之間進行選擇，以進行測試。

要完成的動作：

- 選擇生產資料遷移或合成資料產生
- 設定 DMS 複寫執行個體以進行資料傳輸
- 監控遷移進度並處理資料不一致
- 驗證資料完整性和參考限制
- 在繼續之前確認成功完成

> **Note**
>
> 自動化 DMS 整合： AWS 轉換會抽象化 DMS 組態的複雜性，自動處理端點建立、任務組態和資料類型映射。

> **Note**
>
> 資料驗證：服務透過對來源和目標資料庫執行相同的查詢來執行經驗測試，以確保資料一致性。

每一波的程式碼遷移

轉換 .NET 應用程式程式碼以使用 Aurora PostgreSQL，包括實體架構組態更新、連線字串修改、SQL 查詢調整和架構特定調整。

要完成的動作：

- 執行 SQL Server 相依性的自動化程式碼分析
- 執行架構轉換（實體架構提供者更新）
- 將 SQL 查詢語法調整為 PostgreSQL 相容 SQL
- 設定轉換程式碼的目標分支管理

- 處理複雜模式的手動介入

SQL Server 現代化工作流程

本節提供使用 AWS 轉換完成 SQL Server 現代化程序的step-by-step演練。

步驟 1：建立 SQL Server 現代化任務

在轉換 AWS 主控台中建立新的轉換任務，開始您的現代化旅程。

1. 登入 AWS Transform 主控台
2. 選擇建立現代化任務
3. 選取 Windows 現代化任務，然後選取 SQL Server 現代化
4. 輸入任務詳細資訊：
   - 任務名稱：專案的描述性名稱
   - 描述：選用描述
   - 部署的目標區域： AWS 區域
5. 選擇 Create job (建立任務)

> **Important**
> 請勿在任務名稱中包含個人身分識別資訊 (PII)。

步驟 2：連線至 SQL Server 資料庫

將 AWS 轉換連接至 SQL Server 資料庫，以啟用結構描述分析和轉換。

建立資料庫連接器

1. 在您的 SQL Server 現代化任務中，導覽至連線至 資源
2. 選擇連線至 SQL Server 資料庫
3. 選擇建立新連接器
4. 輸入連接器資訊：
   - Connector 名稱：描述性名稱
   - AWS 帳戶 ID：託管 SQL Server 的帳戶

5. 確認後，您會收到核准的連結。複製核准連結，從您帳戶的 AWS 管理員取得核准。核准後，您就可以繼續進行下一個步驟。
6. 管理員核准連接器請求後，請按一下提交以繼續至原始碼連線設定。

步驟 3：連接原始程式碼儲存庫

AWS 轉換需要存取 .NET 應用程式原始程式碼，以分析和轉換與 SQL Server 資料庫互動的程式碼。AWS 轉換支援提供原始程式碼的三種方法。

選擇您的身分驗證方法

個人存取字符 (PAT) 連接器 （建議）

最適合需要自訂許可範圍、自我託管供應商支援或存取供應商特定 APIs團隊，例如 GitHub Secrets。您可以在原始碼提供者中建立具有自訂許可的 PAT、將它存放在 中 AWS Secrets Manager，然後視需要 AWS 進行轉換擷取。您負責管理權杖輪換和過期。

AWS CodeConnections

最適合需要自動憑證管理的團隊。 AWS CodeConnections 使用透過 OAuth 2.0 授權流程處理身分驗證的受管供應商整合。 AWS 會管理整個憑證生命週期，包括自動權杖重新整理和輪換。不需要手動憑證管理。

Amazon S3

將您的原始碼直接上傳至 Amazon S3 儲存貯體。 AWS 轉換會在轉換任務期間從儲存貯體存取程式碼。

功能	PAT 連接器 （建議）	AWS CodeConnections
憑證管理	手動 （客戶受管）	自動AWS（受管）
字符生命週期	需要手動輪換	自動重新整理
許可彈性	完全可自訂的範圍	已修正許可
自我託管提供者支援	支援	不適用
設定複雜性	中等 （手動權杖建立和儲存）	低 （一次性授權）
字符儲存	客戶的 AWS Secrets Manager	AWS受管

設定 PAT 連接器 （ 建議 ）

使用 PAT 連接器，您可以在具有自訂許可的原始碼提供者中建立個人存取字符，將其安全地存放在 中 AWS Secrets Manager，並視需要 AWS 轉換擷取它。您負責管理字符生命週期，包括輪換和過期。AWS Transform 會自動建立具有存取秘密許可的必要 IAM 角色。

PAT 連接器支援下列提供者，包括自我託管和自訂 DNS/URL 版本：

- GitHub 和 GitHub Enterprise Server
- GitLab.com 和 GitLab 自我管理
- Bitbucket 雲端和 Bitbucket 資料中心
- Azure DevOps 和 Azure DevOps 伺服器

建立個人存取字符

在原始碼提供者中建立 PAT。所需的許可因提供者而異。選擇供應商的索引標籤。

> **Important**
>
> 建立後立即複製字符。您無法再次檢視它。設定轉換任務持續時間的過期時間。請勿將過期設定為永不過期。

> **Warning**
>
> 切勿將 PAT 字符遞交至程式碼儲存庫，或透過不安全的管道共用它們。一律將其存放在 中 AWS Secrets Manager。

GitHub

導覽至設定、開發人員設定、個人存取字符、精細字符。選取要轉換的儲存庫，並授予下列許可。

儲存庫許可

權限	存取	用途
目錄	讀取和寫入	讀取原始程式碼並將轉換後的程式碼寫回儲存庫

權限	存取	用途
中繼資料	唯讀	存取基本儲存庫資訊

組織許可（組織儲存庫需要）

權限	存取	用途
成員	唯讀	列出可供儲存庫探索字符存取的組織

GitLab

導覽至編輯設定檔、存取字符。選取下列範圍。

Scope (範圍)	用途
`read_api`	讀取儲存庫中繼資料、專案資訊、使用者詳細資訊，並列出群組和分支
`read_repository`	讀取來源碼檔案和儲存庫結構以供分析
`write_repository`	將轉換的程式碼寫回儲存庫

Bitbucket

導覽至帳戶設定、安全性、建立和管理 API 權杖。所需的範圍取決於您的字符類型。

工作區/儲存庫字符 (ATCT — 承載身分驗證，不需要使用者名稱）

權限	存取	用途
儲存庫	讀取和寫入	列出儲存庫、讀取分支，並透過 git 推送寫入轉換的程式碼

帳戶 API 字符 (ATAT — 含電子郵件的基本身分驗證） 或應用程式密碼 (ATBB — 含使用者名稱的基本身分驗證）

Scope (範圍)	用途
`read:account`	識別已驗證的使用者以解析儲存庫成員資格
`read:workspace:bitbucket`	列出字符可以存取的工作區，以便 AWS 轉換可以列舉其儲存庫。如果您在秘密中指定工作區清單，則不需要。
`read:repository:bitbucket`	列出儲存庫並讀取中繼資料和分支資訊
`write:repository:bitbucket`	透過 git 推送將轉換的程式碼寫回儲存庫

Azure DevOps

導覽至使用者設定、個人存取字符。選取自訂定義的範圍。針對組織範圍，選擇所有可存取的組織（建議）或指定單一組織。

Scope (範圍)	存取	用途
Code	讀取和寫入	讀取原始程式碼、列出儲存庫和分支，以及將轉換後的程式碼寫回
使用者設定檔	讀取	驗證字符存取並探索使用者身分以進行組織查詢
成員權利管理	讀取	列出可供儲存庫探索字符存取的組織

將 PAT 存放在 AWS Secrets Manager

1. 開啟 AWS Secrets Manager 主控台。
2. 選擇存放新的機密。
3. 針對機密類型，選擇其他類型的機密。
4. 根據您的提供者和託管類型新增鍵/值對：
   - 雲端託管提供者 — 使用 `token` PAT 新增名為 的金鑰做為 值。
     - 對於具有特定組織的 Azure DevOps，也請使用您的組織名稱新增名為 `organization` 的金鑰。

    - 對於 Bitbucket 應用程式密碼 (ATBB)，也請使用您的 Bitbucket 使用者名稱新增名為 `username`的金鑰。對於 Bitbucket 帳戶 API 字符 (ATAT)，請使用您的 Bitbucket 電子郵件地址新增名為 `email`的金鑰。
- 自我託管和自訂 DNS/URL 提供者 — 新增下列金鑰： `host`（您的伺服器 URL，例如 `https://github.mycompany.com`)、 `provider_type`(`github`、`bitbucket`、 `gitlab`或 `ado`) 和 `token`（您的 PAT)。
    - 對於具有特定組織的 Azure DevOps，也請使用您的組織名稱新增名為 `organization` 的金鑰。
    - 對於 Bitbucket 應用程式密碼 (ATBB)，也請使用您的 Bitbucket 使用者名稱新增名為 `username`的金鑰。對於 Bitbucket 帳戶 API 字符 (ATAT)，請使用您的 Bitbucket 電子郵件地址新增名為 `email`的金鑰。

    下列範例顯示秘密如何 AWS Secrets Manager 尋找 GitHub 雲端託管提供者：

    ```
    {
      "token": "your-github-personal-access-token"
    }
    ```

    下列範例顯示 Bitbucket 應用程式密碼 (ATBB)：

    ```
    {
      "token": "your-bitbucket-app-password",
      "username": "my-bitbucket-username"
    }
    ```

    下列範例顯示自我託管的 GitLab 執行個體：

    ```
    {
      "host": "https://gitlab.mycompany.com",
      "provider_type": "gitlab",
      "token": "your-gitlab-personal-access-token"
    }
    ```

5. 選擇下一步。
6. 輸入秘密名稱，例如 `github-pat-myproject`。
7. （選用）選取要加密的客戶受管 KMS 金鑰。
8. 完成精靈，然後選擇儲存。

9. 複製秘密 ARN。設定 AWS 轉換任務時，您需要此值。

如果您使用客戶受管 KMS 金鑰來加密秘密（而非預設受管金鑰），則必須更新 KMS AWS金鑰政策，以允許 AWS Transform 解密秘密。將下列陳述式新增至客戶管理的 KMS 金鑰政策：

```
{
  "Sid": "Allow AWS Transform to decrypt secrets",
  "Effect": "Allow",
  "Principal": {
    "Service": "transform.amazonaws.com"
  },
  "Action": [
    "kms:Decrypt",
    "kms:DescribeKey"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:ViaService": "secretsmanager.REGION.amazonaws.com",
      "kms:EncryptionContext:SecretARN": "YOUR-SECRET-ARN"
    }
  }
}
```

將 *REGION* 取代為您的 AWS 區域（例如 us-east-1），並將 *YOUR-SECRET-ARN* 取代為您秘密的 ARN。kms:ViaService 條件可確保 KMS 金鑰只能透過 AWS Secrets Manager 服務使用。kms:EncryptionContext:SecretARN 條件會將解密限制為您的特定秘密。

若要更新您的 KMS 金鑰政策：

1. 在 開啟 AWS KMS 主控台https://console.aws.amazon.com/kms。
2. 在導覽窗格中，選擇 Customer managed keys (客戶受管金鑰)。
3. 選取您的 KMS 金鑰。
4. 在金鑰政策標籤中，選擇編輯。
5. 將政策陳述式新增至現有政策。
6. 選擇儲存變更。

> **Note**
>
> 如果您使用預設受管金鑰 AWS(`aws/secretsmanager`)，則不需要修改任何 KMS 金鑰政策。

設定 AWS 轉換任務

1. 在您的 AWS 轉換任務中，導覽至連線至 資源。
2. 選擇 Connect 原始碼儲存庫。
3. 選取 PAT Connector 做為身分驗證方法。
4. 輸入步驟 2 中的秘密 ARN。
5. （選用）如果您使用客戶管理的 KMS 金鑰，請輸入 KMS 金鑰 ARN。
6. 選取您的儲存庫和分支。
7. 選擇繼續。

AWS 轉換會自動建立具有存取秘密所需許可的 IAM 角色。

權杖輪換和維護

您有責任在 PAT 權杖過期之前輪換它們。若要輪換權杖：

1. 在您的原始碼提供者中產生具有相同許可的新 PAT。
2. 更新 中的秘密值 AWS Secrets Manager。
3. 確認您的 AWS 轉換任務可以使用新的字符存取儲存庫。
4. 撤銷原始碼提供者中的舊 PAT。

故障診斷 PAT 連接器問題

拒絕存取 — 無效的 PAT

確認 PAT 尚未過期。確認 PAT 具有您的提供者所需的範圍。檢查 PAT 是否正確存放於其中 AWS Secrets Manager。

無法擷取秘密

驗證秘密 ARN 是否正確。檢查任務日誌以確認 AWS Transform 已建立 IAM 角色。如果您使用客戶管理的 KMS 金鑰，請驗證金鑰政策。

許可不足

PAT 可能缺少操作所需的範圍。使用所需的範圍重新產生 PAT，並在其中更新秘密值 AWS Secrets Manager。

設定 AWS CodeConnections

AWS CodeConnections 使用受管提供者整合，透過 OAuth 2.0 授權流程自動擷取臨時 OAuth 憑證。許可是在提供者應用程式中設定，並完全由 管理 AWS。您授權應用程式一次，並 AWS 處理所有登入資料管理。

1. 在您的 SQL Server 現代化任務中，導覽至連線至 資源。
2. 選擇 Connect 原始程式碼儲存庫。
3. 如果您沒有現有的連線，請選擇建立連線。
4. 選取您的儲存庫提供者：
   - GitHub / GitHub Enterprise
   - GitLab.com
   - Bitbucket Cloud
   - Azure 儲存庫
5. 遵循供應商的授權流程。
6. 授權後，選擇連線。

選取您的儲存庫和分支

1. 從清單中選取您的儲存庫。
2. 選擇您要轉換的分支（通常是主要分支、主要分支或開發分支）。
3. （選用）如果您的 .NET 應用程式不在儲存庫根目錄中，請指定子目錄。
4. 選擇繼續。

> **Note**
>
> AWS 轉換會為轉換的程式碼建立新的分支。您可以透過一般程式碼檢閱程序來檢閱和合併變更。

儲存庫存取核准

對於 GitHub 和其他一些平台，儲存庫管理員必須核准連線請求：

1. AWS 轉換會顯示驗證連結。
2. 與您的儲存庫管理員共用此連結。
3. 管理員會在其儲存庫設定中檢閱和核准請求。
4. 管理員核准請求後，連線狀態會變更為已核准。

> **Important**
>
> 核准程序可能需要一些時間，視您組織的政策而定。請妥善規劃。

步驟 4：建立部署連接器（選用）

如果您想要將轉換的應用程式部署到 AWS 您的帳戶，您可以選擇部署連接器。

設定部署連接器

1. 如果您想要部署應用程式，請選取是。選取否會略過此步驟。
2. 新增您要部署轉換應用程式 AWS 的帳戶。
3. 新增可協助您輕鬆記住連接器的名稱
4. 提交連接器請求以進行核准。

部署連接器核准

AWS 您的帳戶管理員必須核准部署連接器的連線請求。

1. AWS 轉換會顯示驗證連結
2. 與您的 AWS 帳戶管理員共用此連結
3. 管理員在其儲存庫設定中檢閱並核准請求
4. 核准後，連線狀態會變更為已核准

> **Important**
>
> 核准程序可能需要一些時間，視您組織的政策而定。請妥善規劃。

步驟 5：確認您的資源

連線至資料庫和儲存庫後， AWS Transform 會驗證所有必要的資源是否可存取並準備好進行轉換。

AWS 轉換驗證的內容

- 資料庫連線：連線作用中、使用者具有必要的許可、可存取資料庫、支援版本
- 儲存庫存取：可存取儲存庫、分支存在、偵測到 .NET 專案檔案、可探索資料庫連線
- 環境準備：VPC 組態支援 DMS、存在必要的 AWS 服務角色、已建立網路連線、已確認區域相容性

檢閱飛行前檢查清單

1. 導覽至在任務計畫中確認您的資源
2. 檢閱檢查清單項目：
   - # 資料庫連線已驗證
   - # 儲存庫存取已確認
   - # 支援的 .NET 版本
   - # 偵測到實體架構或 ADO.NET
   - # 網路組態有效
   - # 授予的必要許可
3. 如果所有項目都顯示為完成，請選擇繼續
4. 如果有任何項目顯示警告或錯誤，請在繼續之前解決它們

步驟 6：探索和評估

AWS Transform 會分析 SQL Server 資料庫和 .NET 應用程式，以了解現代化的範圍和複雜性。

探索的內容

- 資料庫物件：資料表、檢視、索引、預存程序、函數、觸發條件、限制條件、資料類型、運算資料欄、身分資料欄、外部索引鍵關係

- 應用程式碼：.NET 專案結構、實體架構模型和組態、ADO.NET 資料存取碼、資料庫連線字串、預存程序呼叫、程式碼中的 SQL 查詢
- 相依性：哪些應用程式使用哪些資料庫、跨資料庫相依性、共用預存程序、常見的資料存取模式

探索程序

- AWS 轉換會在資源確認後自動開始探索
- 探索通常需要 5-15 分鐘，取決於資料庫大小和應用程式的複雜性
- 監控工作日誌中的進度
- AWS 轉換會在發現物件時顯示即時更新

檢閱探索結果

探索完成後，導覽至探索和評估以檢閱：

資料庫分析：

- 物件計數：資料表、檢視、預存程序、函數、觸發器的數量
- 複雜性分數：評估轉換複雜性（低、中、高）
- 動作項目：可能需要人工注意的物件
- 支援的功能：會自動轉換的資料庫功能
- 不支援的功能：需要解決方法的功能

應用程式分析：

- 專案類型：ASP.NET Core、主控台應用程式、類別程式庫等。
- .NET 版本：偵測到的 .NET Core 版本
- 資料存取架構：實體架構版本或 https：//ADO.NET
- 資料庫連線：找到的連線字串數目
- 程式碼複雜性：評估轉換複雜性

相依性映射：

- application-to-database關係的視覺化呈現
- 跨資料庫相依性

- 共用元件

了解複雜性評估

AWS 轉換會將您的現代化分為三個類別：

複雜性	特性	預期結果
低 （類別 A)	標準 SQL 模式 (ANSI SQL)、簡易預存程序、基本資料類型、具有標準組態的實體架構	預期人力介入最少，自動化成功率高
中 (B 類）	進階 T-SQL 模式、具有商業邏輯的複雜預存程序、使用者定義的函數、運算資料欄	需要一些人工介入，建議進行專家審查
高 (C 類）	CLR 組件、連結的伺服器、Service Broker、複雜的全文搜尋	需要大量人工重構，考慮分階段方法

評估報告

AWS 轉換會產生詳細的評估報告，其中包括：

- 具有高階概觀的執行摘要
- 完成資料庫清查
- 應用程式庫存
- 轉換準備度百分比
- 嘗試估算
- 風險評估和緩解策略
- 建議方法

您可以下載評估報告，以便離線檢閱並與利益相關者共用。

步驟 7：產生並檢閱波動計畫

對於具有多個資料庫和應用程式的大型資產， AWS Transform 會產生波動計畫，在邏輯群組中序列化現代化。

什麼是波動計畫？

波動計畫會根據下列項目將您的現代化組織成階段（波動）：

- 資料庫和應用程式之間的相依性
- 業務優先順序
- 風險承受能力
- 資源可用性
- 技術複雜性

每個波動都包含一組資料庫和應用程式，這些資料庫和應用程式可以一起現代化，而不會中斷相依性。

檢閱波動計畫

1. 導覽至任務計畫中的 Wave 規劃
2. 檢閱提議的波紋
3. 對於每個波動，請檢閱：
   - 包含的資料庫
   - 包含的應用程式
   - 其他波的相依性
   - 預估轉換時間
   - 複雜性層級
   - 可部署的應用程式

自訂波動計畫

您可以透過 2 種方式自訂波動計畫，以符合您的業務需求：

使用 JSON：

1. 選擇下載所有波，以取得具有所有波的 JSON 檔案
2. 在 JSON 中修改波浪的方式如下：
   - 在波浪之間移動資料庫
   - 將波分成較小的群組
   - 將波浪合併在一起

- 變更波動序列
- 從範圍新增或移除資料庫

3. 選擇上傳波動計畫，將 JSON 檔案上傳回主控台
4. AWS 轉換會驗證您的變更，並在違反相依性時發出警告
5. 選擇確認波浪以更新波浪計劃

使用聊天：

您可以與客服人員聊天，並要求其將儲存庫和資料庫移至特定波，以修改波計畫。如果您需要對波浪進行次要編輯，則此方法可正常運作。

> **Important**
>
> 確保在自訂波時遵守相依性。在資料庫可能導致問題之前轉換相依的應用程式。

單一資料庫現代化

如果您正在現代化單一資料庫和應用程式， AWS Transform 會建立一個波動的簡單計劃。您可以直接進行轉換，無需波浪規劃。

核准波動計畫

1. 在檢閱和自訂（如有需要）之後，選擇核准波動計畫
2. AWS 轉換會鎖定波動計畫並繼續轉換
3. 您稍後仍然可以選擇編輯波動計畫來修改計畫

步驟 8：結構描述轉換

AWS 轉換會將 SQL Server 資料庫結構描述轉換為 Aurora PostgreSQL，包括資料表、檢視、預存程序、函數和觸發。

結構描述轉換的運作方式

AWS 轉換使用透過生成式 AI 增強的 AWS DMS 結構描述轉換來：

- 分析 SQL Server 結構描述和關係

- 將資料類型從 SQL Server 映射至 PostgreSQL 對等項目
- 將 T-SQL 轉換為 PL/pgSQL
- 處理身分資料欄、運算資料欄和限制條件
- 驗證轉換和參考完整性
- 為需要人工檢閱的物件產生動作項目

支援的轉換

自動轉換：

- 資料表、檢視和索引
- 主索引鍵和外部索引鍵
- 檢查限制條件和預設值
- 最常見的資料類型
- 簡單預存程序
- 基本函數和觸發條件
- 身分資料欄（轉換為 SERIAL 或 GENERATED)
- 最常運算的資料欄

可能需要人工審核：

- 使用進階 T-SQL 的複雜預存程序
- SQL Server 特定函數 (GETUTCDATE、SUSER_SNAME 等）
- 具有複雜表達式的運算資料欄
- 全文搜尋索引
- XML 資料類型操作
- HIERARCHYID 資料類型（需要 ltree 延伸）

未自動轉換：

- CLR 組件
- 連結伺服器
- Service Broker

- SQL Server 代理程式任務

開始結構描述轉換

1. 導覽至任務計畫中的結構描述轉換
2. 檢閱轉換設定：
   - Target PostgreSQL 版本
   - 延伸選項 (ltree、PostGIS 等)
   - 命名慣例
3. 選擇開始轉換
4. 監控工作日誌中的進度
5. 轉換通常需要 10-30 分鐘，取決於資料庫物件的數量

檢閱轉換結果

轉換完成後，導覽至檢閱結構描述轉換：

轉換摘要：

- 轉換的物件：成功轉換的物件計數
- 動作項目：需要人為注意的物件
- 警告：要檢閱的潛在問題
- 錯誤：無法轉換的物件

依物件類型檢閱：

- 資料表：資料類型映射、限制條件、索引
- 存放程序：T-SQL 轉換為 PL/pgSQL
- 函數：函數簽章和邏輯變更
- 觸發：觸發語法和時間變更

檢閱動作項目

1. 選擇檢視動作項目
2. 針對每個動作項目，檢閱：

- 物件名稱：資料庫物件
- 問題類型：什麼需要注意
- 嚴重性：關鍵、警告或資訊
- 建議：建議的解析度
- 原始程式碼：SQL Server 版本
- 轉換後的程式碼：PostgreSQL 版本

3. 對於每個動作項目，您可以：
   - 接受：使用轉換後的程式碼
   - 修改：編輯轉換後的程式碼
   - 稍後標記：標記以在轉換後進行人工檢閱

範例：預存程序轉換

SQL Server T-SQL：

```
CREATE PROCEDURE GetProductsByCategory
    @CategoryId INT,
    @PageSize INT = 10
AS
BEGIN
    SET NOCOUNT ON;

    SELECT TOP (@PageSize)
        ProductId,
        Name,
        Price,
        DATEDIFF(DAY, CreatedDate, GETUTCDATE()) AS DaysOld
    FROM Products
    WHERE CategoryId = @CategoryId
    ORDER BY Name
END
```

轉換後的 PostgreSQL PL/pgSQL：

```
CREATE OR REPLACE FUNCTION get_products_by_category(
    p_category_id INTEGER,
    p_page_size INTEGER DEFAULT 10
)
```

```
RETURNS TABLE (
    product_id INTEGER,
    name VARCHAR(255),
    price NUMERIC(18,2),
    days_old INTEGER
) AS $$
BEGIN
    RETURN QUERY
    SELECT
        p.product_id,
        p.name,
        p.price,
        EXTRACT(DAY FROM (NOW() - p.created_date))::INTEGER AS days_old
    FROM products p
    WHERE p.category_id = p_category_id
    ORDER BY p.name
    LIMIT p_page_size;
END;
$$ LANGUAGE plpgsql;
```

所做的變更：

- 程序轉換為函數傳回 TABLE
- 字首為 p_ 的參數名稱
- TOP 轉換為 LIMIT
- DATEDIFF 轉換為 EXTRACT
- GETUTCDATE() 轉換為 NOW()
- 資料欄名稱轉換為小寫 (PostgreSQL 慣例)

核准結構描述轉換

1. 檢閱所有動作項目並進行必要的修改之後
2. 選擇核准結構描述轉換
3. AWS Transform 準備轉換後的結構描述以部署到 Aurora PostgreSQL

> **Note**
>
> 您可以將轉換後的結構描述下載為 SQL 指令碼，以進行離線檢閱或版本控制。

步驟 9：資料遷移 （選用）

AWS 轉換提供將資料從 SQL Server 遷移至 Aurora PostgreSQL 的選項。資料遷移是選用的，如果您只需要結構描述和程式碼轉換，則可以略過。

資料遷移選項

選項 1：生產資料遷移

使用 DMS AWS 遷移實際生產資料：

- 所有資料的完整初始載入
- 測試期間持續複寫 (CDC)
- 最短的停機時間切換
- 資料驗證和完整性檢查

選項 2：略過資料遷移

僅轉換結構描述和程式碼：

- 適用於開發/測試環境
- 何時將分別遷移資料
- 對於proof-of-concept專案

設定資料遷移

1. 導覽至任務計畫中的資料遷移
2. 選擇您的遷移選項：
   - 遷移生產資料
   - 略過資料遷移
3. 若要遷移生產資料，請設定：
   - 遷移類型：完全載入或完全載入 + CDC
   - 驗證：啟用資料驗證
   - 效能：DMS 執行個體大小
   - 選擇 >開始遷移

生產資料遷移程序

如果您選擇遷移生產資料：

1. 初始同步： AWS DMS 會執行所有資料表的完整載入
2. 持續複寫：（如果啟用 CDC) 保持資料同步
3. 驗證：驗證資料列計數和資料完整性
4. 切換準備：準備最終同步

遷移時間軸：

- 小型資料庫 (< 10 GB)：30 分鐘 - 2 小時
- 中型資料庫 (10-100 GB)：2-8 小時
- 大型資料庫 (> 100 GB)：8 小時以上

資料驗證

AWS 轉換會使用下列檢查來驗證遷移的資料：

- 資料列計數比較（來源與目標）
- 主索引鍵完整性
- 外部金鑰關係
- 資料類型相容性
- 運算的資料欄結果
- Null 值處理

步驟 10：應用程式程式碼轉換

AWS 轉換會將您的 .NET 應用程式程式碼轉換為使用 Aurora PostgreSQL 而非 SQL Server。它會要求儲存庫中的目標分支名稱遞交轉換後的原始程式碼。輸入分支名稱後， AWS Transform 將建立新的分支，並啟動轉換以符合 PostgreSQL 資料庫。

要轉換的內容

實體架構變更：

- 資料庫提供者：UseSqlServer() → UseNpgsql()
- 連線字串：SQL Server 格式 → PostgreSQL 格式
- 資料類型映射：SQL Server 類型 → PostgreSQL 類型
- DbContext 組態：SQL Server 特定 → PostgreSQL 特定
- 遷移檔案：針對 PostgreSQL 相容性更新

ADO.NET 變更：

- 連線類別：SqlConnection → NpgsqlConnection
- 命令類別：SqlCommand → NpgsqlCommand
- 資料讀取器：SqlDataReader → NpgsqlDataReader
- 參數：SqlParameter → NpgsqlParameter
- SQL 語法：T-SQL → PostgreSQL SQL

組態變更：

- appsettings.json 中的連線字串
- 資料庫提供者 NuGet 套件
- 相依性注入組態
- 啟動/Program.cs 組態

開始程式碼轉換

1. 導覽至任務計畫中的應用程式轉換
2. 檢閱轉換設定：
   - 目標 .NET 版本（如果升級）
   - PostgreSQL 供應商版本
   - 程式碼樣式偏好設定
3. 選擇開始轉換
4. 監控工作日誌中的進度
5. 轉換通常需要 15-45 分鐘，取決於程式碼庫大小

步驟 11：檢閱轉換結果

在繼續部署之前，請檢閱完整的轉換結果，以確保一切已準備好進行測試。

您可以從儲存庫分支下載轉換後的程式碼，用於：

- 本機測試和驗證
- IDE 中的程式碼檢閱
- 與您的 CI/CD 管道整合
- 版本控制遞交

您也可以下載轉換摘要，以檢閱 AWS Transform 在轉換過程中所做的自然語言變更。

轉換摘要

1. 導覽至任務計畫中的轉換摘要
2. 檢閱整體結果：
   - 結構描述轉換：轉換的物件、動作項目、警告
   - 資料遷移：遷移的資料表、傳輸的資料列、驗證狀態
   - 程式碼轉換：檔案已變更、行已修改、問題已解決
   - 準備度分數：部署的整體準備度

產生轉換報告

AWS 轉換會產生全面的轉換報告：

1. 選擇產生報告
2. 選取報告類型：
   - 執行摘要：利益相關者的高階概觀
   - 技術詳細資訊：完成轉換文件
   - 動作項目：所需的人力任務清單
3. 選擇下載報告

報告包括：

- 轉換範圍和目標

- 物件和程式碼已轉換
- 遇到的問題和解決方法
- 驗證結果
- 部署準備度評估
- 測試建議

步驟 12：驗證和測試

在部署到生產環境之前，請驗證轉換的應用程式是否與 Aurora PostgreSQL 正常運作。

驗證類型

自動化驗證： AWS Transform 會執行自動化檢查：

- 針對來源資料庫的結構描述驗證
- 資料完整性驗證
- 查詢對等測試
- 連線字串驗證
- 組態驗證

人工驗證：您應該執行其他測試：

- 應用程式功能的功能測試
- 與其他系統的整合測試
- 效能測試和基準測試
- 使用者接受度測試
- 安全性測試

執行自動驗證

1. 導覽至任務計畫中的驗證
2. 選擇執行驗證
3. AWS 轉換會執行驗證測試：
   - 資料庫連線

- 結構描述相容性
- 資料完整性
- 應用程式建置
- 基本功能

4. 檢閱驗證結果：
   - 通過：成功測試
   - 失敗：需要注意的測試
   - 警告：要檢閱的潛在問題

測試檢查清單

資料庫功能：

- 可存取的所有資料表
- 存放程序正確執行
- 函數傳回預期結果
- 適當地觸發觸發
- 限制條件已正確強制執行
- 索引可改善查詢效能

應用程式功能：

- 應用程式已成功啟動
- 已建立資料庫連線
- CRUD 操作可正常運作
- 儲存的程序呼叫成功
- 交易正確遞交/轉返
- 錯誤處理如預期般運作

資料完整性：

- 資料列計數比對來源
- 主索引鍵是唯一的

- 外部金鑰有效
- 運算的資料欄正確
- 適當處理空值
- 資料類型相容

效能：

- 可接受的查詢回應時間
- 連線集區已設定
- 索引最佳化
- 沒有 N+1 查詢問題
- 批次操作效率
- 資源使用率合理

步驟 13：部署

成功驗證後，將您的現代化應用程式和資料庫部署到生產環境。

部署選項

- Amazon ECS 和 Amazon EC2 Linux

部署前檢查清單

部署至生產環境之前：

- 通過的所有驗證測試
- 已完成效能測試
- 安全性檢閱已完成
- 備份和復原計劃已記錄
- 已設定監控和提醒
- 在新環境中訓練的團隊
- 利益相關者收到部署通知
- 排定的維護時段

部署至 Amazon ECS

1. 導覽至任務計畫中的部署
2. 選擇部署到 ECS
3. 設定部署設定：
   - 叢集：選取或建立 ECS 叢集
   - 服務：設定 ECS 服務
   - 任務定義：檢閱產生的任務定義
   - 負載平衡器：設定 ALB/NLB
   - 自動擴展：設定擴展政策
4. 檢閱infrastructure-as-code(CloudFormation 範本或 AWS CDK 程式碼）
5. 選擇部署

監控部署

AWS 轉換會部署您的應用程式：

1. 建立 Aurora PostgreSQL 叢集
2. 套用資料庫結構描述
3. 載入資料（如適用）
4. 部署應用程式容器
5. 設定負載平衡器
6. 設定自動擴展

監控部署進度並驗證：

- 基礎設施佈建
- 資料庫初始化
- 應用程式部署
- 通過運作狀態檢查
- 應用程式可存取
- 資料庫連線運作中
- 顯示正常操作的日誌

部署後驗證

部署之後：

煙霧測試：

- 驗證關鍵功能
- 測試金鑰使用者工作流程
- 檢查整合點
- 監控錯誤率

效能監控：

- 追蹤回應時間
- 監控資料庫查詢
- 檢查資源使用率
- 檢閱應用程式日誌

使用者驗證：

- 執行使用者接受度測試
- 收集意見回饋
- 解決任何問題
- 記錄學到的經驗教訓

轉返程序

如果在部署之後發生問題：

立即轉返：

- 還原至先前的應用程式版本
- 切換回 SQL Server （ 如果仍然可用 ）
- 視需要從備份還原

部分轉返：

- 復原特定元件
- 保留資料庫變更
- 僅還原應用程式程式碼

轉送修正：

- 將 Hotfix 套用至 Aurora PostgreSQL 版本
- 部署更新的應用程式程式碼
- 監控解析度

> **Important**
>
> 在切換後保持 SQL Server 資料庫可用一段時間，以在需要時啟用轉返。

部署後最佳化

成功部署後：

效能調校：

- 最佳化慢查詢
- 調整連線集區設定
- 微調 Aurora PostgreSQL 參數
- 檢閱和最佳化索引

成本最佳化：

- 適當大小的 Aurora 執行個體
- 適當地設定自動擴展
- 檢閱儲存設定
- 最佳化備份保留

監控設定：

- 設定 CloudWatch 儀表板

- 設定提醒
- Enable Enhanced Monitoring (啟用增強型監控)
- 設定績效詳情

文件：

- 更新執行手冊
- 文件架構變更
- 訓練營運團隊
- 建立故障診斷指南

轉換後測試和部署

將轉換的應用程式部署到登陸區域，並驗證應用程式與轉換資料庫之間的連線，以及選擇性地設定 CI/CD 管道。會產生範例 CI/CD 管道組態做為參考，協助您實作部署自動化。此最終階段會驗證完整的現代化。

設定 資源

您需要設定部署中使用的資源，例如 IAM 角色、執行個體描述檔和 S3 儲存貯體。 AWS Transform 沒有建立 S3 儲存貯體或在您的 IAM 中進行變更的許可。此動作需要由具有建立新角色許可的使用者執行。通常是帳戶管理員。

為了簡化程序，我們提供自動執行下列動作的設定指令碼：

- 執行必要的 CloudFormation 範本
- 建立 ECS 服務連結角色
- 設定所有必要的 IAM 資源

> **Important**
>
> 依原狀執行提供的設定指令碼 - 請勿修改範本或指令碼中的任何資源名稱，因為這可能會影響部署程序。

適用於 Linux：

```
./setup.sh --region <YOUR-Region>
```

針對 Windows：

```
./setup.ps1 -Region <YOUR-Region>
```

檢查 VPC 中的安全群組

AWS 轉換會將應用程式部署到與 Aurora PostgreSQL 執行個體相同的子網路和相同的安全群組。

為了讓應用程式連線到 Aurora 執行個體，請確定此安全群組具有允許連線到相同安全群組的傳出規則，以及允許來自相同安全群組連線的傳入規則。

選取和設定應用程式

AWS 轉換 UI 會顯示可部署的應用程式清單。選取應用程式，然後按一下設定和遞交以開啟您可以指定的組態視窗：

- 應用程式的目標基礎設施：選取 ECS 或其中一個 EC2 執行個體
- 應用程式或執行個體參數

完成並關閉組態視窗後， AWS Transform：

- 根據您的組態產生部署成品
- 將這些成品遞交至您的儲存庫，包括：
  - 部署指令碼
  - CloudFormation 範本
  - CI/CD 管道組態範例 （ 可用來做為設定部署自動化的參考 ）

遞交完成後，應用程式狀態會變更為已設定並遞交。然後，您可以選取應用程式，並使用右上角的部署按鈕來啟動部署。

ECS 部署

所有具有目標 ECS 的應用程式都會部署到您帳戶中建立的新 ECS 叢集。每個應用程式部署在自己的專用容器中 - 不支援每個容器多個應用程式。您可以個別設定每個應用程式的容器參數，例如所需的 CPU 和記憶體。

EC2 部署

您可以選取其中一個提議的 EC2 執行個體，也可以設定其參數，例如執行個體類型。多個應用程式可以部署到相同的 EC2 執行個體：

- 若要將多個應用程式部署到單一執行個體，請在組態期間為每個應用程式選取相同的目標 EC2 執行個體。
- 選取與目標相同執行個體的所有應用程式都會部署到該執行個體，並指派不同的隨機連接埠。
- 請注意，如果您編輯一個應用程式的執行個體參數，然後編輯另一個以相同執行個體為目標的應用程式，則變更會影響部署到該執行個體的所有應用程式。

部署成功

成功部署後，您的應用程式會在 Aurora PostgreSQL 上執行，並降低授權成本、改善效能和雲端原生可擴展性。除非明確停止，否則任務會保持開啟狀態。這允許使用更新的部署參數進行可能重新部署的選項。

上傳 DDL 檔案 （離線工作流程）

在此工作流程中， AWS Transform 完全從上傳的 DDL 檔案現代化您的結構描述，不需要直接連線至資料庫。您可以針對 SQL Server 執行提供的擷取指令碼、上傳產生的結構描述檔案，以及 AWS 轉換探索、評估、轉換和部署結構描述至 Amazon Aurora PostgreSQL。當您的資料庫無法公開至直接連線，或您希望在授予網路存取之前進行可行性評估和結構描述轉換時，請選擇此工作流程。

> **Important**
>
> 離線工作流程只會轉換和部署您的結構描述。它不會遷移真實資料。如果可用，您可以產生合成測試資料來驗證目標。如果您需要遷移真實資料，請使用 AWS DMS 主控台建立新的資料遷移專案。

離線工作流程的先決條件

- 支援的 SQL Server 版本 (2008 R2 到 2022，所有版本）。
- PowerShell 7 或更新版本來執行擷取指令碼。PowerShell 已預先安裝在 Windows 上。在 macOS 或 Linux 上安裝 PowerShell 7+ 並使用 執行指令碼`pwsh`。請參閱 Microsoft 安裝指南。
- PATH 上可用的`sqlcmd`公用程式。請參閱 sqlcmd 公用程式。

- 至少具有 和 `VIEW ANY DEFINITION`許可`VIEW SERVER STATE`的 SQL Server 身分驗證登入（使用者名稱和密碼）。指令碼不支援 Windows 或網域身分驗證。
- 啟用 IAM Identity Center 或 IAM 身分驗證後期階段 AWS 的帳戶（建立 Aurora PostgreSQL 目標並部署轉換後的結構描述）。
- 結構描述分析和轉換階段 AWS 不需要對 進行傳入或傳出資料庫連線。

工作流程步驟

1. 上傳 DDL 檔案 — AWS Transform 在聊天中提供擷取指令碼的下載按鈕。針對 SQL Server 下載並執行指令碼。選擇性地限制擷取到具有逗號分隔包含清單（不區分大小寫）的特定資料庫。指令碼會產生 SQL DDL 檔案`.zip`的時間戳記。使用聊天上傳按鈕上傳 `.zip`（或個別`.sql`檔案）。
2. 探索 – AWS 轉換會剖析上傳的檔案，並依資料庫分組為資料庫物件（資料表、預存程序、檢視、觸發條件、索引、限制條件、序列等）編製目錄。您可以檢閱每個資料庫摘要，然後選擇要評估的資料庫。如果某些陳述式無法剖析， AWS Transform 會報告問題，並可讓您繼續使用剖析的物件、選擇特定資料庫或上傳更正的檔案。
3. 評估： AWS Transform 會評估所選資料庫的轉換可行性，並產生可下載的報告，其中包含執行摘要、每個資料庫物件摘要，以及level-of-effort (LOE) 估計。自訂 LOE 分數、上傳其他檔案，或繼續轉換。
4. 結構描述轉換： AWS 轉換會將 SQL Server 結構描述（包括 T-SQL 預存程序）轉換為 Aurora PostgreSQL，一次一個資料庫。單一資料庫會自動轉換；使用多個資料庫，您可以選擇要轉換哪個資料庫。資料庫會獨立並平行轉換。
5. 目標佈建 — 對於每個轉換的資料庫， AWS Transform 會在您的帳戶中建立或重複使用 Amazon Aurora PostgreSQL 叢集 AWS 。您可以透過引導式提示選擇聯網和目標組態。
6. 結構描述部署 — AWS Transform 會將轉換後的結構描述套用至 Aurora 叢集。部署後，修正聊天或 IDE 中的剩餘物件、產生合成測試資料（如果可用）或完成。
7. 應用程式碼現代化（選用） — AWS Transform 可以更新相關聯的 .NET 6+ 應用程式，以使用 Aurora PostgreSQL。此服務會更新來源碼中的資料庫連線，並修改實體架構和 ADO.NET 中的 ORM 程式碼，以在人工監督的統一工作流程中與 Aurora PostgreSQL 相容。使用適用於 GitHub 和 GitLab 的 AWS CodeConnections 或個人存取字符 (PAT) 連接您的原始碼儲存庫，或為包含原始碼的 zip 檔案提供 S3 URI。

> **Note**
>
> Amazon Aurora PostgreSQL 是此工作流程唯一支援的目標引擎。

離線工作流程的服務限制

下列預設限制適用於離線工作流程。有些限制可為每個帳戶設定；請聯絡您的 AWS 客戶團隊請求增加。

限制	預設	適用對象
上傳每個任務的大小	1，024 MB (1 GB)，跨任務中的所有上傳累積	上傳 DDL 檔案
每月轉換的資料庫	每個帳戶 10 個	結構描述轉換
每個資料庫的存放程序	250	結構描述轉換
並行結構描述轉換	一次 5 個資料庫	結構描述轉換
並行執行中的任務	5	每個帳戶

- 上傳大小限制是每個工作的累積預算。如果您重設輸入設定，預算會清除（這會捨棄已上傳的檔案，並在相同任務中重新執行探索和評估）。
- 當您選擇超過 5 個資料庫進行轉換時，其他資料庫會排入佇列，並在執行轉換完成時自動啟動。
- Storagestored-procedure-per-database 限制絕不會封鎖評估；只會影響結構描述轉換。

離線工作流程疑難排解

擷取指令碼

- **`pwsh: command not found`** (macOS/Linux) — 未安裝 PowerShell 7+。安裝並執行 `pwsh ./ExtractDatabaseMetadata.ps1`。
- 參考錯誤 **`sqlcmd`** — `sqlcmd`公用程式不在 PATH 上。安裝它，並確保它位於 PATH 上。
- 登入或許可錯誤：搭配 `VIEW SERVER STATE`和 使用 SQL Server 身分驗證登入`VIEW ANY DEFINITION`。不支援 Windows/網域身分驗證。
- 只有一些匯出的資料庫 — 包含清單縮小範圍。在沒有它的情況下重新執行，或指定正確的逗號分隔資料庫名稱。

上傳

- 使用大小訊息拒絕上傳 — 超過每個工作的上傳預算。上傳較小的檔案，或要求客服人員重設輸入設定，以清除相同任務中的預算。向客服人員詢問目前的剩餘預算，而不是預估。
- 不接受檔案 — 上傳指令碼.zip產生的 或個別.sql檔案。將多個檔案壓縮為單一封存。

探索

- 偵測到 SQL 語法問題 — 下載問題報告。無錯誤區段中的物件仍會編製目錄。選擇 以繼續剖析的物件、選擇特定資料庫，或上傳更正的檔案。
- 以通用名稱分組的物件 — 剖析器找不到USE [Database]陳述式。出現提示時，請提供正確的資料庫名稱。
- 找不到物件 — 檔案不包含CREATE任何陳述式，或全部無法剖析。重新上傳有效的 DDL。

評估

- LOE 預估注視 — 選擇自訂 LOE 分數、編輯範本並重新上傳以重新產生評估。
- 遺失物件 — 選擇上傳其他 SQL 檔案；探索和評估會自動重新執行。

結構描述轉換

- 資料庫轉換失敗 — AWS 轉換報告原因。回覆要求重試；轉換會重新啟動該資料庫。
- 回應傳送至錯誤的資料庫 — 當多個資料庫正在等待輸入時，請指定訊息的資料庫。您可以使用 處理特定資料庫@DatabaseName:。

目標佈建和部署

- 無法建立 Aurora 叢集 — 完成引導憑證和聯網提示，並確保帳戶具有建立 Aurora PostgreSQL 的許可。
- 有些物件未部署 — 使用部署後選項來修正聊天或 IDE 中剩餘的物件，然後重新部署。

最佳實務和疑難排解

在現代化過程中的最佳實務、常見問題及其解決方案。

ECS 應用程式日誌

CloudWatch 日誌

- 所有 ECS 容器日誌都會自動傳送至 CloudWatch Logs
- 在 CloudWatch 主控台的日誌群組下存取日誌
- 日誌群組命名格式：/aws/ecs/{application-name}
- 每個容器執行個體都會在 群組中建立新的日誌串流

檢視日誌

透過 AWS 主控台：

- 導覽至 CloudWatch > 日誌群組
- 選取應用程式的日誌群組
- 選擇相關的日誌串流以檢視容器日誌

使用 AWS CLI：

```
aws logs get-log-events --log-group-name /aws/ecs/your-app-name --log-stream-name your-
stream-name
```

常見日誌位置

- 應用程式日誌：CloudWatch Logs
- ECS 服務事件：ECS 主控台 > 叢集 > 服務 > 事件索引標籤
- 容器運作狀態/狀態：ECS 主控台 > 叢集 > 服務 > 任務索引標籤

資料庫連線管理

應用程式使用環境變數進行資料庫連線設定

如果您遇到連線問題：

- 驗證您環境變數中的目前連線設定
- 更新環境變數以視需要修改資料庫連線字串
- 連線字串變更可以透過環境變數更新進行，無需重新部署應用程式

資料庫連線問題

問題：無法將 AWS 轉換連線至 SQL Server

解決方案：

- 驗證 AWS Transform 與 SQL Server 之間的網路連線
- 檢查安全群組規則是否有適當的連接埠存取 (1433)
- 在 Secrets Manager 中確認資料庫登入資料
- 使用建立的使用者測試資料庫許可
- 確保 SQL Server 已設定為混合模式身分驗證
- 確認秘密具有必要的標籤（專案：atx-db-modernization、擁有者：資料庫連接器）

防火牆和安全群組問題

問題：連線逾時或「無法連線資料庫」錯誤

根本原因：封鎖流量的安全群組或網路 ACLs

解決方案：

1. 驗證安全群組組態：
   - 確認您的 SQL Server 安全群組具有傳入規則，允許來自 DMS 結構描述轉換安全群組的連接埠 1433
   - 檢查來源是否為安全群組 ID（例如 sg-0123456789abcdef0），而非 IP 地址
   - 確認執行個體設定檔中已正確指定 DMS 結構描述轉換安全群組
   - 確保沒有衝突的拒絕規則
2. 檢查網路 ACLs：
   - 驗證子網路層級網路 ACLs連接埠 1433 上的傳入流量
   - 確保網路 ACLs 允許傳回流量的傳出暫時性連接埠
   - 檢查資料庫子網路和 DMS 子網路網路 ACLs
3. 驗證 VPC 組態：
   - 確認 DMS 結構描述轉換執行個體和 SQL Server 位於相同的 VPC 中或具有適當的 VPC 對等互連
   - 檢查路由表允許子網路之間的流量
   - 確認沒有防火牆設備封鎖流量

4. 測試連線：
   - 在與 DMS 結構描述轉換相同的子網路中啟動測試 EC2 執行個體
   - 連接與 DMS 結構描述轉換相同的安全群組
   - 使用 telnet 或 SQL Server Management Studio 測試 SQL Server 的連線
   - 如果測試成功，問題是 AWS 轉換組態；如果失敗，問題是網路/防火牆

常見錯誤：開啟連接埠 1433 至 0.0.0.0/0（所有來源）是安全風險。一律使用安全群組型存取控制，將存取權限制為僅限 DMS 結構描述轉換安全群組。

結構描述轉換問題

問題：結構描述轉換顯示許多動作項目

解決方案：

- 檢閱轉換報告中的動作項目
- 根據影響排定優先順序
- 使用 Amazon Q Developer 進行複雜的 SQL 轉換
- 如需指引，請參閱 AWS Support
- 考慮複雜資料庫的分階段方法

應用程式轉換問題

問題：應用程式轉換無法建置

解決方案：

- 檢閱轉換報告中的建置錯誤
- 視需要設定私有 NuGet 饋送
- 視需要更新套件參考
- 檢查 Windows 特定的相依性
- 檢閱轉換日誌以了解詳細錯誤

資料遷移問題

問題：資料遷移驗證失敗

解決方案：

- 檢閱特定失敗的驗證報告
- 檢查資料類型映射
- 驗證身分資料欄組態（由預設產生與一律產生）
- 檢閱運算的資料欄表達式
- 請聯絡 AWS Support 了解複雜的資料問題

資源清除問題

問題：轉換任務失敗，發生資源錯誤

解決方案：

- 檢查現有的 DMS 資源（遷移專案、資料提供者、執行個體描述檔）
- 清除先前嘗試失敗或不完整的資源
- 確認未排定刪除秘密
- 檢查 DMS 和 Aurora PostgreSQL 的服務配額
- 如果清除無法解決問題，請聯絡 AWS Support

部署問題

問題：轉換的應用程式無法連線至 Aurora PostgreSQL

解決方案：

- 驗證 PostgreSQL 的連線字串格式
- 檢查安全群組規則
- 驗證 Secrets Manager 中的資料庫登入資料
- 確保 SSL/TLS 已正確設定
- 使用 psql 或 pgAdmin 測試連線

取得其他協助

聯絡 AWS Support 時，請提供：

- 轉換任務 ID
- AWS 帳戶 ID
- 區域
- 錯誤訊息和螢幕擷取畫面
- 轉換日誌 （可在 AWS 轉換主控台中使用）

AWS 轉換中的安全性

的雲端安全性 AWS 是最高優先順序。身為 AWS 客戶，您可以受益於資料中心和網路架構，這些架構專為滿足最安全敏感組織的需求而建置。

安全性是 AWS 與您之間的共同責任。共同責任模式將其描述為雲端的安全性，和雲端中的安全性：

- 雲端的安全性 – AWS 負責保護在 中執行 AWS 服務的基礎設施 AWS 雲端。 AWS 也為您提供可安全使用的服務。在AWS 合規計畫中，第三方稽核人員會定期測試和驗證我們安全的有效性。若要了解適用於 AWS 轉換的合規計劃，請參閱AWS 合規計劃的 服務範圍。
- 雲端的安全性 – 您的責任取決於您使用 AWS 的服務。您也必須對其他因素負責，包括資料的機密性、您公司的要求和適用法律和法規。

本文件可協助您了解如何在使用 AWS 轉換時套用共同責任模型。下列主題說明如何設定 AWS Transform 以符合您的安全與合規目標。您也會了解如何使用其他 AWS 服務來協助您監控和保護 AWS 轉換資源。

主題

- 中的資料保護 AWS Transform
- AWS 轉換的身分和存取管理
- AWS 轉換的合規驗證
- AWS 轉換中的彈性
- AWS Transform 和介面端點 (AWS PrivateLink)
- 從 VPC 存取 AWS Transform Web 應用程式

中的資料保護 AWS Transform

共同責任模型適用於 AWS 中的資料保護 AWS Transform。如此模型所述， AWS 負責保護執行所有的全域基礎設施 AWS 雲端。您負責維護在此基礎設施上託管內容的控制權。您也必須負責 AWS 服務您使用之 的安全組態和管理任務。如需有關資料隱私權的詳細資訊，請參閱資料隱私權常見問答集。如需有關歐洲資料保護的相關資訊，請參閱 AWS 安全部落格上的 AWS 共同責任模型和 GDPR 部落格文章。

基於資料保護目的，我們建議您保護 AWS 帳戶 登入資料，並使用 AWS Identity and Access Management () 設定個別使用者IAM。如此一來，每個使用者都只會獲得授予完成其任務所必須的許可。我們也建議您採用下列方式保護資料：

- 每個帳戶均要使用多重要素驗證 (MFA)。
- 使用 SSL/TLS 與 AWS 資源通訊。建議使用 TLS 1.2 或更新版本。
- 使用 設定 API 和使用者活動記錄 AWS CloudTrail。
- 使用 AWS 加密解決方案，以及其中的所有預設安全控制 AWS 服務。
- 使用進階受管安全服務 Amazon Macie，例如 ，協助探索和保護存放在其中的敏感資料 Amazon S3。
- 如果您在 AWS 透過命令列界面或 API 存取 時需要 FIPS 140-2 驗證的密碼編譯模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的更多相關資訊，請參閱聯邦資訊處理標準 (FIPS) 140-2 概觀。

我們強烈建議您絕對不要將客戶的電子郵件地址等機密或敏感資訊，放在標籤或自由格式的文字欄位中，例如名稱欄位。這包括當您使用 AWS Transform 或其他 AWS 服務 使用 AWS 管理主控台 API、AWS Command Line Interface (AWS CLI) 或 AWS SDKs時。您在標籤或自由格式文字欄位中輸入的任何資料都可能用於計費或診斷日誌。如需 AWS Transform 如何使用內容的詳細資訊，請參閱 AWS Transform 服務改進。

AWS Transform 會儲存您的問題、其回應和其他內容，例如 IDE 中的主控台中繼資料和程式碼，以產生對問題的回應。如需資料如何加密的相關資訊，請參閱 中的資料加密 AWS Transform。如需有關 如何使用您提出 AWS 的一些問題 AWS Transform 及其回應來改善服務的資訊，請參閱 AWS Transform 服務改進。

在 中 AWS Transform，您的資料會儲存在建立 AWS Transform 設定檔的 AWS 區域中。

透過交叉推論，您對 的請求 AWS Transform 可能會在存放資料的地理位置內不同區域中進行處理。如需詳細資訊，請參閱跨區域推論。

主題

- 中的跨區域處理 AWS Transform
- 中的資料加密 AWS Transform
- AWS Transform 服務改進

中的跨區域處理 AWS Transform

下列各節說明如何使用跨區域推論和跨區域呼叫來提供服務 AWS Transform 。

跨區域推論

AWS Transform 採用 Amazon Bedrock 技術，並使用跨區域推論將流量分散到不同的 AWS 區域 ，以增強大型語言模型 (LLM) 推論效能和可靠性。利用跨區域推論可實現以下目標：

- 在高需求期間提高輸送量和彈性
- 提升效能
- 存取以 Amazon Bedrock 上託管的最強大 LLMs 為基礎的新啟動 AWS Transform 功能

跨區域推論請求會保留在 內 AWS 區域 ，而該 是資料最初所在地理位置的一部分。例如，從美國 AWS Transform 組態發出的請求會保留 AWS 區域 在美國的 內。雖然跨區域推論不會變更資料儲存的位置，但您的請求和輸出結果可能會移到資料原本所在的區域之外。所有資料在透過 Amazon 的安全網路傳輸時都會進行加密。使用跨區域推論無需額外付費。

跨區域推論不會影響資料儲存的位置。如需使用 時資料存放位置的資訊 AWS Transform，請參閱 中的資料保護 AWS Transform。

AWS Transform 支援跨區域推論的區域

您對 提出的某些請求 AWS Transform 可能需要跨區域呼叫。下表說明根據發出請求的地理位置而定，您的請求可能會路由傳送到哪些區域。

來源區域	目的地區域
美國東部 (維吉尼亞北部) (us-east-1)	美國東部 (維吉尼亞北部) (us-east-1) 美國東部 (俄亥俄) (us-east-2) 美國西部 (奧勒岡) (us-west-2)
歐洲 (法蘭克福) (eu-central-1)	歐洲 (法蘭克福) (eu-central-1) 歐洲 (斯德哥爾摩) (eu-north-1) 歐洲 (米蘭) (eu-south-1)

來源區域	目的地區域
	歐洲 (西班牙) (eu-south-2) 歐洲 (愛爾蘭) (eu-west-1) 歐洲 (巴黎) (eu-west-3)
亞太地區 (孟買) (ap-south-1)	亞太地區 (東京) (ap-northeast-1) 亞太地區 (首爾) (ap-northeast-2) 亞太地區 (大阪) (ap-northeast-3) 亞太地區 (孟買) (ap-south-1) 亞太區域 (海德拉巴) (ap-south-2) 亞太地區 (新加坡) (ap-southeast-1) 亞太地區 (雪梨) (ap-southeast-2) 亞太區域 (墨爾本) (ap-southeast-4)
亞太地區 (東京) (ap-northeast-1)	亞太地區 (東京) (ap-northeast-1) 亞太地區 (大阪) (ap-northeast-3)
亞太地區 (首爾) (ap-northeast-2)	亞太地區 (東京) (ap-northeast-1) 亞太地區 (首爾) (ap-northeast-2) 亞太地區 (大阪) (ap-northeast-3) 亞太地區 (孟買) (ap-south-1) 亞太區域 (海德拉巴) (ap-south-2) 亞太地區 (新加坡) (ap-southeast-1) 亞太地區 (雪梨) (ap-southeast-2) 亞太區域 (墨爾本) (ap-southeast-4)

來源區域	目的地區域
亞太地區 (雪梨) (ap-southeast-2)	亞太地區 (雪梨) (ap-southeast-2) 亞太區域 (墨爾本) (ap-southeast-4)
歐洲 (倫敦) (eu-west-2)	歐洲 (法蘭克福) (eu-central-1) 歐洲 (斯德哥爾摩) (eu-north-1) 歐洲 (米蘭) (eu-south-1) 歐洲 (西班牙) (eu-south-2) 歐洲 (愛爾蘭) (eu-west-1) 歐洲 (倫敦) (eu-west-2) 歐洲 (巴黎) (eu-west-3)
加拿大 (中部) (ca-central-1)	Commercial AWS 區域 + Canada （中部）(ca-central-1)
南美洲 (聖保羅) (sa-east-1)	Commercial AWS 區域 + South America （聖保羅）(sa-east-1)

如需您可以使用的區域完整清單 AWS Transform，請參閱 支援的 區域 AWS Transform。

跨區域知識

當您詢問有關 AWS Transform 服務、轉換工作流程或相關文件的一般問題時 AWS ， AWS Transform 可能會向美國東部 （維吉尼亞）(us-east-1) 提出美國區域或歐洲 （法蘭克福）(eu-central-1) 的跨區域請求，以擷取文件並滿足您的請求。例如，當您詢問有關如何使用 Lambda 等 AWS 其他服務的問題時， AWS Transform 可能會進行跨區域呼叫，以擷取相關文件 AWS 來回應您的問題。下表說明根據發出請求的地理位置而定，您的請求可能會路由傳送到哪些區域。

來源區域	目的地區域
美國東部 (維吉尼亞北部) (us-east-1)	美國東部 (維吉尼亞北部) (us-east-1)

來源區域	目的地區域
歐洲 (法蘭克福) (eu-central-1)	歐洲 (法蘭克福) (eu-central-1)
歐洲 (倫敦) (eu-west-2)	歐洲 (法蘭克福) (eu-central-1)
亞太地區 (東京) (ap-northeast-1)	歐洲 (法蘭克福) (eu-central-1)
亞太地區 (雪梨) (ap-southeast-2)	歐洲 (法蘭克福) (eu-central-1)
亞太地區 (首爾) (ap-northeast-2)	歐洲 (法蘭克福) (eu-central-1)
亞太地區 (孟買) (ap-south-1)	歐洲 (法蘭克福) (eu-central-1)
加拿大 (中部) (ca-central-1)	歐洲 (法蘭克福) (eu-central-1)
南美洲 (聖保羅) (sa-east-1)	歐洲 (法蘭克福) (eu-central-1)

此設定預設為啟用。帳戶管理員可以修改此設定。停用此功能會導致無法存取 AWS Transform 需要從其他區域擷取知識的功能。這可能會導致回應不準確。

若要停用 發出的跨區域呼叫 AWS Transform：

1. 第一次設定時 AWS Transform，導覽至入門頁面並完成組態。對於現有 AWS Transform 組態，請導覽至設定頁面。
2. 切換 啟用跨區域呼叫，以回答關閉位置的一般 AWS 相關問題。

AWS Transform 適用於 Windows 跨區域推論

下表顯示您可以從中呼叫推論設定檔的來源區域，以及可路由請求的目的地區域：

來源區域	推論目的地區域
美國東部 (維吉尼亞北部) (us-east-1)	美國東部 (維吉尼亞北部) (us-east-1) 美國東部 (俄亥俄) (us-east-2) 美國西部 (奧勒岡) (us-west-2)
歐洲 (法蘭克福) (eu-central-1)	歐洲 (法蘭克福) (eu-central-1)

來源區域	推論目的地區域
	歐洲 (斯德哥爾摩) (eu-north-1) 歐洲 (米蘭) (eu-south-1) 歐洲 (西班牙) (eu-south-2) 歐洲 (愛爾蘭) (eu-west-1) 歐洲 (巴黎) (eu-west-3)
亞太地區 (東京) (ap-northeast-1)	亞太地區 (東京) (ap-northeast-1) 亞太地區 (大阪) (ap-northeast-3)
亞太地區 (雪梨) (ap-southeast-2)	亞太地區 (雪梨) (ap-southeast-2) 亞太區域 (墨爾本) (ap-southeast-4)
亞太地區 (首爾) (ap-northeast-2)	所有商業區域
亞太地區 (孟買) (ap-south-1)	所有商業區域
加拿大 (中部) (ca-central-1)	所有商業區域

AWS Transform 適用於遷移的跨區域推論

下表顯示您可以從中呼叫推論設定檔的來源區域，以及可路由請求的目的地區域：

來源區域	推論目的地區域
美國東部 (維吉尼亞北部) (us-east-1)	所有商業區域
歐洲 (法蘭克福) (eu-central-1)	所有商業區域
歐洲 (倫敦) (eu-west-2)	所有商業區域
亞太地區 (東京) (ap-northeast-1)	亞太地區 (東京) (ap-northeast-1) 亞太地區 (大阪) (ap-northeast-3)

來源區域	推論目的地區域
亞太地區 (雪梨) (ap-southeast-2)	亞太地區 (雪梨) (ap-southeast-2) 亞太區域 (墨爾本) (ap-southeast-4)
亞太地區 (首爾) (ap-northeast-2)	所有商業區域
亞太地區 (孟買) (ap-south-1)	所有商業區域
加拿大 (中部) (ca-central-1)	所有商業區域

AWS Transform 適用於大型主機跨區域推論

AWS Transform 適用於大型主機的 使用 Amazon Bedrock 地理跨區域推論。這表示您的部分呼叫可能會路由到來源區域 AWS 區域 以外的 。下表顯示您可以從中呼叫推論設定檔的來源區域，以及可路由請求的目的地區域：

來源區域	推論目的地區域
美國東部 (維吉尼亞北部) (us-east-1)	美國東部 (維吉尼亞北部) (us-east-1) 美國東部 (俄亥俄) (us-east-2) 美國西部 (奧勒岡) (us-west-2)
歐洲 (法蘭克福) (eu-central-1)	歐洲 (法蘭克福) (eu-central-1) 歐洲 (斯德哥爾摩) (eu-north-1) 歐洲 (米蘭) (eu-south-1) 歐洲 (西班牙) (eu-south-2) 歐洲 (愛爾蘭) (eu-west-1) 歐洲 (巴黎) (eu-west-3)
歐洲 (倫敦) (eu-west-2)	歐洲 (法蘭克福) (eu-central-1) 歐洲 (斯德哥爾摩) (eu-north-1)

來源區域	推論目的地區域
	歐洲 (米蘭) (eu-south-1) 歐洲 (西班牙) (eu-south-2) 歐洲 (愛爾蘭) (eu-west-1) 歐洲 (倫敦) (eu-west-2) 歐洲 (巴黎) (eu-west-3)
亞太地區 (東京) (ap-northeast-1)	亞太地區 (東京) (ap-northeast-1) 亞太地區 (大阪) (ap-northeast-3)
亞太地區 (雪梨) (ap-southeast-2)	亞太地區 (雪梨) (ap-southeast-2) 亞太區域 (墨爾本) (ap-southeast-4)
亞太地區 (首爾) (ap-northeast-2)	所有商業區域
亞太地區 (孟買) (ap-south-1)	所有商業區域
加拿大 (中部) (ca-central-1)	加拿大 (中部) (ca-central-1) 美國東部 (維吉尼亞北部) (us-east-1) 美國東部 (俄亥俄) (us-east-2) 美國西部 (奧勒岡) (us-west-2)
南美洲 (聖保羅) (sa-east-1)	所有商業區域

AWS Transform 自訂

AWS Transform 自訂使用 Amazon Bedrock 地理跨區域推論。這表示您的部分呼叫可能會路由到來源區域 AWS 區域 以外的 。下表顯示您可以從中呼叫推論設定檔的來源區域，以及可路由請求的目的地區域：

來源區域	推論目的地區域
美國東部 (維吉尼亞北部) (us-east-1)	美國東部 (維吉尼亞北部) (us-east-1) 美國東部 (俄亥俄) (us-east-2) 美國西部 (奧勒岡) (us-west-2)
歐洲 (法蘭克福) (eu-central-1)	歐洲 (法蘭克福) (eu-central-1) 歐洲 (斯德哥爾摩) (eu-north-1) 歐洲 (米蘭) (eu-south-1) 歐洲 (西班牙) (eu-south-2) 歐洲 (愛爾蘭) (eu-west-1) 歐洲 (巴黎) (eu-west-3)
歐洲 (倫敦) (eu-west-2)	歐洲 (法蘭克福) (eu-central-1) 歐洲 (斯德哥爾摩) (eu-north-1) 歐洲 (米蘭) (eu-south-1) 歐洲 (西班牙) (eu-south-2) 歐洲 (愛爾蘭) (eu-west-1) 歐洲 (倫敦) (eu-west-2) 歐洲 (巴黎) (eu-west-3)
亞太地區 (東京) (ap-northeast-1)	所有商業區域
亞太地區 (雪梨) (ap-southeast-2)	亞太地區 (雪梨) (ap-southeast-2) 亞太區域 (墨爾本) (ap-southeast-4)
亞太地區 (首爾) (ap-northeast-2)	所有商業區域

來源區域	推論目的地區域
亞太地區 (孟買) (ap-south-1)	所有商業區域
加拿大 (中部) (ca-central-1)	加拿大 (中部) (ca-central-1) 美國東部 (維吉尼亞北部) (us-east-1) 美國東部 (俄亥俄) (us-east-2) 美國西部 (奧勒岡) (us-west-2)

中的資料加密 AWS Transform

本主題提供有關傳輸中 AWS Transform 加密和靜態加密的特定資訊。

AWS Transform 根據預設提供加密，以使用 AWS 擁有的金鑰加密來保護靜態敏感客戶資料。

加密類型

傳輸中加密

使用 TLS 1.2 或更新版本的連線，保護客戶與 之間的通訊， AWS Transform 以及 AWS Transform 與其下游相依性之間的通訊。

> **Important**
>
> 當您連接探索帳戶時， AWS Transform 會在該帳戶中代表您建立 Amazon S3 儲存貯體。根據預設，該儲存貯體尚未`SecureTransport`啟用。如果您希望儲存貯體政策包含安全傳輸，則必須更新政策。如需詳細資訊，請參閱 Amazon S3 的安全最佳實務。

靜態加密

AWS Transform 使用 Amazon DynamoDB 和 Amazon Simple Storage Service (Amazon S3) 存放靜態資料。預設情況下，靜態資料會使用 AWS 加密解決方案進行加密。 會使用來自 AWS Key Management Service (AWS KMS) AWS Transform 的 AWS 擁有金鑰加密您的資料。您不需要採取任何動作來保護加密資料的 AWS 受管金鑰。如需詳細資訊，請參閱《AWS Key Management Service 開發人員指南》中的 AWS 擁有的金鑰。

資料類型	AWS擁有的金鑰加密	客戶自管金鑰加密 (選用)
客戶儲存貯體資料 客戶輸入和輸出，例如存放在 Amazon S3 儲存貯體中的程式碼和文件	已啟用	已啟用
成品存放區 中繼成品是存放在 S3 儲存貯體中程式碼轉換的一部分	已啟用	已啟用
任務目標 客戶對存放在 Amazon S3 儲存貯體中之任務的意圖	已啟用	已啟用
聊天訊息 客戶與 之間 AWS Transform 存放在 Amazon S3 儲存貯體中的訊息	已啟用	已啟用
聊天知識庫 與存放在 Amazon OpenSearch 中並透過 AWS Bedrock 處理 AWS Transform 的客戶聊天相關的索引資料	已啟用	已啟用

注意：客戶可以註冊自己的客戶受管金鑰 (CMK)，用於加密上述所有資料類型。

客戶受管金鑰是您帳戶中建立、擁有和管理 AWS 的 KMS 金鑰，可透過控制對 KMS 金鑰的存取，直接控制對資料的存取。僅支援對稱金鑰。如需建立您自己的 KMS 金鑰的資訊，請參閱《 AWS Key Management Service 開發人員指南》中的建立金鑰。

當您使用客戶受管金鑰時， AWS Transform 會使用 KMS 授予，允許授權的使用者、角色或應用程式使用 KMS 金鑰。當 AWS Transform 管理員選擇在組態期間使用客戶受管金鑰進行加密時，會為其建

立授權。此授權可讓最終使用者使用加密金鑰進行靜態資料加密。如需授權的詳細資訊，請參閱 AWS KMS中的授權。

AWS 擁有的金鑰 （預設）

> **Note**
>
> AWS 擁有的金鑰 — 預設 AWS Transform 使用這些金鑰自動加密個人身分識別資料。您無法檢視、管理或使用 AWS 擁有的金鑰，或稽核其使用方式。不過，您不需要採取任何動作或變更任何程式，即可保護加密您資料的金鑰。如需詳細資訊，請參閱 Key Management Service 開發人員指南中的 AWS 擁有 AWS的金鑰。

依預設加密靜態資料，有助於降低保護敏感資料所涉及的營運開銷和複雜性。同時，其可讓您建置符合嚴格加密合規性和法規要求的安全應用程式。

雖然您無法停用此層加密或選取替代加密類型，但您可以在建立轉換時選擇客戶受管金鑰，在現有 AWS 擁有的加密金鑰上新增第二層加密：

客戶受管金鑰 （選用）

客戶受管金鑰 — AWS Transform 支援使用您建立、擁有和管理的對稱客戶受管金鑰，以使用 AWS 擁有的金鑰在現有加密上新增第二層加密。您可以完全控制此層加密，因此能執行以下任務：

- 建立和維護金鑰政策
- 建立和維護 IAM 政策和授予操作
- 啟用和停用金鑰政策
- 輪換金鑰密碼編譯資料
- 新增 標籤
- 建立金鑰別名
- 輪換金鑰密碼編譯資料
- 新增 標籤
- 建立金鑰別名
- 安排金鑰供刪除
- 如需詳細資訊，請參閱《AWS Key Management Service 開發人員指南》中的客戶自管金鑰。

> **Note**
>
> AWS Transform 會使用 AWS 擁有的金鑰自動啟用靜態加密，免費保護個人身分識別資料。不過，使用客戶受管金鑰會產生 AWS KMS 費用。如需定價的詳細資訊，請參閱 AWS Key Management Service 定價。

如需詳細資訊 AWS KMS，請參閱什麼是 AWS Key Management Service？

如何在 中使用 AWS Transform 授予 AWS Key Management Service

AWS Transform 需要授予才能使用您的客戶受管金鑰。

當您建立使用客戶受管金鑰加密的 【資源名稱】 時， AWS Transform 會透過傳送 CreateGrant 請求至 來代表您建立授予 AWS Key Management Service。中的授予 AWS Key Management Service 用於授予客戶帳戶中 KMS 金鑰的 AWS Transform 存取權。

AWS Transform 需要授予 ，才能將客戶受管金鑰用於下列內部操作：

- 將 【KMS API】 請求傳送至 AWS KMS ，以驗證建立 【資源名稱】 時輸入的對稱客戶受管 KMS 金鑰 ID 是否有效。
- 將 【KMS API】 請求傳送至 AWS KMS ，以產生由客戶受管金鑰加密的資料金鑰。
- 將 【KMS API】 請求傳送至 AWS KMS 以解密加密的資料金鑰，以便用來加密您的資料。

您可以隨時撤銷授予的存取權，或移除服務對客戶受管金鑰的存取權。如果您這麼做， AWS Transform 則無法存取客戶受管金鑰加密的任何資料，這會影響依賴該資料的操作。例如，如果您嘗試從 AWS Transform 無法存取的加密 【資源名稱】 取得 【資源名稱】 ，則操作會傳回 AccessDeniedException 錯誤。

建立客戶自管金鑰

您可以使用 AWS 管理主控台或 AWS Key Management Service APIs 來建立對稱客戶受管金鑰。

若要建立對稱客戶受管金鑰，請遵循《 AWS Key Management Service 開發人員指南》中的建立對稱客戶受管金鑰的步驟。

若要將客戶受管金鑰與 AWS Transform 資源搭配使用，必須在金鑰政策中允許下列 API 操作：

kms:CreateGrant — 新增客戶自管金鑰的授予。授予控制對指定 KMS 金鑰的存取，以允許存取授予操作 AWS Transform 所需的 。如需詳細資訊，請參閱 AWS Key Management Service Developer Guide 中的 Using Grants。

這可讓 AWS Transform 執行下列動作：

- 呼叫 【KMS API (GenerateDataKeyWithoutPlainText/GenerateDatakey) 以產生加密的資料金鑰並將其儲存，因為資料金鑰不會立即用於加密。
- 呼叫 【KMS API (Decrypt)】 以使用儲存的加密資料金鑰來存取加密的資料。
- 設定淘汰委託人，以允許服務轉換為 RetireGrant。
- kms:DescribeKey – 提供客戶受管金鑰詳細資訊，以允許 【服務名稱】 驗證金鑰。

SQL 現代化加密

在 SQL Server 現代化程序期間， 會在您的帳戶中 AWS Transform 建立資源，例如 EC2 執行個體、ECS 叢集、ECR 映像和 S3 物件。您可以選擇提供客戶受管金鑰來加密帳戶中的資料。您需要使用金鑰 CreatedFor 和值 AWSTransform 來標記 KMS 金鑰。如果您沒有預設金鑰政策，此範例政策會列出金鑰政策中所需的最低許可。如果您有預設金鑰政策，除了預設金鑰政策之外，您仍然需要手動更新 KMS 金鑰，以允許 ECS 使用您的金鑰。

```
"Statement": [
   {
     "Effect": "Allow",
     "Principal": {
       "AWS": "arn:aws:iam::111122223333:root"
     },
     "Action": [
       "kms:Decrypt",
       "kms:GenerateDataKey"
     ],
     "Resource": "*",
     "Condition": {
       "StringLike": {
         "kms:ViaService": "s3.*.amazonaws.com",
         "kms:EncryptionContext:aws-transform": "*"
       },
       "ArnLike": {
         "aws:PrincipalArn": "arn:aws:iam::*:role/*AWSTransform*"
       }
     }
```

```
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
      },
      "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncrypt*"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:ViaService": "ec2.*.amazonaws.com"
        },
        "ArnLike": {
          "aws:PrincipalArn": "arn:aws:iam::*:role/*AWSTransform*"
        }
      }
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
      },
      "Action": "kms:CreateGrant",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:ViaService": [
            "ec2.*.amazonaws.com",
            "ecr.*.amazonaws.com"
          ]
        },
        "Bool": {
          "kms:GrantIsForAWSResource": "true"
        },
        "ArnLike": {
          "aws:PrincipalArn": "arn:aws:iam::*:role/*AWSTransform*"
        }
      }
    },
```

```
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "fargate.amazonaws.com"
      },
      "Action": "kms:GenerateDataKeyWithoutPlaintext",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:EncryptionContext:aws:ecs:clusterName": "AWSTransform*"
        }
      }
    },
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "fargate.amazonaws.com"
      },
      "Action": "kms:CreateGrant",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:EncryptionContext:aws:ecs:clusterName": "AWSTransform*"
        },
        "ForAllValues:StringEquals": {
          "kms:GrantOperations": "Decrypt"
        }
      }
    }
  ]
```

資料庫遷移的加密

在資料庫遷移程序期間，AWS Transform 會使用 AWS Database Migration Service (DMS) 來遷移您的資料庫資料。您可以選擇性地提供客戶受管金鑰，以在遷移期間加密資料庫資料。

下列政策包含三個陳述式。第一個陳述式會授予 AWS KMS 金鑰的根帳戶許可。第二個陳述式允許連接器角色在探索期間驗證金鑰。第三個陳述式允許連接器角色使用 金鑰進行 DMS 操作。

```
"Statement": [
    {
      "Sid": "Enable IAM User Permissions",
      "Effect": "Allow",
```

```
      "Principal": { "AWS": "arn:aws:iam::111122223333:root" },
      "Action": "kms:*",
      "Resource": "*"
    },
    {
      "Sid": "Allow connector role to validate key during discovery",
      "Effect": "Allow",
      "Principal": { "AWS": "connector-role-arn" },
      "Action": "kms:DescribeKey",
      "Resource": "*"
    },
    {
      "Sid": "Allow connector role to use key via DMS",
      "Effect": "Allow",
      "Principal": { "AWS": "connector-role-arn" },
      "Action": [
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:DescribeKey",
        "kms:Encrypt",
        "kms:GenerateDataKey*",
        "kms:ReEncrypt*"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "kms:ViaService": "dms.us-east-1.amazonaws.com"
        }
      }
    }
  ]
```

使用客戶自管 KMS 金鑰

建立客戶受管 KMS 金鑰之後， AWS Transform 管理員必須在 AWS Transform 主控台中提供金鑰，以使用它來加密資料。

若要設定客戶受管金鑰來加密其中的資料 AWS Transform，管理員需要使用 許可 AWS KMS。

若要使用以客戶受管金鑰加密的功能，使用者需要允許 AWS Transform 存取客戶受管金鑰的許可。

如果您在使用 時看到與 KMS 授予相關的錯誤 AWS Transform，您可能需要更新許可， AWS Transform 以允許 建立授予。若要自動設定所需的許可，請前往 AWS Transform 主控台，然後在頁面

頂端的橫幅中選擇更新許可。若要允許 AWS Transform 建立授予，您需要更新 AWS Transform 主控台頁面上的許可。

允許 AWS Transform 存取客戶受管金鑰

下列範例政策陳述式會授予使用者許可，以允許存取金鑰來 AWS Transform 存取以客戶受管金鑰加密的功能。 AWS Transform 如果管理員已設定客戶受管金鑰進行加密，則需要使用此政策。

> **Note**
>
> 此資訊不適用於使用 CMK 的 SQL Server 現代化部署工作流程。

```
"Statement": [
   {
     "Sid": "QKMSDecryptGenerateDataKeyPermissions",
     "Effect": "Allow",
     "Action": [
       "kms:Decrypt",
       "kms:GenerateDataKey",
       "kms:GenerateDataKeyWithoutPlaintext",
       "kms:ReEncryptFrom",
       "kms:ReEncryptTo"
     ],
     "Resource": [
       "arn:aws:kms:arn:aws::111122223333:key/[[key_id]]"
     ],
     "Condition": {
       "StringLike": {
         "kms:ViaService": [
           "q.us-east-1.amazonaws.com"
         ]
       }
     }
   }
 ]
```

AWS Transform 服務改進

為了協助 AWS Transform 提供最相關的資訊，我們可能會使用來自 的特定內容 AWS Transform，例如您提出的問題 AWS Transform 及其回應，以改善服務。此頁面說明我們會使用哪些內容，以及如何選擇退出。

AWS Transform 用於改善服務的內容

我們可能會使用 中的特定內容 AWS Transform 來改善服務。例如， AWS Transform 您可以使用此內容來提供更好的常見問題回應、修正 AWS Transform 操作問題、除錯或模型訓練。

例如， AWS 可能用於改善服務的內容包括您對 的問題， AWS Transform 以及 AWS Transform 產生的回應和程式碼。

如何選擇退出

您選擇不使用 AWS Transform 內容進行服務改進的方式取決於您使用的環境 AWS Transform。

在 中 AWS Transform 設定 AI 服務選擇退出政策 AWS Organizations。如需詳細資訊，請參閱《AWS Organizations 使用者指南》中的 AI 服務退出政策。

若要選擇退出在 IDE Visual Studio 中共用您的內容，請使用下列程序。

前往工具 -> 選項 -> AWS Toolkit -> Amazon Q

將與 AWS共用 Amazon Q 內容切換至 True 或 False。

若要選擇退出在 AWS Toolkit for 中分享您的遙測資料Visual Studio，請使用此程序：

1. 在工具下，選擇選項。
2. 在選項窗格中，選擇 AWS Toolkit，然後選擇一般。
3. 取消選取允許 AWS 工具組收集用量資訊。

AWS 轉換的身分和存取管理

AWS Identity and Access Management (IAM) 是一種 AWS 服務 ，可協助管理員安全地控制對 AWS 資源的存取。IAM 管理員可控制誰可以進行身分驗證 （登入） 和授權 （具有許可），以使用 AWS 轉換資源。IAM 是 AWS 服務 您可以免費使用的 。

主題

- 目標對象
- 使用身分驗證
- 使用政策管理存取權
- AWS 轉換如何與 IAM 搭配使用
- AWS 轉換的身分型政策範例
- 對 AWS 轉換身分和存取進行故障診斷
- 使用 的服務連結角色 AWS Transform
- AWS AWS Transform 的 受管政策
- AWS 轉換許可參考

目標對象

使用方式 AWS Identity and Access Management (IAM) 會根據您的角色而有所不同：

- 服務使用者 — 若無法存取某些功能，請向管理員申請所需許可 (請參閱 對 AWS 轉換身分和存取進行故障診斷)
- 服務管理員 — 負責設定使用者存取權並提交相關許可請求 (請參閱 AWS 轉換如何與 IAM 搭配使用)
- IAM 管理員 — 撰寫政策以管理存取控制 (請參閱 AWS 轉換的身分型政策範例)

使用身分驗證

身分驗證是您 AWS 使用身分憑證登入 的方式。您必須以 AWS 帳戶根使用者、IAM 使用者或擔任 IAM 角色身分進行身分驗證。

您可以使用身分來源的登入資料，例如 AWS IAM Identity Center (IAM Identity Center)、單一登入身分驗證或 Google/Facebook 登入資料，以聯合身分的形式登入。如需有關登入的詳細資訊，請參閱《AWS 登入 使用者指南》中的如何登入您的 AWS 帳戶。

對於程式設計存取， AWS 提供 SDK 和 CLI 以密碼編譯方式簽署請求。如需詳細資訊，請參閱《IAM 使用者指南》中的 API 請求的AWS 第 4 版簽署程序。

AWS 帳戶 根使用者

當您建立 時 AWS 帳戶，您會從一個名為 AWS 帳戶 theroot 使用者的登入身分開始，該身分具有對所有 AWS 服務 和 資源的完整存取權。強烈建議不要使用根使用者來執行日常任務。有關需要根使用者憑證的任務，請參閱《IAM 使用者指南》中的需要根使用者憑證的任務。

聯合身分

最佳實務是要求人類使用者使用聯合身分提供者，以 AWS 服務 使用臨時憑證存取 。

聯合身分是來自您企業目錄、Web 身分提供者的使用者，或使用來自身分來源的 AWS 服務 憑證存取 Directory Service 的使用者。聯合身分會擔任角色，而該角色會提供臨時憑證。

若需集中化管理存取權限，建議使用 AWS IAM Identity Center。如需詳細資訊，請參閱 AWS IAM Identity Center 使用者指南中的什麼是 IAM Identity Center？。

IAM 使用者和群組

IAM 使用者https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users.html是一種身分具備單人或應用程式的特定許可權。建議以臨時憑證取代具備長期憑證的 IAM 使用者。如需詳細資訊，請參閱《IAM 使用者指南》中的要求人類使用者使用聯合身分提供者來 AWS 使用臨時憑證存取 。

IAM 群組會指定 IAM 使用者集合，使管理大量使用者的許可權更加輕鬆。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM 使用者的使用案例。

IAM 角色

IAM 角色https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html的身分具有特定許可權，其可以提供臨時憑證。您可以透過從使用者切換到 IAM 角色 （主控台） 或呼叫 AWS CLI 或 AWS API 操作來擔任角色。如需詳細資訊，請參閱《IAM 使用者指南》中的擔任角色的方法。

IAM 角色適用於聯合身分使用者存取、臨時 IAM 使用者許可、跨帳戶存取權與跨服務存取，以及在 Amazon EC2 執行的應用程式。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM 中的快帳戶資源存取。

使用政策管理存取權

您可以透過建立政策並將其連接到身分或資源 AWS 來控制 AWS 中的存取。政策定義與身分或資源相關聯的許可。當委託人提出請求時 AWS ， 會評估這些政策。大多數政策會以 JSON 文件 AWS 形式存放在 中。如需進一步了解 JSON 政策文件，請參閱《IAM 使用者指南》中的 JSON 政策概觀。

管理員會使用政策，透過定義哪些主體可在哪些條件下對哪些資源執行動作，以指定可存取的範圍。

預設情況下，使用者和角色沒有許可。IAM 管理員會建立 IAM 政策並將其新增至角色，供使用者後續擔任。IAM 政策定義動作的許可，無論採用何種方式執行。

身分型政策

身分型政策是附加至身分 (使用者、使用者群組或角色) 的 JSON 許可政策文件。這類政策控制身分可對哪些資源執行哪些動作，以及適用的條件。如需了解如何建立身分型政策，請參閱《IAM 使用者指南》中的透過客戶管理政策定義自訂 IAM 許可。

身分型政策可分為內嵌政策 (直接內嵌於單一身分) 與受管政策 (可附加至多個身分的獨立政策)。如需了解如何在受管政策及內嵌政策之間做選擇，請參閱《IAM 使用者指南》中的在受管政策與內嵌政策之間選擇。

資源型政策

資源型政策是附加到資源的 JSON 政策文件。範例包括 IAM 角色信任政策與 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。您必須在資源型政策中指定主體。

資源型政策是位於該服務中的內嵌政策。您無法在資源型政策中使用來自 IAM 的 AWS 受管政策。

其他政策類型

AWS 支援其他政策類型，可設定更多常見政策類型授予的最大許可：

- 許可界限 — 設定身分型政策可授與 IAM 實體的最大許可。如需詳細資訊，請參閱《 IAM 使用者指南》中的 IAM 實體許可界限。
- 服務控制政策 (SCP) — 為 AWS Organizations中的組織或組織單位指定最大許可。如需詳細資訊，請參閱《AWS Organizations 使用者指南》中的服務控制政策。
- 資源控制政策 (RCP) — 設定您帳戶中資源可用許可的上限。如需詳細資訊，請參閱《AWS Organizations 使用者指南》中的資源控制政策 (RCP)。
- 工作階段政策 — 在以程式設計方式為角色或聯合身分使用者建立臨時工作階段時，以參數形式傳遞的進階政策。如需詳細資訊，請參《IAM 使用者指南》中的工作階段政策。

多種政策類型

當多種類型的政策適用於請求時，產生的許可會更複雜而無法理解。若要了解如何 AWS 決定是否在涉及多個政策類型時允許請求，請參閱《IAM 使用者指南》中的政策評估邏輯。

AWS 轉換如何與 IAM 搭配使用

在您使用 IAM 管理 AWS 轉換的存取權之前，請先了解哪些 IAM 功能可與 AWS 轉換搭配使用。

IAM 功能	AWS 轉換支援
身分型政策	是
資源型政策	否
政策動作	是
政策資源	是
政策條件索引鍵	是
ACL	否
ABAC(政策中的標籤)	部分
臨時憑證	是
主體許可	是
服務角色	是
服務連結角色	是

若要全面了解 AWS Transform 和其他 AWS 服務如何與大多數 IAM 功能搭配使用，請參閱《IAM 使用者指南》中的AWS 與 IAM 搭配使用的 服務。

AWS 轉換的身分型政策

支援身分型政策：是

身分型政策是可以附加到身分 (例如 IAM 使用者、使用者群組或角色) 的 JSON 許可政策文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。如需了解如何建立身分型政策，請參閱《IAM 使用者指南》中的透過客戶管理政策定義自訂 IAM 許可。

使用 IAM 身分型政策，您可以指定允許或拒絕的動作和資源，以及在何種條件下允許或拒絕動作。如要了解您在 JSON 政策中使用的所有元素，請參閱《IAM 使用者指南》中的 IAM JSON 政策元素參考。

AWS 轉換的身分型政策範例

若要檢視 AWS 轉換身分型政策的範例，請參閱 AWS 轉換的身分型政策範例。

AWS 轉換中的資源型政策

支援資源型政策：否

資源型政策是附加到資源的 JSON 政策文件。資源型政策的最常見範例是 IAM 角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中指定主體。委託人可以包括帳戶、使用者、角色、聯合身分使用者或 AWS 服務。

如需啟用跨帳戶存取權，您可以在其他帳戶內指定所有帳戶或 IAM 實體作為資源型政策的主體。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM 中的快帳戶資源存取。

AWS 轉換的政策動作

支援政策動作：是

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

JSON 政策的 `Action` 元素描述您可以用來允許或拒絕政策中存取的動作。政策會使用動作來授予執行相關聯動作的許可。

若要查看 AWS 轉換動作的清單，請參閱《服務授權參考》中的AWS 轉換的動作、資源和條件索引鍵。

若要查看 AWS 轉換自訂的動作清單，請參閱《服務授權參考》中的AWS 轉換自訂的動作、資源和條件索引鍵。

AWS 轉換中的政策動作在動作之前使用下列字首：

```
transform
```

若要在單一陳述式中指定多個動作，請用逗號分隔。

```
"Action": [
      "transform:action1",
      "transform:action2"
         ]
```

若要檢視 AWS 轉換身分型政策的範例，請參閱 AWS 轉換的身分型政策範例。

AWS 轉換的政策資源

支援政策資源：是

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Resource JSON 政策元素可指定要套用動作的物件。最佳實務是使用其 Amazon Resource Name (ARN) 來指定資源。若動作不支援資源層級許可，使用萬用字元 (*) 表示該陳述式適用於所有資源。

```
"Resource": "*"
```

若要查看 AWS 轉換資源類型及其 ARNs 的清單，以及您可以使用哪些動作指定每個資源的 ARN，請參閱服務授權參考中的AWS 轉換的動作、資源和條件索引鍵。

若要查看資源類型及其 ARNs 的清單，以及您可以使用哪些動作指定 AWS 轉換自訂每個資源的 ARN，請參閱服務授權參考中的AWS 轉換自訂的動作、資源和條件索引鍵。

若要檢視 AWS 轉換身分型政策的範例，請參閱 AWS 轉換的身分型政策範例。

AWS 轉換的政策條件索引鍵

支援服務特定政策條件金鑰：是

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Condition 元素會根據定義的條件，指定陳述式的執行時機。您可以建立使用條件運算子的條件運算式 (例如等於或小於)，來比對政策中的條件和請求中的值。若要查看所有 AWS 全域條件索引鍵，請參閱《IAM 使用者指南》中的AWS 全域條件內容索引鍵。

若要查看 AWS 轉換條件索引鍵的清單，以及您可以使用條件索引鍵的動作和資源，請參閱《服務授權參考》中的AWS 轉換的動作、資源和條件索引鍵。

若要查看條件索引鍵清單，以及您可以使用 AWS 轉換自訂條件索引鍵來執行哪些動作和資源，請參閱《服務授權參考》中的AWS 轉換自訂的動作、資源和條件索引鍵。

若要檢視 AWS 轉換身分型政策的範例，請參閱 AWS 轉換的身分型政策範例。

AWS 轉換中的 ACLs

支援 ACL：否

存取控制清單 (ACL) 可控制哪些主體 (帳戶成員、使用者或角色) 擁有存取某資源的許可。ACL 類似於資源型政策，但它們不使用 JSON 政策文件格式。

ABAC 與 AWS 轉換

支援 ABAC (政策中的標籤)：部分

屬性型存取控制 (ABAC) 是一種授權策略，根據稱為標籤的屬性定義許可權。您可以將標籤連接至 IAM 實體 AWS 和資源，然後設計 ABAC 政策，以便在委託人的標籤符合資源上的標籤時允許操作。

如需根據標籤控制存取，請使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 條件索引鍵，在政策的條件元素中，提供標籤資訊。

如果服務支援每個資源類型的全部三個條件金鑰，則對該服務而言，值為 Yes。如果服務僅支援某些資源類型的全部三個條件金鑰，則值為 Partial。

如需 ABAC 的詳細資訊，請參閱《IAM 使用者指南》中的使用 ABAC 授權定義許可。如要查看含有設定 ABAC 步驟的教學課程，請參閱《IAM 使用者指南》中的使用屬性型存取控制 (ABAC)。

搭配 AWS Transform 使用暫時登入資料

支援臨時憑證：是

臨時登入資料提供 AWS 資源的短期存取權，當您使用聯合或切換角色時，會自動建立。 AWS 建議您動態產生臨時登入資料，而不是使用長期存取金鑰。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM 中的臨時安全憑證與可與 IAM 搭配運作的AWS 服務。

AWS 轉換的跨服務主體許可

支援轉寄存取工作階段 (FAS)：是

轉送存取工作階段 (FAS) 使用呼叫 的委託人許可 AWS 服務，並結合 AWS 服務 請求向下游服務提出請求。如需提出 FAS 請求時的政策詳細資訊，請參閱轉發存取工作階段。

AWS 轉換的服務角色

支援服務角色：是

服務角色是服務擔任的 IAM 角色，可代您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需詳細資訊，請參閱《IAM 使用者指南》中的建立角色以委派許可給 AWS 服務。

> **Warning**
>
> 變更服務角色的許可可能會中斷 AWS 轉換功能。只有在 AWS Transform 提供指引時，才能編輯服務角色。

AWS 轉換的服務連結角色

支援服務連結角色：是

服務連結角色是連結至 的一種服務角色 AWS 服務。服務可以擔任代表您執行動作的角色。服務連結角色會出現在您的 中 AWS 帳戶 ，並由服務擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

如需建立或管理 AWS 轉換服務連結角色的詳細資訊，請參閱 使用 的服務連結角色 AWS Transform。

AWS 轉換的身分型政策範例

根據預設，使用者和角色沒有建立或修改 AWS 轉換資源的許可。若要授予使用者對其所需資源執行動作的許可，IAM 管理員可以建立 IAM 政策。

如需了解如何使用這些範例 JSON 政策文件建立 IAM 身分型政策，請參閱《IAM 使用者指南》中的建立 IAM 政策 (主控台)。

如需 AWS Transform 所定義之動作和資源類型的詳細資訊，包括每種資源類型的 ARNs 格式，請參閱《服務授權參考》中的適用於 AWS Transform 的動作、資源和條件金鑰。

主題

- 政策最佳實務
- 使用 AWS 轉換主控台
- 允許使用者檢視他們自己的許可
- 允許管理員接受來自 AWS 轉換帳戶的連接器請求
- 允許管理員指派現有的 IAM Identity Center 使用者，並建立新的 IAM Identity Center 使用者以指派給 AWS 轉換
- 允許管理員啟用 AWS 轉換

- 允許使用者使用 IAM 登入資料存取 AWS Transform

政策最佳實務

身分型政策會判斷您帳戶中的某人是否可以建立、存取或刪除 AWS 轉換資源。這些動作可能會讓您的 AWS 帳戶產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

- 開始使用 AWS 受管政策並邁向最低權限許可 – 若要開始將許可授予您的使用者和工作負載，請使用將許可授予許多常見使用案例的 AWS 受管政策。它們可在您的 中使用 AWS 帳戶。我們建議您定義特定於使用案例 AWS 的客戶受管政策，進一步減少許可。如需更多資訊，請參閱《IAM 使用者指南》中的 AWS 受管政策或任務職能的AWS 受管政策。
- 套用最低權限許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的許可。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需使用 IAM 套用許可的更多相關資訊，請參閱《IAM 使用者指南》中的 IAM 中的政策和許可。
- 使用 IAM 政策中的條件進一步限制存取權 – 您可以將條件新增至政策，以限制動作和資源的存取。例如，您可以撰寫政策條件，指定必須使用 SSL 傳送所有請求。如果透過特定 例如 使用服務動作 AWS 服務，您也可以使用條件來授予其存取權 CloudFormation。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM JSON 政策元素：條件。
- 使用 IAM Access Analyzer 驗證 IAM 政策，確保許可安全且可正常運作 – IAM Access Analyzer 驗證新政策和現有政策，確保這些政策遵從 IAM 政策語言 (JSON) 和 IAM 最佳實務。IAM Access Analyzer 提供 100 多項政策檢查及切實可行的建議，可協助您撰寫安全且實用的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的使用 IAM Access Analyzer 驗證政策。
- 需要多重要素驗證 (MFA) – 如果您的案例需要 IAM 使用者或 中的根使用者 AWS 帳戶，請開啟 MFA 以提高安全性。如需在呼叫 API 操作時請求 MFA，請將 MFA 條件新增至您的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的透過 MFA 的安全 API 存取。

如需 IAM 中最佳實務的相關資訊，請參閱《IAM 使用者指南》中的 IAM 安全最佳實務。

使用 AWS 轉換主控台

若要存取 AWS 轉換主控台，您必須擁有一組最低許可。這些許可必須允許您列出和檢視 中 AWS 轉換資源的詳細資訊 AWS 帳戶。如果您建立比最基本必要許可更嚴格的身分型政策，則對於具有該政策的實體 (使用者或角色) 而言，主控台就無法如預期運作。

對於僅呼叫 AWS CLI 或 AWS API 的使用者，您不需要允許最低主控台許可。反之，只需允許存取符合他們嘗試執行之 API 操作的動作就可以了。

允許使用者檢視他們自己的許可

此範例會示範如何建立政策，允許 IAM 使用者檢視附加到他們使用者身分的內嵌及受管政策。此政策包含在主控台或使用 或 AWS CLI AWS API 以程式設計方式完成此動作的許可。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

允許管理員接受來自 AWS 轉換帳戶的連接器請求

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "transform:GetConnector",
                "transform:AssociateConnectorResource",
                "transform:RejectConnector"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetBucketPublicAccessBlock",
                "s3:GetAccountPublicAccessBlock"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:CreateRole",
                "iam:AttachRolePolicy",
                "iam:PassRole"
            ],
            "Resource": "arn:aws:iam::111122223333:role/service-role/
AWSTransform-*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:CreatePolicy"
            ],
            "Resource": "arn:aws:iam::111122223333:policy/service-role/
AWSTransform-*"
        }
    ]
```

```
}
```

允許管理員指派現有的 IAM Identity Center 使用者，並建立新的 IAM Identity Center 使用者以指派給 AWS 轉換

下列政策授予管理員在 AWS 轉換主控台中管理 IAM Identity Center 使用者和群組所需的許可。透過此政策，管理員可以指派和移除使用者和群組、檢視顯示名稱、建立新的 IAM Identity Center 使用者、管理應用程式指派，以及設定應用程式工作階段設定。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "SSOApplicationAssignments",
      "Effect": "Allow",
      "Action": [
        "sso:ListApplicationAssignments",
        "sso:CreateApplicationAssignment",
        "sso:DeleteApplicationAssignment",
        "sso:ListInstances",
        "sso:DescribeInstance",
        "sso:ListDirectoryAssociations",
        "sso:GetApplicationGrant",
        "sso:GetApplicationAccessScope",
        "sso:GetApplicationSessionConfiguration",
        "sso:PutApplicationSessionConfiguration"
      ],
      "Resource": "*"
    },
    {
      "Sid": "SSODirectoryCreateUser",
      "Effect": "Allow",
      "Action": [
        "sso-directory:CreateUser"
      ],
      "Resource": "*"
    },
    {
      "Sid": "IdentityStoreAccess",
      "Effect": "Allow",
      "Action": [
        "identitystore:DescribeUser",
```

```
        "identitystore:DescribeGroup",
        "identitystore:ListUsers",
        "identitystore:ListGroups"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowKmsAccessViaIdentityCenter",
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": "*",
      "Condition": {
        "ArnLike": {
          "kms:EncryptionContext:aws:sso:instance-arn": "arn:*:sso:::instance/*"
        },
        "StringLike": {
          "kms:ViaService": "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid": "AllowKmsAccessViaIdentityStore",
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": "*",
      "Condition": {
        "ArnLike": {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn":
 "arn:*:identitystore::*:identitystore/*"
        },
        "StringLike": {
          "kms:ViaService": "identitystore.*.amazonaws.com"
        }
      }
    }
  ]
}
```

允許管理員啟用 AWS 轉換

下列政策授予管理員透過 AWS 主控台啟用和管理 AWS Transform 所需的許可。這包括管理設定檔、設定客服人員和管理連接器。此政策僅適用於管理員，且應範圍限定為您帳戶中的受信任委託人。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "SSOEnableTransform",
      "Effect": "Allow",
      "Action": [
        "sso:ListInstances",
        "sso:CreateInstance",
        "sso:CreateApplication",
        "sso:PutApplicationAuthenticationMethod",
        "sso:PutApplicationGrant",
        "sso:PutApplicationAssignmentConfiguration",
        "sso:ListApplications",
        "sso:GetSharedSsoConfiguration",
        "sso:DescribeInstance",
        "sso:PutApplicationAccessScope",
        "sso:DescribeApplication",
        "sso:DeleteApplication",
        "sso:UpdateApplication",
        "sso:DescribeRegisteredRegions",
        "sso:GetSSOStatus"
      ],
      "Resource": "*"
    },
    {
      "Sid": "SSODirectoryActions",
      "Effect": "Allow",
      "Action": [
        "sso-directory:GetUserPoolInfo",
        "sso-directory:DescribeUsers",
        "sso-directory:DescribeGroups",
        "sso-directory:SearchGroups",
        "sso-directory:SearchUsers",
        "sso-directory:DescribeDirectory"
      ],
      "Resource": "*"
    },
```

```
    {
      "Sid": "KMSListAliases",
      "Effect": "Allow",
      "Action": [
        "kms:ListAliases"
      ],
      "Resource": "*"
    },
    {
      "Sid": "KMSActions",
      "Effect": "Allow",
      "Action": [
        "kms:CreateGrant",
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:GenerateDataKey*",
        "kms:RetireGrant",
        "kms:DescribeKey"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:ViaService": "transform.*.amazonaws.com"
        }
      }
    },
    {
      "Sid": "IAMServiceLinkedRole",
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource": [
        "arn:*:iam::*:role/aws-service-role/transform.amazonaws.com/
AWSServiceRoleForAWSTransform"
      ]
    },
    {
      "Sid": "TransformConsoleActions",
      "Effect": "Allow",
      "Action": [
        "transform:GetAccountSettings",
        "transform:UpdateAccountSettings",
        "transform:CreateProfile",
```

```
        "transform:UpdateProfile",
        "transform:DeleteProfile",
        "transform:ListProfiles",
        "transform:GetConnector",
        "transform:ListConnectors",
        "transform:DeleteConnector",
        "transform:AssociateConnectorResource",
        "transform:RejectConnector",
        "transform:ListAgents",
        "transform:GetAgent",
        "transform:GetAgentRuntimeConfiguration",
        "transform:PutAgentRuntimeConfiguration",
        "transform:UpdateAgentAccess",
        "transform:TagResource",
        "transform:UntagResource",
        "transform:ListTagsForResource",
        "transform:GetWebAppUrl"
      ],
      "Resource": "*"
    }
  ]
}
```

允許使用者使用 IAM 登入資料存取 AWS Transform

下列政策會使用 IAM 憑證授予 IAM 主體對 AWS Transform Web 應用程式和 APIs存取權。IAM 限定存取和與身分提供者一起啟用的 IAM 存取需要此政策。

將 *region*、 *account-id*和 取代*profile-id*為您的值。您可以在 AWS 轉換主控台的設定下找到設定檔 ID。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowTransformAccess",
      "Effect": "Allow",
      "Action": "transform:AccessTransformProfile",
      "Resource": "arn:aws:transform:region:account-id:profile/profile-id"
    }
  ]
}
```

若要授予 帳戶中所有設定檔的存取權，請針對設定檔 ID 使用萬用字元：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowTransformAccessAllProfiles",
      "Effect": "Allow",
      "Action": "transform:AccessTransformProfile",
      "Resource": "arn:aws:transform:region:account-id:profile/*"
    }
  ]
}
```

> **Note**
>
> `transform:AccessTransformProfile` 動作只會授予 AWS 對 Transform 的存取權。工作區內的動作是由 AWS 轉換工作區角色（管理員、貢獻者、核准者、唯讀）控制，而非由 IAM 政策控制。工作區角色決定使用者可以做什麼，例如建立任務、管理協作者或核准任務。

對 AWS 轉換身分和存取進行故障診斷

使用以下資訊來協助您診斷和修正使用 AWS Transform 和 IAM 時可能遇到的常見問題。

主題

- 我無權在 AWS Transform 中執行動作
- 我未獲得執行 iam:PassRole 的授權
- 我想要允許 以外的人員 AWS 帳戶 存取我的 AWS 轉換資源

我無權在 AWS Transform 中執行動作

如果您收到錯誤，告知您未獲授權執行動作，您的政策必須更新，允許您執行動作。

下列範例錯誤會在`mateojackson` IAM 使用者嘗試使用主控台檢視一個虛構 *my-example-widget* 資源的詳細資訊，但卻無虛構 `AWS Transform:GetWidget` 許可時發生。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform: AWS
 Transform:GetWidget on resource: my-example-widget
```

在此情況下，必須更新 mateojackson 使用者的政策，允許使用 AWS Transform:*GetWidget* 動作存取 *my-example-widget* 資源。

如果您需要協助，請聯絡您的 AWS 管理員。您的管理員提供您的簽署憑證。

我未獲得執行 iam:PassRole 的授權

如果您收到錯誤，告知您無權執行 iam:PassRole動作，您的政策必須更新，以允許您將角色傳遞至 AWS 轉換。

有些 AWS 服務 可讓您將現有角色傳遞給該服務，而不是建立新的服務角色或服務連結角色。如需執行此作業，您必須擁有將角色傳遞至該服務的許可。

當名為 的 IAM marymajor 使用者嘗試使用主控台在 AWS Transform 中執行動作時，會發生下列範例錯誤。但是，動作請求服務具備服務角色授予的許可。Mary 沒有將角色傳遞給服務的許可。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

在這種情況下，Mary 的政策必須更新，允許她執行 iam:PassRole 動作。

如果您需要協助，請聯絡您的 AWS 管理員。您的管理員提供您的簽署憑證。

我想要允許 以外的人員 AWS 帳戶 存取我的 AWS 轉換資源

您可以建立一個角色，讓其他帳戶中的使用者或您組織外部的人員存取您的資源。您可以指定要允許哪些信任物件取得該角色。針對支援基於資源的政策或存取控制清單 (ACL) 的服務，您可以使用那些政策來授予人員存取您的資源的許可。

如需進一步了解，請參閱以下內容：

- 若要了解 AWS Transform 是否支援這些功能，請參閱 AWS 轉換如何與 IAM 搭配使用。
- 若要了解如何在您擁有 AWS 帳戶 的 資源之間提供存取權，請參閱《IAM 使用者指南》中的在您擁有 AWS 帳戶 的另一個 中提供存取權給 IAM 使用者。
- 若要了解如何將資源的存取權提供給第三方 AWS 帳戶，請參閱《IAM 使用者指南》中的將存取權提供給第三方 AWS 帳戶 擁有。

- 如需了解如何透過聯合身分提供存取權，請參閱《IAM 使用者指南》中的將存取權提供給在外部進行身分驗證的使用者 (聯合身分)。
- 如需了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱《IAM 使用者指南》中的 IAM 中的跨帳戶資源存取。

使用 的服務連結角色 AWS Transform

AWS Transform use AWS Identity and Access Management (IAM) 服務連結角色。服務連結角色是直接連結至 的唯一 IAM 角色類型 AWS Transform。服務連結角色由 預先定義， AWS Transform 並包含該服務代表您呼叫其他 AWS 服務所需的所有許可。

使用 的服務連結角色 AWS Transform

AWS Transform use AWS Identity and Access Management (IAM) 服務連結角色。服務連結角色是直接連結至 的唯一 IAM 角色類型 AWS Transform。服務連結角色由 預先定義， AWS Transform 並包含該服務代表您呼叫其他 AWS 服務所需的所有許可。

服務連結角色可讓您更 AWS Transform 輕鬆地設定，因為您不必手動新增必要的許可。 AWS Transform 會定義其服務連結角色的許可，除非另有定義，否則只能 AWS Transform 擔任其角色。定義的許可包括信任政策和許可政策，且該許可政策無法附加至其他 IAM 實體。

您必須先刪除服務連結角色的相關資源，才能將其刪除。這可保護您的 AWS Transform 資源，因為您不會不小心移除存取資源的許可。

如需有關支援服務連結角色的其他 服務的資訊，請參閱 AWS IAM 適用的服務，並在服務連結角色欄中尋找具有是的服務。選擇具有連結的是，以檢視該服務的服務連結角色文件。

的服務連結角色許可 AWS Transform

AWS Transform 使用名為 AWSServiceRoleForAWSTransform 的服務連結角色 – 此服務連結角色提供 AWS 轉換功能，可提供用量資訊。

AWSServiceRoleForAWSTransform 服務連結角色信任下列服務擔任該角色：

- `transform.amazonaws.com`

名為 AWSServiceRoleForAWSTransform 的角色許可政策允許 對指定的資源 AWS Transform 完成下列動作：

- cloudwatch:PutMetricData

  - 將自訂指標傳送至 CloudWatch 以進行 AWS Transform 操作
  - 追蹤轉型進度、成功率和效能指標
  - 啟用轉換工作流程的監控和提醒
- sso：DescribeApplication
  - 在 Identity Center 中檢視特定應用程式的詳細資訊
  - 取得應用程式中繼資料，例如名稱、描述、狀態和組態
- sso：GetApplicationAssignmentConfiguration
  - 擷取應用程式的指派組態設定
  - 了解使用者/群組如何設定為指派給應用程式
- sso：ListApplicationAssignmentsForPrincipal
  - 列出指派給特定使用者或群組的所有應用程式（委託人）
  - 檢視特定身分可存取的應用程式
- 透過 IAM Identity Center 存取時，啟用 KMS 加密資料的解密。只有在加密內容包含有效的 IAM Identity Center 執行個體 ARN 且必須透過 IAM Identity Center 服務端點存取時，才能運作。
- 允許透過 Identity Store 存取時解密 KMS 加密的資料。只有在加密內容包含有效的 Identity Store ARN 且必須透過 Identity Store 服務端點存取時，才能運作。
- secretsmanager:GetSecretValue
  - 存取用於存放外部身分提供者用戶端秘密 AWS Transform 的服務連結秘密
  - 資源：arn：aws：secretsmanager：*：*：secret：transform-preprod！*
  - 條件：必須由 transform-preprod 服務擁有，並從相同的帳戶存取
- support：CreateCase， support：DescribeCases， support：DescribeCommunications， support：AddCommunicationToCase， support：ResolveCase
  - 從 AWS Transform Web 應用程式建立和管理進階支援案例
  - 檢視案例詳細資訊和通訊
  - 新增通訊並解決支援案例

您必須設定許可，以允許您的使用者、群組或角色建立、編輯或刪除服務連結角色。如需詳細資訊，請參閱 IAM 使用者指南中的服務連結角色許可。

為 建立服務連結角色 AWS Transform

您不需要手動建立服務連結角色，當您在 AWS Transform 中建立 的設定檔時 AWS 管理主控台， 會為您 AWS Transform 建立服務連結角色。

若您刪除此服務連結角色，之後需要再次建立，您可以在帳戶中使用相同程序重新建立角色。當您更新設定時， AWS Transform 會再次為您建立服務連結角色。

您也可以使用 IAM 主控台或 AWS CLI 來建立具有服務名稱`transform.amazonaws.com`的服務連結角色。如需詳細資訊，請參閱《IAM 使用者指南》中的「建立服務連結角色」。如果您刪除此服務連結角色，您可以使用此相同的程序以再次建立該角色。

編輯 的服務連結角色 AWS Transform

AWS Transform 不允許您編輯 AWSServiceRoleForAWSTransform 服務連結角色。因為有各種實體可能會參考服務連結角色，所以您無法在建立角色之後變更角色名稱。然而，您可使用 IAM 來編輯角色描述。如需詳細資訊，請參閱《IAM 使用者指南》中的編輯服務連結角色。

刪除 的服務連結角色 AWS Transform

若您不再使用需要服務連結角色的功能或服務，我們建議您刪除該角色。如此一來，您就沒有未主動監控或維護的未使用實體。然而，在手動刪除服務連結角色之前，您必須先清除資源。

> **Note**
>
> 如果 AWS Transform 服務在您嘗試刪除資源時使用 角色，則刪除可能會失敗。若此情況發生，請等待數分鐘後並再次嘗試操作。

使用 IAM 手動刪除服務連結角色

使用 IAM 主控台 AWS CLI、 或 AWS API 來刪除 AWSServiceRoleForAWSTransform 服務連結角色。如需詳細資訊，請參閱《IAM 使用者指南》中的刪除服務連結角色。

AWS Transform 服務連結角色支援的區域

AWS Transform 不支援在提供服務的每個區域中使用服務連結角色。您可以在下列區域中使用 AWSServiceRoleForAWSTransform 角色。如需詳細資訊，請參閱 AWS 區域與端點。

區域名稱	區域身分	中的支援 AWS Transform
美國東部 (維吉尼亞北部)	us-east-1	是
歐洲 (法蘭克福)	eu-central-1	是

使用適用於 AWS Transform Custom 的服務連結角色

AWS Transform Custom 會使用名為 AWSServiceRoleForAWSTransformCustom 的服務連結角色，代表您將指標和日誌發佈至您的帳戶。這些指標可讓您直接在儀表板中監控轉換計數、延遲和狀態碼。日誌可讓您了解轉換期間遇到的問題。

此服務連結角色是由 AWS Transform Custom 預先定義，且僅包含服務所需的許可。您不需要手動新增任何許可，而且角色只能由 AWS Transform Custom 擔任。如需服務連結角色的一般資訊，請參閱《IAM 使用者指南》中的使用服務連結角色。

AWS Transform Custom 的服務連結角色許可

AWSServiceRoleForAWSTransformCustom 服務連結角色信任下列服務擔任該角色：

- `transform-custom.amazonaws.com`

名為 AWSServiceRoleForAWSTransformCustom 的角色許可政策允許 AWS Transform Custom 對指定的資源完成下列動作：

- `cloudwatch:PutMetricData` 在所有 AWS 資源上
  - 在`AWS/TransformCustom`命名空間下發佈操作指標至
  - 追蹤轉換計數、延遲和狀態碼
  - 透過`cloudwatch:namespace`條件索引鍵範圍限定於`AWS/TransformCustom`命名空間
- `logs:CreateLogGroup` `/aws/TransformCustom`日誌群組`logs:PutRetentionPolicy`上的和
  - 建立 CloudWatch Logs 日誌群組以發佈轉換日誌
  - 在日誌群組上設定日誌保留政策
  - 範圍為 `arn:aws:logs:*:*:log-group:/aws/TransformCustom`，其`aws:ResourceAccount`條件可確保僅在您的帳戶內存取
- `logs:CreateLogStream` `logs:PutLogEvents`日誌群組內的 和 `/aws/TransformCustom`日誌串流
  - 建立日誌串流並發佈轉換操作的日誌事件
  - 範圍為 `arn:aws:logs:*:*:log-group:/aws/TransformCustom:log-stream:*`，其`aws:ResourceAccount`條件可確保僅在您的帳戶內存取

您必須設定許可，以允許您的使用者、群組或角色建立、編輯或刪除服務連結角色。如需詳細資訊，請參閱 IAM 使用者指南中的服務連結角色許可。

為 AWS Transform Custom 建立服務連結角色

您不需要手動建立服務連結角色，當您使用 Transform Custom CLI 執行 AWS 轉換時， AWS Transform Custom 會為您建立服務連結角色。

若您刪除此服務連結角色，之後需要再次建立，您可以在帳戶中使用相同程序重新建立角色。當您使用 Transform Custom CLI 執行 AWS 轉換時， AWS Transform Custom 會再次為您建立服務連結角色。

您也可以使用 IAM 主控台建立具有 AWSServiceRoleForAWSTransformCustom 使用案例的服務連結角色。在 AWS CLI 或 AWS API 中，使用服務名稱建立`transform-custom.amazonaws.com`服務連結角色。如需詳細資訊，請參閱《IAM 使用者指南》中的「建立服務連結角色」。如果您刪除此服務連結角色，您可以使用此相同的程序以再次建立該角色。

編輯 AWS Transform Custom 的服務連結角色

AWS Transform Custom 不允許您編輯 AWSServiceRoleForAWSTransformCustom 服務連結角色。因為有各種實體可能會參考服務連結角色，所以您無法在建立角色之後變更角色名稱。然而，您可使用 IAM 來編輯角色描述。如需詳細資訊，請參閱《IAM 使用者指南》中的編輯服務連結角色。

刪除 AWS Transform Custom 的服務連結角色

若您不再使用需要服務連結角色的功能或服務，我們建議您刪除該角色。如此一來，您就沒有未主動監控或維護的未使用實體。

AWSServiceRoleForAWSTransformCustom 服務連結角色不會在您的帳戶中建立持久性資源。您可以直接刪除它，無需任何資源清理。

如果您刪除此角色，稍後使用轉換自訂 CLI 執行 AWS 轉換，則會自動重新建立服務連結角色。

使用 IAM 手動刪除服務連結角色

使用 IAM 主控台 AWS CLI、 或 AWS API 來刪除 AWSServiceRoleForAWSTransformCustom 服務連結角色。如需詳細資訊，請參閱《IAM 使用者指南》中的刪除服務連結角色。

AWS Transform Custom 服務連結角色支援的 區域

AWS 在可使用 Transform Custom 的所有區域中， AWS Transform Custom 支援使用服務連結角色。如需支援的區域清單，請參閱支援的區域。

AWS AWS Transform 的 受管政策

AWS 受管政策是由 AWS AWS 受管政策建立和管理的獨立政策旨在為許多常用案例提供許可，以便您可以開始將許可指派給使用者、群組和角色。

請記住， AWS 受管政策可能不會授予特定使用案例的最低權限許可，因為這些許可可供所有 AWS 客戶使用。我們建議您定義特定於使用案例的客戶管理政策，以便進一步減少許可。

您無法變更 AWS 受管政策中定義的許可。如果 AWS 更新受 AWS 管政策中定義的許可，則更新會影響政策連接的所有主體身分（使用者、群組和角色）。當新的 AWS 服務 啟動或新的 API 操作可用於現有服務時， AWS 最有可能更新 AWS 受管政策。

如需詳細資訊，請參閱 IAM 使用者指南中的 AWS 受管政策。

AWS 轉換 AWS 受管政策的更新

檢視自 2021 年 3 月 1 日起對 AWS Transform 受 AWS 管政策進行更新的詳細資訊。

變更	描述	日期
AWSTransformInfrastructureExecutorAccessBatch – 更新的政策	縮小明確函數允許清單的 AWS Lambda 許可範圍、新增批次附屬輸出的 Amazon S3 寫入存取、擴大 CloudFormation 和 Amazon EventBridge 排程器資源範圍，以進行多堆疊部署，以及新增區域 AWS Key Management Service 金鑰別名變體的支援。	2026 年 7 月 27 日
AWSTransformInfrastructureExecutorAccessEC2 – 更新的政策	為多堆疊部署擴充 CloudFormation、Amazon EventBridge 排程器和 AWS Identity and Access Management PassRole 資源範圍、新增 Security Agent 基礎設施可見性，以及新增區域 AWS Key	2026 年 7 月 27 日

變更	描述	日期
	Management Service 金鑰別名變體的支援。	
AWSTransformSecurityAgentExecutorAccess – 更新的政策	新增 CloudFormation 許可，以探索和描述 Security Agent 基礎設施堆疊，並將 Amazon S3 儲存貯體字首從 遷移`kct-security-agent-*` 至 `atx-security-agent-*`。	2026 年 7 月 27 日
AWSTransformInfrastructureExecutorAccessBatch – 新政策	新增了新的 AWS 受管政策，授予使用 AWS Batch 執行 AWS Transform Continuous Modernization 評估和轉換所需的許可，包括上傳原始程式碼、擷取結果、監控 Batch 任務狀態、讀取日誌和管理轉換排程。	2026 年 7 月 20 日
AWSTransformInfrastructureExecutorAccessEC2 – 新政策	新增了新的 AWS 受管政策，授予使用 Amazon EC2 執行 AWS 轉換持續現代化評估和轉換所需的許可，包括上傳原始程式碼、擷取結果、監控任務狀態和管理轉換排程。	2026 年 7 月 20 日
AWSTransformSecurityAgentExecutorAccess – 新政策	新增了新的 AWS 受管政策，授予 AWS Transform Continuous Modernization 呼叫 AWS Security Agent 服務以進行自動程式碼安全審查和修復所需的許可，包括上傳掃描成品和擷取問題清單。	2026 年 6 月 30 日

變更	描述	日期
AWSServiceRoleForAWSTransformCustom – 已更新政策	新增 CloudWatch Logs 許可，以允許 AWS 轉換自訂將日誌發佈至您帳戶中的/aws/TransformCustom 日誌群組。	2026 年 5 月 5 日
AWSTransformCustomExecuteTransformations – 更新的政策	新增建立 AWS 轉換自訂服務連結角色 (AWSServiceRoleForAWSTransformCustom) 的許可，以啟用 CloudWatch 指標發射到客戶帳戶。	2026 年 4 月 27 日
AWSTransformCustomManageTransformations – 更新的政策	新增建立 AWS 轉換自訂服務連結角色 (AWSServiceRoleForAWSTransformCustom) 的許可，以啟用 CloudWatch 指標發射到客戶帳戶。	2026 年 4 月 27 日
AWSTransformCustomFullAccess – 更新的政策	新增建立 AWS 轉換自訂服務連結角色 (AWSServiceRoleForAWSTransformCustom) 的許可，以啟用 CloudWatch 指標發射到客戶帳戶。	2026 年 4 月 7 日
AWSServiceRoleForAWSTransformCustom – 新政策	新增 AWS 轉換自訂服務連結角色的新 AWS 受管政策。此政策允許 AWS 轉換自訂 將 CloudWatch 指標發佈至您的帳戶。	2026 年 3 月 23 日
DBModProvisioningAndMigration – 新政策	此政策會授予資料庫佈建和遷移功能。	2026 年 3 月 24 日

變更	描述	日期
DBModDiscoveryAndAssessment – 新政策	新增了新的 AWS 受管政策，可提供全面的資料庫現代化探索和評估功能。	2026 年 3 月 24 日
AWSTransformCustomFullAccess – 新政策	新增了新的 AWS 受管政策，提供 AWS 轉換自訂的完整存取權。	2025 年 12 月 5 日
AWSTransformCustomExecuteTransformations – 新政策	新增了新的 AWS 受管政策，提供在轉換自訂中執行 AWS 轉換的存取權。	2025 年 12 月 5 日
AWSTransformCustomManageTransformations – 新政策	新增了新的 AWS 受管政策，提供在轉換自訂中建立、更新、讀取和刪除 AWS 轉換資源的存取權，以及執行轉換。	2025 年 12 月 5 日
AWSServiceRoleForAWSTransform – 已更新政策	新增存取 AWS Transform 服務連結秘密的許可，用於存放外部身分提供者的用戶端秘密。 新增從 AWS Transform Web 應用程式建立進階支援案例的許可。	2025 年 12 月 1 日
AWSTransformApplicationECSDeploymentPolicy – 已更新政策	新增 IAM 角色檢查許可、建立 ECS 服務連結角色，以及支援 ECR 加密的 KMS 許可。	2025 年 11 月 22 日
AWSTransformApplicationDeploymentPolicy – 已更新政策	新增 EC2 網路許可、IAM 角色檢查許可、S3 儲存貯體清單許可，以及增強型部署功能的 KMS 加密支援。	2025 年 11 月 22 日
AWSServiceRoleForAWSTransform – 已更新政策	新增對 IAM Identity Center 中客戶受管金鑰的支援。	2025 年 9 月 17 日

變更	描述	日期
AWSTransformApplicationDeploymentPolicy – 新政策	新增了新的 AWS 受管政策，可讓 AWS Transform 透過建立和管理 Amazon EC2 執行個體、 CloudFormation 堆疊和相關資源來部署轉換的 .NET 應用程式。	2025 年 8 月 28 日
AWSServiceRoleForAWSTransform – 已更新政策	新增了新的政策。	2025 年 5 月 15 日

AWS 受管政策：AWSServiceRoleForAWSTransform

此政策會連接至 AWSServiceRoleForAWSTransform 服務連結角色 (SLR)。

許可詳細資訊

若要檢視政策許可詳細資訊，請參閱《 AWS 受管政策參考指南》中的 AWSServiceRoleForAWSTransform。

AWS 受管政策：AWSServiceRoleForAWSTransformCustom

此政策會連接至 AWSServiceRoleForAWSTransformCustom 服務連結角色 (SLR)。此角色允許 AWS 轉換自訂代表您將 CloudWatch 指標和日誌發佈至您的帳戶。

Description

此政策包含以下許可：

- Amazon CloudWatch – 允許在`AWS/TransformCustom`命名空間下將指標發佈至 CloudWatch。這可讓您監控 CloudWatch 儀表板中的轉換計數、延遲和狀態碼。
- Amazon CloudWatch Logs – 允許建立日誌群組、日誌串流、設定保留政策，以及將日誌事件發佈至`/aws/TransformCustom`日誌群組。這可讓您了解轉換期間遇到的問題。

AWS 受管政策：AWSTransformApplicationDeploymentPolicy

此政策可讓 AWS Transform 透過建立和管理 Amazon EC2 執行個體、 CloudFormation 堆疊和相關聯的資源來部署轉換的 .NET 應用程式。

Description

此政策包含以下許可：

- CloudFormation – 允許建立、更新、刪除和描述名稱開頭為 AWSTransform 的 CloudFormation 堆疊。堆疊操作僅限於以 CreatedBy：AWSTransform 標記的資源，且僅限於相同的 AWS 帳戶。
- Amazon EC2 – 允許描述 VPCs、子網路、安全群組、映像、執行個體、路由表和網際網路閘道。允許執行、啟動、停止、終止和修改 EC2 執行個體，但僅限於透過 CloudFormation 呼叫 時。標籤建立僅限於特定允許的標籤金鑰，且僅限於 CloudFormation 操作期間。
- AWS Identity and Access Management (IAM) – 允許取得和傳遞 AWSTransform 部署執行個體的特定 IAM 角色。包含檢查角色政策和附件的許可。存取僅限於相同的 AWS 帳戶。
- Amazon EC2 Systems Manager (SSM) – 允許從 AWS受管參數存放區擷取 Amazon Linux AMI 參數，並將命令傳送至 AWSTransform 標記的執行個體。
- Amazon S3 – 允許管理 AWSTransform 部署儲存貯體中的物件，包括列出儲存貯體，以及在相同 AWS 帳戶中取得儲存貯體位置。
- AWS Key Management Service (KMS) – 允許使用為 AWSTransform 加上標籤的 KMS 金鑰進行加密和解密操作，並限制 S3 和 EC2 服務用量。

此政策會透過資源層級許可、標籤型條件、使用 的服務控制限制`aws:CalledVia`、帳戶層級限制和明確拒絕陳述式來實作最低權限存取，以防止在 CloudFormation 操作之外進行未經授權的標籤修改。

許可詳細資訊

若要檢視政策許可詳細資訊，請參閱《 AWS 受管政策參考指南》中的 AWSTransformApplicationDeploymentPolicy。

AWS 受管政策：AWSTransformApplicationECSDeploymentPolicy

此政策可讓 AWS Transform 透過建立和管理 ECS 叢集、服務、任務和相關聯的資源，將轉換的應用程式部署到 Amazon ECS。

Description

此政策包含以下許可：

- CloudFormation – 允許建立、更新、刪除和描述名稱開頭為 AWSTransform 的 CloudFormation 堆疊。堆疊操作僅限於以 CreatedBy：AWSTransform 標記的資源，且僅限於相同的 AWS 帳戶。

- Amazon ECS – 允許建立、更新和刪除 ECS 叢集、服務和任務定義。允許執行中的任務、列出任務，以及描述任務狀態。所有操作僅限於名稱開頭為 AWSTransform 並以 CreatedBy：AWSTransform 標記的資源。
- AWS Identity and Access Management (IAM) – 允許取得和傳遞 ECS 任務的特定 IAM 角色 (AWSTransform-Deploy-ECS-Task-Role 和 AWSTransform-Deploy-ECS-Execution-Role)。包含檢查角色政策的許可，並在需要時建立 ECS 服務連結角色。
- Amazon CloudWatch Logs – 允許建立、刪除和管理名稱開頭為 /aws/ecs/AWSTransform 的日誌群組。允許擷取日誌事件，以對部署的應用程式進行故障診斷。
- Amazon ECR – 允許建立名稱開頭為 awstransform 的容器儲存庫，以存放應用程式容器映像。
- AWS Key Management Service (KMS) – 允許在使用客戶受管 KMS 金鑰時建立授予和產生 ECR 加密的資料金鑰。

此政策會透過資源層級許可、標籤型條件和帳戶層級限制實作最低權限存取，以確保操作僅限於相同 AWS 帳戶中的 AWSTransform 受管資源。

許可詳細資訊

若要檢視政策許可詳細資訊，請參閱《 AWS 受管政策參考指南》中的 AWSTransformApplicationECSDeploymentPolicy。

AWS 受管政策：AWSTransformCustomFullAccess

此政策提供 AWS 轉換自訂的完整存取權。

Description

此政策包含以下許可：

- AWS 轉換自訂 – 允許所有 AWS 轉換自訂資源上的所有動作。這可提供 服務的完整管理存取權。
- AWS Identity and Access Management (IAM) – 允許建立 AWS 轉換自訂服務連結角色 (`AWSServiceRoleForAWSTransformCustom`)。 AWS 轉換自訂需要此角色，才能將 CloudWatch 指標和日誌傳送到您的帳戶。許可的範圍僅限於允許建立此特定服務連結角色。

許可詳細資訊

若要檢視政策許可詳細資訊，請參閱《 AWS 受管政策參考指南》中的 AWSTransformCustomFullAccess。

AWS 受管政策：AWSTransformCustomExecuteTransformations

此政策提供在轉換自訂中執行 AWS 轉換的存取權。

Description

此政策包含以下許可：

- AWS 轉換自訂 – 允許串流對話、執行轉換和管理行銷活動。包括取得行銷活動詳細資訊、更新行銷活動儲存庫狀態和更新行銷活動的許可。
- AWS Identity and Access Management (IAM) – 允許建立 AWS 轉換自訂服務連結角色 (`AWSServiceRoleForAWSTransformCustom`)。 AWS 轉換自訂需要此角色，才能將 CloudWatch 指標和日誌傳送到您的帳戶。許可的範圍僅限於允許建立此特定服務連結角色。

許可詳細資訊

若要檢視政策許可詳細資訊，請參閱《 AWS 受管政策參考指南》中的 AWSTransformCustomExecuteTransformations。

AWS 受管政策：AWSTransformCustomManageTransformations

此政策提供在轉換自訂中建立、更新、讀取和刪除 AWS 轉換資源的存取權，以及執行轉換。

Description

此政策包含以下許可：

- AWS 轉換自訂 – 允許全面管理轉換資源，包括串流對話、執行轉換和管理轉換套件。允許建立、取得和刪除轉換套件 URLs以及完成套件上傳。
- 知識管理 – 允許列出、取得、刪除和更新知識項目及其組態和狀態。
- 行銷活動管理 – 允許取得行銷活動詳細資訊、更新行銷活動儲存庫狀態，以及更新行銷活動。
- 資源標記 – 允許列出、新增和移除 AWS 轉換自訂資源的標籤。
- AWS Identity and Access Management (IAM) – 允許建立 AWS 轉換自訂服務連結角色 (`AWSServiceRoleForAWSTransformCustom`)。 AWS 轉換自訂需要此角色，才能將 CloudWatch 指標和日誌傳送到您的帳戶。許可的範圍僅限於允許建立此特定服務連結角色。

許可詳細資訊

若要檢視政策許可詳細資訊，請參閱《 AWS 受管政策參考指南》中的 AWSTransformCustomManageTransformations。

AWS 受管政策：AWSTransformInfrastructureExecutorAccessBatch

此政策授予使用 AWS Batch 執行 AWS Transform Continuous Modernization 評估和轉換所需的許可。將此政策連接至您帳戶中的 IAM 角色。 AWS 轉換持續現代化 CLI 和客服人員會擔任此角色，以上傳原始程式碼、擷取結果、監控批次任務狀態、讀取日誌和管理轉換排程。

Description

此政策包含以下許可：

- AWS Lambda – 允許調用和擷取協調轉換工作流程的特定 `atx`字首 Lambda 函數的組態，包括任務觸發、狀態擷取和任務清單函數。
- Amazon S3 – 允許將原始碼上傳至儲存`atx-source-code-*`貯體、從 `atx-custom-output-*`和 儲存`atx-ct-output-*`貯體下載轉換結果，以及將批次附屬輸出寫入儲存`atx-custom-output-*`貯體。
- AWS Key Management Service (KMS) – 允許使用 AWS 轉換加密金鑰 () 加密和解密資料`alias/atx-encryption-key`。
- Amazon CloudWatch Logs – 允許讀取 Batch 任務和 Lambda 執行日誌事件以進行轉換監控和偵錯。
- Amazon CloudWatch – 允許取得和列出 AWS Transform CLI 儀表板以取得操作可見性。
- AWS 批次 – 允許描述和列出運算環境、任務佇列、任務定義和任務狀態。
- CloudFormation – 允許描述和列出 AWS 轉換基礎設施堆疊，包括 Security Agent 堆疊，以檢查部署狀態。
- 資源群組標記 API – 允許擷取已標記的資源，以探索您帳戶中的 AWS 轉換基礎設施。
- AWS Secrets Manager – 允許擷取和描述儲存在`atx/`字首下的 AWS 轉換秘密。
- Amazon EventBridge 排程器 – 允許在`atx-ct`排程群組中管理排程轉換任務。
- Amazon EC2 – 允許描述批次運算環境聯網的 VPC、子網路、安全群組、路由表和 NAT 閘道組態。
- AWS Identity and Access Management (IAM) – 允許讀取 `ATX`字首和 `Atx`字首角色組態，以驗證基礎設施設定，並將 傳遞`AtxSchedulerInvocationRole`至 Amazon EventBridge 排程器，使其可以調用排程任務。

此政策會透過資源層級許可、標籤型條件、aws:ResourceAccount條件和服務範圍iam:PassedToService條件實作最低權限存取，以確保操作僅限於相同 AWS 帳戶中的 AWS 轉換資源。

許可詳細資訊

若要檢視政策許可詳細資訊，請參閱《 AWS 受管政策參考指南》中的AWSTransformInfrastructureExecutorAccessBatch。

AWS 受管政策：AWSTransformInfrastructureExecutorAccessEC2

此政策授予使用 Amazon EC2 執行 AWS 轉型持續現代化評估和轉換所需的許可。將此政策連接至您帳戶中的 IAM 角色。 AWS Transform Continuous Modernization CLI 和代理程式會擔任此角色，以上傳原始程式碼、擷取結果、監控任務狀態，以及管理轉換排程。

Description

此政策包含以下許可：

- CloudFormation – 允許描述 AWS 轉換基礎設施堆疊 （包括安全代理程式堆疊）、堆疊事件、堆疊資源和偏離偵測狀態、列出堆疊，以及在部署之前驗證 CloudFormation 範本。
- Amazon EC2 – 允許描述執行個體、AMIs、VPCs、子網路、安全群組、金鑰對、路由表、NAT 閘道和網際網路閘道。允許啟動和停止以 標記的 EC2 執行個體atx-remote-infra: true。
- Amazon EC2 Systems Manager (SSM) – 允許監控命令執行狀態，以及在具有 AWS 轉換標籤的執行個體上執行命令和工作階段，包括執行AWS-RunShellScript文件。
- Amazon S3 – 允許管理 AWS 轉換儲存貯體中的原始程式碼和輸出成品，包括取得、放置和刪除物件和列出儲存貯體。
- AWS Key Management Service (KMS) – 允許使用 AWS 轉換加密金鑰 () 加密和解密資料alias/atx-encryption-key。
- AWS Secrets Manager – 允許擷取和描述存放在atx/字首下的轉換秘密，例如儲存庫登入資料。
- Amazon EventBridge 排程器 – 允許在atx-ct排程群組中管理排程轉換任務。
- 資源群組標記 API – 允許擷取已標記的資源，以探索您帳戶中的 AWS 轉換基礎設施。
- AWS Identity and Access Management (IAM) – 允許將atx-transform-role*角色傳遞至 Amazon EC2，並將 傳遞AtxSchedulerInvocationRole至 Amazon EventBridge 排程器，以及讀取 EC2 執行個體的角色和執行個體描述檔組態。

此政策會透過資源層級許可、標籤型條件、aws:ResourceAccount條件和服務範圍iam:PassedToService條件實作最低權限存取，以確保操作僅限於相同 AWS 帳戶中的 AWS 轉換資源。

許可詳細資訊

若要檢視政策許可詳細資訊，請參閱《 AWS 受管政策參考指南》中的AWSTransformInfrastructureExecutorAccessEC2。

AWS 受管政策：AWSTransformSecurityAgentExecutorAccess

此政策授予 AWS Transform Continuous Modernization 調用 AWS Security Agent 服務以進行自動程式碼安全檢閱和修復所需的許可。將此政策連接到您帳戶中的 IAM 角色， AWS 轉換持續現代化 CLI 和代理程式會擔任此角色，以上傳掃描成品並擷取問題清單。

Description

此政策包含以下許可：

- AWS 安全代理程式 – 允許列出代理程式空間、建立程式碼檢閱、啟動程式碼檢閱任務、列出和擷取問題清單，以及啟動程式碼修復。這些動作的範圍限定為您帳戶中的客服人員空間。
- Amazon S3 – 允許從儲存atx-security-agent-*貯體下載掃描結果和調查結果，並將用於安全性掃描的原始碼上傳至該儲存貯體內的security-scans/*字首。
- AWS Identity and Access Management (IAM) – 允許將security-agent-*角色傳遞至 AWS Security Agent 服務，使其可執行掃描。
- CloudFormation – 允許列出帳戶中的堆疊，並描述AtxSecurityAgentStack-*堆疊以探索和監控 Security Agent 基礎設施部署狀態。

此政策會透過資源層級許可、S3 儲存貯體和金鑰字首、 aws:ResourceAccount和s3:ResourceAccount條件和服務範圍iam:PassedToService條件來實作最低權限存取，以確保操作僅限於 AWS 相同 AWS 帳戶中的安全代理程式資源。

許可詳細資訊

若要檢視政策許可詳細資訊，請參閱《 AWS 受管政策參考指南》中的AWSTransformSecurityAgentExecutorAccess。

AWS 受管政策：DBModDiscoveryAndAssessment

此政策提供 AWS Transform 的全方位資料庫現代化探索和評估功能。

Description

此政策包含以下許可：

- Amazon EC2 – 允許描述基礎設施元件，包括執行個體、VPCs、子網路、安全群組、可用區域、VPC 端點和網際網路閘道。
- Amazon RDS – 允許描述資料庫執行個體、叢集和子網路群組。允許修改相同 AWS 帳戶中的資料庫子網路群組以進行遷移準備。
- Amazon RDS Data API – 允許啟用和停用 HTTP 端點，以及在標記資料庫現代化專案的資料庫叢集上執行 SQL 陳述式。
- AWS DMS – 允許描述端點、複寫執行個體、任務、子網路群組和可排序的執行個體。允許列出資料提供者、執行個體描述檔和遷移專案。允許描述資料表統計資料、評估執行和中繼資料模型操作。詳細描述和中繼資料操作僅限於為資料庫現代化專案加上標籤的資源。
- ：允許列出秘密以探索資料庫登入資料。
- AWS Identity and Access Management (IAM) – 允許檢查特定 AWS DMS 服務角色及其連接的政策。包括讀取 AWS受管 AWS DMS 政策的存取權。
- AWS Key Management Service (KMS) – 允許列出金鑰別名和描述金鑰。允許透過整合解密秘密，僅限於相同的 AWS 帳戶。

此政策會透過資源層級許可、標籤型條件和帳戶層級限制實作最低權限存取，以確保操作僅限於相同 AWS 帳戶中的資料庫現代化專案資源。

許可詳細資訊

若要檢視政策許可詳細資訊，請參閱《 AWS 受管政策參考指南》中的 DBModDiscoveryAndAssessment。

AWS 受管政策：DBModProvisioningAndMigration

此政策為 AWS 轉換資料庫現代化專案提供資料庫佈建和遷移功能。它包含建立和管理遷移基礎設施、佈建目標資料庫和存放遷移資料的許可。

Description

此政策包含以下許可：

- AWS DMS – 允許建立和管理複寫子網路群組、執行個體描述檔、資料提供者、遷移專案、端點、複寫執行個體和複寫任務。包括結構描述轉換操作，例如中繼資料模型匯入、轉換、匯出和評估。允許

複寫執行個體（建立、刪除、修改、重新啟動）和複寫任務（刪除、啟動、停止、評估）的生命週期管理。所有寫入操作僅限於為資料庫現代化專案加上標籤的資源。

- Amazon RDS – 允許建立資料庫子網路群組、資料庫叢集和資料庫執行個體。所有資源都必須為資料庫現代化專案加上標籤。
- – 允許使用資料庫現代化命名字首建立、更新和標記秘密。允許擷取秘密值並描述已標記資源的秘密。
- Amazon S3 – 允許建立和管理 S3 儲存貯體和物件以進行遷移資料儲存。包括儲存貯體標記、版本控制和物件生命週期操作。僅限於具有資料庫現代化命名字首的儲存貯體。
- AWS Identity and Access Management (IAM) – 允許將特定 AWS DMS 服務角色傳遞至 AWS DMS 和 結構描述轉換服務。允許建立資料庫操作所需的 Amazon RDS 服務連結角色。

此政策會透過資源層級許可、標籤型條件和帳戶層級限制實作最低權限存取，以確保操作僅限於相同 AWS 帳戶中的資料庫現代化專案資源。

許可詳細資訊

若要檢視政策許可詳細資訊，請參閱《 AWS 受管政策參考指南》中的 DBModProvisioningAndMigration。

AWS 轉換許可參考

本節提供 AWS Transform 所使用的 APIs 及其功能的相關資訊。

主題

- AWS 轉換 APIs

AWS 轉換 APIs

- transform：BatchGetMessage
- transform：BatchGetUserDetails
- transform：CompleteArtifactUpload
- transform：CreateArtifactDownloadUrl
- transform：CreateArtifactUploadUrl
- transform：CreateAssetDownloadUrl

- transform：CreateConnector
- transform：CreateFeedback
- transform：CreateJob
- transform：CreateSession
- transform：CreateWorkspace
- transform：DeleteConnector
- transform：DeleteJob
- transform：DeleteSelfRoleMappings
- transform：DeleteUserRoleMappings
- transform：DeleteWorkspace
- transform：DetectIsAllowedForOperation
- transform：GetConnector
- transform：GetFeedbackQuestions
- transform：GetHitlTask
- transform：GetJob
- transform：GetLoginRedirectUri
- transform：GetUserDetails
- transform：GetUserPreferences
- transform：GetWebAppUrl
- transform：GetWorkspace
- transform：ListArtifacts
- transform：ListConnectors
- transform：ListHitlTasks
- transform：ListJobPlanSteps
- transform：ListJobs
- transform：ListMessages
- transform：ListPlanUpdates
- transform：ListUserRoleMappings

- transform：ListWorklogs
- transform：ListWorkspaces
- transform：PutUserPreferences
- transform：PutUserRoleMappings
- transform：RevokeSession
- transform：SearchUsers
- transform：SearchUsersTypeahead
- transform：SendMessage
- transform：StartJob
- transform：StopJob
- transform：SubmitCriticalHitlTask
- transform：SubmitStandardHitlTask
- transform：TestReleaseTraitPreProd
- transform：TestReleaseTraitProd
- transform：UpdateHitlTask
- transform：UpdateJob
- transform：UpdateWorkspace
- transform：VerifySession

AWS 轉換的合規驗證

我們的新 AWS 註冊體驗並非針對受管制的工作負載而設計。如果您正在使用我們新的 AWS 註冊體驗，但想要將 AWS 用於受管制的工作負載，您可以註冊 AWS（進階）或為您的 AWS 環境啟用進階功能。

若要了解 是否 AWS 服務 在特定合規計劃範圍內，請參閱AWS 服務 合規計劃範圍內然後選擇您感興趣的合規計劃。如需一般資訊，請參閱AWS 合規計劃。

您可以使用 下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱下載報告下載 AWS Artifact。

您使用 時的合規責任 AWS 服務 取決於資料的機密性、您公司的合規目標，以及適用的法律和法規。如需使用 時合規責任的詳細資訊 AWS 服務，請參閱 AWS 安全文件。

AWS 轉換中的彈性

AWS 全球基礎設施是以 AWS 區域 和 可用區域為基礎建置。 AWS 區域 提供多個實體分隔和隔離的可用區域，這些可用區域與低延遲、高輸送量和高備援聯網連接。透過可用區域，您可以設計與操作的應用程式和資料庫，在可用區域之間自動容錯移轉而不會發生中斷。可用區域的可用性、容錯能力和擴展能力，均較單一或多個資料中心的傳統基礎設施還高。

如需 AWS 區域 和可用區域的詳細資訊，請參閱 AWS 全球基礎設施。

除了 AWS 全球基礎設施之外， AWS Transform 還提供數種功能，以協助支援您的資料彈性和備份需求。

AWS Transform 和介面端點 (AWS PrivateLink)

您可以建立介面 VPC 端點， AWS Transform 在 VPC 和 之間建立私有連線。介面端點採用 AWS PrivateLink技術，可讓您在沒有網際網路閘道、NAT 裝置、VPN 連接或 Direct Connect 連線的情況下私密存取 AWS Transform 主控台。VPC 與 之間的流量 AWS Transform 不會離開 Amazon 網路。

每個介面端點都是由您子網路中的一或多個彈性網路介面表示。

如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的介面 VPC 端點 (AWS PrivateLink)。

> **Note**
>
> 如需 AWS Transform 自訂 PrivateLink 文件，請參閱 AWS Transform 自訂和界面端點 (AWS PrivateLink)。

AWS Transform VPC 端點的考量事項

設定介面 VPC 端點之前 AWS Transform，請務必檢閱《Amazon VPC 使用者指南》中的介面端點屬性和限制。

先決條件

開始進行下方任何程序之前，務必先備妥下列各項：

- 具有適當許可來建立和設定資源 AWS 的帳戶。
- 已在 AWS 您的帳戶中建立 VPC。

- 熟悉 AWS 服務，特別是 Amazon VPC 和 AWS Transform。

建立 的介面 VPC 端點 AWS Transform

您可以使用 Amazon VPC 主控台或 AWS Command Line Interface () 來建立 AWS Transform 服務的 VPC 端點AWS CLI。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的建立介面端點。

AWS Transform 支援下列 VPC 端點服務：

服務名稱	Endpoint	注意
控制平面	`com.amazonaws.region.transform`	
代理 API	`com.amazonaws.region.transform-agents`	
Web 應用程式	`com.amazonaws.region.api.transform`	AWS Transform Web 應用程式的必要項目。此端點必須啟用私有 DNS (啟用 DNS 名稱選項），以便 `api.transform.region.on.aws`解析為您 VPC 中的私有 IP 地址。

將##取代為安裝設定檔 AWS AWS Transform 的區域，例如 com.amazonaws.us-east-1.transform。

> **Note**
>
> 如果您使用 AWS Transform Web 應用程式，則需要`api.transform`端點。如需完整的設定指南，請參閱 從 VPC 存取 AWS Transform Web 應用程式。

如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的透過介面端點支援的 區域 AWS Transform存取服務。 https://docs.aws.amazon.com/vpc/latest/userguide/vpce-interface.html#access-service-though-endpoint

使用內部部署電腦連線至 AWS Transform 端點

本節說明使用內部部署電腦 AWS Transform 透過 AWS VPC 中的 AWS PrivateLink 端點連線至 的程序。

1. 在內部部署裝置與 VPC 之間建立 VPN 連線。
2. 建立 的介面 VPC 端點 AWS Transform。
3. 設定傳入 Amazon Route 53 端點。這可讓您從內部部署裝置使用 AWS Transform 端點的 DNS 名稱。

從 VPC 存取 AWS Transform Web 應用程式

當您使用 從 VPC 私下 AWS PrivateLink 存取 AWS Transform API 時，Web 應用程式需要額外的網路組態。它透過需要網際網路連線的 CloudFront 提供靜態內容 (HTML、JavaScript、CSS)。Web 應用程式的 API 呼叫會經過您的 VPC 端點，並保持完全私有。

本指南說明如何設定 VPC 的受控網際網路輸出，讓 Web 應用程式可以載入，同時保持 VPC 鎖定在僅必要網域。

運作方式

AWS Transform Web 應用程式使用兩種網路路徑：

- API 呼叫 – 當您與 Web 應用程式（啟動任務、檢視工作區等）互動時，瀏覽器會將 API 請求傳送至 `api.transform.region.on.aws`。啟用 `com.amazonaws.region.api.transform` VPC 端點和私有 DNS 後，這些請求會解析為 VPC 中的私有 IP 地址，且永遠不會離開 AWS 網路。
- 靜態內容 – Web 應用程式的 HTML、JavaScript 和 CSS 檔案會透過 CloudFront 透過 提供`tenant-id`.transform.`region`.on.aws。載入這些檔案需要網際網路連線，因為 CloudFront 內容交付只能透過公有網際網路提供。
- 身分驗證 – AWS IAM Identity Center 登入流程使用 `region`.signin.aws，這也需要網際網路連線。

若要在維護安全性的同時啟用 Web 應用程式，您可以使用 AWS Network Firewall 搭配網域型篩選來建立受控的輸出路徑。這可讓您的 VPC 僅連接 Web 應用程式所需的特定網域，同時封鎖所有其他網際網路流量。

Architecture

下圖顯示 Web 應用程式流量的網路路徑：

```
EC2 Instance / Workspace (Private Subnet)
    |
    | Route: 0.0.0.0/0 # Network Firewall Endpoint
    v
AWS Network Firewall (Firewall Subnet)
    | Allows: *.cloudfront.net, *.transform.<region>.on.aws,
    |         <region>.signin.aws, SSO domains, S3 presigned URLs
    | Blocks: everything else (TLS SNI inspection)
    |
    | Route: 0.0.0.0/0 # NAT Gateway
    v
NAT Gateway (Public Subnet)
    |
    | Route: 0.0.0.0/0 # Internet Gateway
    v
Internet Gateway # CloudFront Edge Locations
```

Important

Network Firewall 必須查看兩個流量方向（對稱路由），才能執行 TLS SNI 檢查。您必須在 NAT Gateway 子網路中設定傳回路由，以透過防火牆傳送目的地為私有子網路的流量。否則，網域型篩選規則將無法運作。

先決條件

開始前，請確保您具備以下條件：

- 具有建立 VPC 資源、Network Firewall 和 NAT Gateways 許可 AWS 的帳戶。
- 具有私有子網路的 VPC，執行個體或工作負載會在其中執行。
- 連接至 VPC 的網際網路閘道（或建立 VPC 的許可）。
- 啟用私有 DNS `com.amazonaws.region.api.transform`的 AWS Transform VPC 端點。這是 Web 應用程式瀏覽器用戶端使用的端點。如需建立端點的指示，請參閱 AWS Transform 和介面端點 (AWS PrivateLink)。

設定 VPC 端點政策

如果您的 com.amazonaws.*region*.api.transform VPC 端點具有自訂端點政策，您必須新增允許 AWS Transform 操作的陳述式。如果沒有此功能，Web 應用程式將無法透過端點進行 API 呼叫。

將下列陳述式新增至您的 VPC 端點政策。將 *AWS_TRANSFORM_PROFILE_ARN* 取代為您的 AWS Transform 服務設定檔 ARN，您可以在 設定 頁面的 AWS Transform 主控台中找到。

```
{
    "Statement": [
        {
            "Sid": "AllowAWSTransform",
            "Effect": "Allow",
            "Principal": "*",
            "Action": "*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalArn": [
                        "AWS_TRANSFORM_PROFILE_ARN"
                    ]
                }
            }
        }
    ]
}
```

> **Note**
>
> 如果您的 VPC 端點使用預設政策 （ 完整存取 ），則不需要變更，您可以略過此步驟。

設定受控網際網路輸出

完成下列步驟，使用 AWS Transform Web 應用程式的網域型篩選來設定 Network Firewall。

步驟 1：建立防火牆子網路

建立 Network Firewall 端點專用的小型 /28 子網路。此子網路必須與私有子網路位於相同的可用區域。

```
aws ec2 create-subnet \
  --vpc-id your-vpc-id \
  --cidr-block firewall-subnet-cidr \
  --availability-zone your-az \
  --region region
```

步驟 2：建立 NAT 閘道的公有子網路

```
aws ec2 create-subnet \
  --vpc-id your-vpc-id \
  --cidr-block public-subnet-cidr \
  --availability-zone your-az \
  --region region
```

步驟 3：設定公有子網路路由表

為將網際網路流量路由到網際網路閘道的公有子網路建立路由表。

```
# Create route table
PUB_RTB=$(aws ec2 create-route-table \
  --vpc-id your-vpc-id \
  --region region \
  --query 'RouteTable.RouteTableId' --output text)

# Add default route to internet gateway
aws ec2 create-route \
  --route-table-id $PUB_RTB \
  --destination-cidr-block 0.0.0.0/0 \
  --gateway-id your-igw-id \
  --region region

# Associate with public subnet
aws ec2 associate-route-table \
  --route-table-id $PUB_RTB \
  --subnet-id public-subnet-id \
  --region region
```

步驟 4：建立 NAT 閘道

```
# Allocate an Elastic IP
EIP=$(aws ec2 allocate-address --domain vpc \
  --region region --query 'AllocationId' --output text)

# Create NAT Gateway in the public subnet
NAT_ID=$(aws ec2 create-nat-gateway \
  --subnet-id public-subnet-id \
  --allocation-id $EIP \
  --region region \
  --query 'NatGateway.NatGatewayId' --output text)

# Wait for NAT Gateway to become available (~2 minutes)
aws ec2 wait nat-gateway-available \
  --nat-gateway-ids $NAT_ID --region region
```

步驟 5：建立 Network Firewall 規則群組

建立狀態規則群組，僅允許流量流向 AWS Transform Web 應用程式所需的網域。

```
aws network-firewall create-rule-group \
  --rule-group-name transform-webapp-domains \
  --type STATEFUL \
  --capacity 100 \
  --rule-group '{
    "StatefulRuleOptions": {
      "RuleOrder": "STRICT_ORDER"
    },
    "RulesSource": {
      "RulesSourceList": {
        "Targets": [
          ".cloudfront.net",
          ".transform.region.on.aws",
          "region.signin.aws",
          ".s3.region.amazonaws.com",
          "oidc.region.amazonaws.com",
          "portal.sso.region.amazonaws.com",
          "assets.sso-portal.region.amazonaws.com",
          "directory-id.awsapps.com"
```

```
        ],
        "TargetTypes": ["TLS_SNI", "HTTP_HOST"],
        "GeneratedRulesType": "ALLOWLIST"
      }
    }
  }' \
  --region region
```

將##取代為安裝設定檔 AWS AWS Transform 的區域（例如 us-east-1)。將 *directory-id* 取代為您的 IAM Identity Center 目錄 ID（例如 d-1234567890)。您可以在 IAM Identity Center 主控台中找到目錄 ID。

下表說明允許的網域。

網域	用途
.cloudfront.net	CloudFront CDN – 提供 Web 應用程式靜態資產 (JavaScript、CSS、映像）
.transform. *region*.on.aws	Web 應用程式租用戶 URL – 瀏覽器會透過 CloudFront 從此網域載入初始頁面
region.signin.aws	SSO 登入重新導向頁面
.s3.*region*.amazonaws.com	S3 預先簽章URLs – 成品上傳和下載
oidc.*region*.amazonaws.com	SSO 身分驗證的 OIDC 權杖交換
portal.sso. *region*.amazonaws.com	SSO 入口網站登入頁面
assets.sso-portal. *region*.amazonaws.com	SSO 入口網站靜態資產 (CSS、JavaScript)
directory-id .awsapps.com	組織的 IAM Identity Center 入口網站

> **Note**
>
> 萬.cloudfront.net用字元允許任何 CloudFront 分佈的流量，而不只是 AWS Transform Web 應用程式的 。無法縮小網域篩選條件，因為 CloudFront 邊緣 IPs會跨分佈共用，且 TLS SNI 檢查無法區分相同網域後方的個別分佈。

> **Note**
>
> 要api.transform.*region*.on.aws進行 AWS PrivateLink 且不需要網際網路輸出的 API 呼叫。它們不受防火牆影響。

步驟 6：建立防火牆政策

政策必須使用STRICT_ORDER規則評估搭配 drop_established做為預設動作。這可確保捨棄不符合允許清單的任何流量。

```
# Get the rule group ARN
RG_ARN=$(aws network-firewall describe-rule-group \
  --rule-group-name transform-webapp-domains \
  --type STATEFUL --region region \
  --query 'RuleGroupResponse.RuleGroupArn' --output text)

# Create the firewall policy
aws network-firewall create-firewall-policy \
  --firewall-policy-name transform-webapp-policy \
  --firewall-policy "{
    \"StatelessDefaultActions\": [\"aws:forward_to_sfe\"],
    \"StatelessFragmentDefaultActions\": [\"aws:forward_to_sfe\"],
    \"StatefulRuleGroupReferences\": [
      {
        \"ResourceArn\": \"$RG_ARN\",
        \"Priority\": 1
      }
    ],
    \"StatefulEngineOptions\": {
      \"RuleOrder\": \"STRICT_ORDER\"
    },
    \"StatefulDefaultActions\": [\"aws:drop_established\", \"aws:alert_established\"]
```

```
  }" \
  --region region
```

步驟 7：建立網路防火牆

```
# Get the policy ARN
FW_POLICY_ARN=$(aws network-firewall describe-firewall-policy \
  --firewall-policy-name transform-webapp-policy \
  --region region \
  --query 'FirewallPolicyResponse.FirewallPolicyArn' --output text)

# Create the firewall
aws network-firewall create-firewall \
  --firewall-name transform-webapp-firewall \
  --firewall-policy-arn $FW_POLICY_ARN \
  --vpc-id your-vpc-id \
  --subnet-mappings SubnetId=firewall-subnet-id \
  --region region

# Wait for the firewall to become READY (3-5 minutes)
while true; do
  STATUS=$(aws network-firewall describe-firewall \
    --firewall-name transform-webapp-firewall \
    --region region \
    --query 'FirewallStatus.Status' --output text)
  echo "Status: $STATUS"
  if [ "$STATUS" = "READY" ]; then break; fi
  sleep 15
done
```

步驟 8：取得防火牆端點 ID

```
FW_ENDPOINT=$(aws network-firewall describe-firewall \
  --firewall-name transform-webapp-firewall \
  --region region \
  --query "FirewallStatus.SyncStates.\"your-az\".Attachment.EndpointId" \
  --output text)
echo "Firewall endpoint: $FW_ENDPOINT"
```

步驟 9：設定防火牆子網路路由表

將網際網路繫結流量從防火牆子網路路由到 NAT Gateway。

```
FW_RTB=$(aws ec2 create-route-table \
  --vpc-id your-vpc-id \
  --region region \
  --query 'RouteTable.RouteTableId' --output text)

aws ec2 create-route \
  --route-table-id $FW_RTB \
  --destination-cidr-block 0.0.0.0/0 \
  --nat-gateway-id $NAT_ID \
  --region region

aws ec2 associate-route-table \
  --route-table-id $FW_RTB \
  --subnet-id firewall-subnet-id \
  --region region
```

步驟 10：更新私有子網路路由表

透過防火牆路由來自私有子網路的所有網際網路繫結流量。

```
aws ec2 create-route \
  --route-table-id private-subnet-route-table-id \
  --destination-cidr-block 0.0.0.0/0 \
  --vpc-endpoint-id $FW_ENDPOINT \
  --region region
```

如果預設路由已存在，請使用 `replace-route`而非 `create-route`。

步驟 11：新增對稱傳回路由（必要）

> **Important**
>
> 此步驟至關重要。Network Firewall 使用 TLS SNI 檢查，且必須查看 TCP 連線的兩個方向。在 NAT Gateway 子網路的路由表中新增路由，透過防火牆傳送目的地為私有子網路的傳回流量。

```
aws ec2 create-route \
  --route-table-id $PUB_RTB \
  --destination-cidr-block private-subnet-cidr \
  --vpc-endpoint-id $FW_ENDPOINT \
  --region region
```

將 *private-subnet-cidr* 取代為私有子網路的 CIDR 區塊（例如 `10.0.144.0/20`）。

如果沒有對稱路由，防火牆只會看到一個流量方向。TLS 檢查引擎無法從 TLS 交握中擷取伺服器名稱指示 (SNI)，而且所有以網域為基礎的規則都將無提示地失敗。

步驟 12：移除 IPv6 預設路由（如果有）

如果私有子網路路由表具有直接指向網際網路閘道的 IPv6 預設路由 (`::/0`)，它會略過IPv6-capable目的地的防火牆。移除它：

```
aws ec2 delete-route \
  --route-table-id private-subnet-route-table-id \
  --destination-ipv6-cidr-block ::/0 \
  --region region
```

驗證

從私有子網路中的執行個體，驗證組態：

```
# Should SUCCEED - web application content via CloudFront (allowed)
curl -vL --connect-timeout 15 \
  'https://tenant-id.transform.region.on.aws'

# Should SUCCEED - API via PrivateLink (does not use firewall)
curl -v --connect-timeout 15 \
  'https://api.transform.region.on.aws/'

# Should FAIL - non-allowlisted domain (blocked by firewall)
curl -v --connect-timeout 15 'https://www.example.com'
# Expected: TLS connection error (firewall drops after SNI inspection)
```

疑難排解

防火牆會封鎖對 api.transform 的 API 呼叫

網域`api.transform.region.on.aws`應透過 VPC 端點解析為私有 IP 地址，且不應到達您的網際網路防火牆。

- 確認您已建立`com.amazonaws.region.api.transform`端點。
- 確認已在端點上啟用私有 DNS：

```
aws ec2 describe-vpc-endpoints \
  --filters "Name=service-name,Values=com.amazonaws.region.api.transform" \
  --query 'VpcEndpoints[*].[State,PrivateDnsEnabled]' \
  --output table
```

預期的輸出：`available | True`

Web 應用程式不會載入（連線逾時）

- 確認私有子網路路由表具有指向防火牆端點的`0.0.0.0/0`路由。
- 確認防火牆子網路路由表具有指向 NAT Gateway 的`0.0.0.0/0`路由。
- 驗證 NAT 閘道處於 `available` 狀態。

未允許清單的網域不會遭到封鎖

- 檢查指向網際網路閘道的 IPv6 `::/0`路由。這會略過防火牆。將其移除（步驟 12)。
- 確認已設定對稱路由。NAT Gateway 子網路路由表必須透過防火牆為私有子網路 CIDR 設定傳回路由（步驟 11)。

- 驗證防火牆政策使用 `STRICT_ORDER` 搭配 `drop_established`和 `alert_established`做為預設動作。

成本考量

資源	大約成本
Network Firewall	每個可用區域 ~$0.395/小時 (~$288/月)
NAT 閘道	~$0.045/小時 (~$33/月) + 資料處理費用
彈性 IP （公有 IPv4)	~$0.005/小時 (~$3.60/月)
Network Firewall 資料處理	0.065 USD/GB
NAT Gateway 資料處理	$0.045/GB

單一可用區域部署的預估基本成本約為每月 325 美元。對於生產部署，請在私有子網路存在的每個可用區域中部署防火牆、NAT Gateway 和相關聯的子網路。

清除

若要移除本指南建立的所有資源，請以相反順序執行下列命令。將預留位置取代為部署中的資源 IDs。您可以在 AWS 管理主控台中找到這些值，或使用設定步驟中的`describe`命令。

```
# Remove return route from NAT Gateway subnet
aws ec2 delete-route --route-table-id pub-rtb-id \
  --destination-cidr-block private-subnet-cidr \
  --region region

# Remove route from private subnet
aws ec2 delete-route \
  --route-table-id private-subnet-route-table-id \
  --destination-cidr-block 0.0.0.0/0 --region region

# Delete Network Firewall (takes ~5 minutes)
aws network-firewall delete-firewall \
  --firewall-name transform-webapp-firewall \
  --region region
```

```
# Delete firewall policy and rule group
aws network-firewall delete-firewall-policy \
  --firewall-policy-name transform-webapp-policy \
  --region region
aws network-firewall delete-rule-group \
  --rule-group-name transform-webapp-domains \
  --type STATEFUL --region region

# Delete NAT Gateway (wait ~5 minutes for full deletion)
aws ec2 delete-nat-gateway --nat-gateway-id nat-gateway-id \
  --region region

# Release Elastic IP
aws ec2 release-address --allocation-id eip-allocation-id \
  --region region

# Delete subnets
aws ec2 delete-subnet --subnet-id firewall-subnet-id \
  --region region
aws ec2 delete-subnet --subnet-id public-subnet-id \
  --region region
```

監控 AWS 轉換

監控是維護 AWS Transform 和其他 AWS 解決方案的可靠性、可用性和效能的重要部分。 AWS 提供下列監控工具來監看 AWS Transform、在發生錯誤時回報，以及適時採取自動動作：

- Amazon CloudWatch AWS 會即時監控您的 AWS 資源和您在 上執行的應用程式。您可以收集和追蹤指標、建立自訂儀板表，以及設定警示，在特定指標達到您指定的閾值時通知您或採取動作。例如，您可以讓 CloudWatch 追蹤 CPU 使用量或其他 Amazon EC2 執行個體指標，並在需要時自動啟動新的執行個體。如需詳細資訊，請參閱 Amazon CloudWatch 使用者指南。
- Amazon CloudWatch Logs 可讓您監控、存放和存取來自 Amazon EC2 執行個體、CloudTrail 及其他來源的日誌檔案。CloudWatch Logs 可監控日誌檔案中的資訊，並在達到特定閾值時通知您。您也可以將日誌資料存檔在高耐用性的儲存空間。如需詳細資訊，請參閱 Amazon CloudWatch Logs 使用者指南。
- Amazon EventBridge 可用來自動化您的 AWS 服務，並自動回應系統事件，例如應用程式可用性問題或資源變更。來自 AWS 服務的事件會以近乎即時的方式交付至 EventBridge。您可編寫簡單的規則，來指示您在意的事件，以及當事件符合規則時所要自動執行的動作。如需詳細資訊，請參閱 Amazon EventBridge 使用者指南。
- AWS CloudTrail 會擷取您 AWS 帳戶或代表您的帳戶發出的 API 呼叫和相關事件，並將日誌檔案交付至您指定的 Amazon S3 儲存貯體。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 地址，以及呼叫的時間。如需詳細資訊，請參閱「AWS CloudTrail 使用者指南」。

使用 記錄 AWS 轉換 API 呼叫 AWS CloudTrail

AWS 轉換已與 服務整合 AWS CloudTrail，此服務提供使用者、角色或 AWS 服務在 AWS 轉換中採取之動作的記錄。CloudTrail 會將 AWS Transform 的所有 API 呼叫擷取為事件。擷取的呼叫包括轉換 AWS 主控台的呼叫，以及對 AWS 轉換 API 操作的程式碼呼叫。如果您建立線索，則可以將 CloudTrail 事件持續交付至 Amazon S3 儲存貯體，包括 AWS 轉換的事件。即使您未設定追蹤，依然可以透過 CloudTrail 主控台中的事件歷史記錄檢視最新事件。使用 CloudTrail 所收集的資訊，您可以判斷對 AWS Transform 提出的請求、提出請求的 IP 地址、提出請求的人員、提出請求的時間，以及其他詳細資訊。

若要進一步了解 CloudTrail，請參閱「AWS CloudTrail 使用者指南」。

AWS 轉換 CloudTrail 中的資訊

當您建立帳戶 AWS 帳戶 時，您的 上會啟用 CloudTrail。在 AWS 轉換中發生活動時，該活動會與事件歷史記錄中的其他 AWS 服務事件一起記錄在 CloudTrail 事件中。您可以在 中檢視、搜尋和下載最近的事件 AWS 帳戶。如需詳細資訊，請參閱「使用 CloudTrail 事件歷史記錄檢視事件」。

若要持續記錄 中的事件 AWS 帳戶，包括 AWS 轉換的事件，請建立追蹤。線索能讓 CloudTrail 將日誌檔案交付至 Amazon S3 儲存貯體。依預設，當您在主控台中建立追蹤時，該追蹤會套用至所有的 AWS 區域。線索會記錄 AWS 分割區中所有區域的事件，並將日誌檔案交付至您指定的 Amazon S3 儲存貯體。此外，您可以設定其他 AWS 服務，以進一步分析和處理 CloudTrail 日誌中所收集的事件資料。如需詳細資訊，請參閱下列內容：

- 建立追蹤的概觀
- CloudTrail 支援的服務和整合
- 設定 CloudTrail 的 Amazon SNS 通知
- 接收多個區域的 CloudTrail 日誌檔案和接收多個帳戶的 CloudTrail 日誌檔案

每一筆事件或日誌專案都會包含產生請求者的資訊。身分資訊可協助您判斷下列事項：

- 是否使用根或 AWS Identity and Access Management (IAM) 使用者登入資料提出請求。
- 提出該請求時，是否使用了特定角色或聯合身分使用者的暫時安全憑證。
- 請求是否由其他 AWS 服務提出。

如需詳細資訊，請參閱 CloudTrail userIdentity 元素。

了解 AWS 轉換日誌檔案項目

追蹤是一種組態，能讓事件以日誌檔案的形式交付到您指定的 Amazon S3 儲存貯體。CloudTrail 日誌檔案包含一或多個日誌專案。一個事件為任何來源提出的單一請求，並包含請求動作、請求的日期和時間、請求參數等資訊。CloudTrail 日誌檔並非依公有 API 呼叫的堆疊追蹤排序，因此不會以任何特定順序出現。

通知

AWS 轉換提供電子郵件通知，讓您隨時了解工作區存取變更、任務狀態更新和待定協作者請求。

電子郵件通知

電子郵件通知預設為啟用，並傳送給對任務具有唯讀或更高許可的使用者。使用者可以修改其通知偏好設定。電子郵件通知有三種類別：

- 工作區存取更新

  當您新增至新的工作區，以及在工作區內變更角色時，您會收到通知。

- 每日摘要電子郵件

  如果您有一或多個開啟必要協同合作者請求的作用中任務，您會在太平洋時間上午 9：00 收到摘要進行中任務的每日摘要電子郵件。電子郵件包含顯示工作區名稱、任務名稱、任務狀態、協作者請求詳細資訊和必要動作的資料表 （僅限 10 列）

  > **Note**
  >
  > 每日摘要電子郵件只會針對需要協作者請求的任務傳送。選用的協作者請求不會觸發摘要電子郵件。

- 任務狀態更新

  當您可存取 的任務完成或失敗時，您會收到一封電子郵件。

- 協作器請求更新

  每當任務需要輸入、檢閱或核准時，您會收到一封電子郵件。

管理電子郵件通知

您可以按一下應用程式右上角的設定齒輪，然後選擇通知設定，以修改 Web 應用程式中的電子郵件通知偏好設定。

通知設定頁面提供下列控制項：

通知類型	說明	預設設定
工作區存取更新	新增到工作區或在工作區內變更角色時接收電子郵件	已啟用

通知類型	說明	預設設定
每日協作器請求摘要	接收可存取工作區中任務的開放協作者請求的每日摘要	已啟用
任務完成更新	當任務完成或失敗時接收電子郵件	已啟用
協作器請求更新	當您需要輸入或核准時接收電子郵件	Disabled

您可以使用一般設定來啟用或停用所有通知，或分別設定個別通知類型。

AWS 轉換的配額

AWS 您的帳戶具有每個 AWS 服務的預設配額，先前稱為限制。除非另有說明，否則每個配額都是區域特定的。您可以請求提高某些配額，而其他配額無法提高。

若要檢視 AWS 轉換的配額，請開啟 Service Quotas 主控台。在導覽窗格中，選擇 AWS 服務，然後選取AWS 轉換。

若要請求提升配額，請參閱《Service Quotas 使用者指南》中的請求提升配額。如果 Service Quotas 中尚未提供配額，請使用限制增加表單。

AWS 您的帳戶具有與 AWS 轉換相關的下列配額。

工作負載	維度	配額	可調整	說明
平台	AWS 區域 每個 AWS Transform 已啟用帳戶的工作區數	每個支援的 100 個工作區 AWS 區域	是	每個 AWS Transform已啟用之帳戶的工作區數量上限 AWS 區域
VMWare 遷移	每個波次的伺服器計數	每次波動：150 個伺服器	否	波動中的伺服器數量上限
大型主機	每個 IAM Identity Center 帳戶的並行任務	每個支援區域的 10 個任務	是	IAM Identity Center 帳戶中並行大型主機任務的數量上限
	每個任務的程式碼行	每個支援區域 3，000，000 行程式碼	否	每個任務的程式碼行數上限。
	分析每月程式碼行	每個支援區域 100，000，000 行程式碼	是	一個日曆月中分析程式碼任務目標的程式碼行數上限

工作負載	維度	配額	可調整	說明
	商業文件產生每月程式碼行	每個支援區域 50，000，000 行程式碼	是	一個日曆月中商業文件產生任務目標的程式碼行數上限
	技術文件產生每月程式碼行	每個支援區域 50，000，000 行程式碼	是	一個日曆月中技術文件產生任務目標的程式碼行數上限
	程式碼行的轉換	每個支援區域 10，000，000 行程式碼	是	日曆月中轉換的程式碼行數上限
	分解每月程式碼行	每個支援區域 50，000，000 行程式碼	是	一個日曆月中分解任務目標的程式碼行數上限
	重新建構每月程式碼行	每個支援區域 50，000，000 行程式碼	是	日曆月中 Reforge 任務目標的程式碼行數上限
	擷取商業邏輯每月程式碼行	每個支援區域 50，000，000 行程式碼	是	一個日曆月中已擷取商業邏輯任務目標的程式碼行數上限
.NET	.NET 每月程式碼行 (Web 和 IDE)	每個支援區域的 1，000，000 行程式碼	是	在 IAM Identity Center 帳戶的每個支援的日曆月中，可以轉換 AWS 區域的 .NET 應用程式程式碼行上限

工作負載	維度	配額	可調整	說明
	每個 IAM Identity Center 帳戶的 Microsoft Visual Studio Extension 並行 .NET 任務	每個支援區域的 10 個任務	是	使用 Microsoft Visual Studio 延伸模組時 AWS 區域 ，IAM Identity Center 帳戶每個支援的並行 .NET 轉換任務數量上限。
	每個 IAM Identity Center 帳戶的並行 .NET Web 任務	每個支援區域的 5 個任務	是	使用 AWS Transform Web 應用程式時 AWS 區域 ，IAM Identity Center 帳戶每個支援的並行 .NET 轉換任務數量上限。
自訂轉換	自訂轉換定義	1,000	是	自訂轉換定義的數目上限
	自訂轉換定義大小	10 MB	否	轉換定義中包含的所有檔案的總大小上限，包括文件參考。
	自訂轉換每月 CLI 對話請求	1,000,000	是	一個日曆月在 CLI 中允許的自訂轉換對話請求數目上限
評估	每個評估的伺服器計數限制	每次評估：30，000 個伺服器	否	單一評估任務中的伺服器數量上限

支援的 區域 AWS Transform

> **Note**
>
> 如果您提出的請求需要從此頁面未列出的選擇加入區域 AWS Transform 擷取資訊， AWS Transform 可以呼叫該區域。若要管理對 區域的存取 AWS Transform 可以呼叫 ，請參閱 AWS 轉換中的安全性。

本主題說明您可以使用 AWS 區域 的 AWS Transform。如需 的詳細資訊 AWS 區域，請參閱《 AWS 帳戶管理 參考指南》中的指定 AWS 區域 您的帳戶可以使用哪些 。

您的資料可能會在與您使用 的區域不同的區域中進行處理 AWS Transform。如需 中跨區域處理的資訊 AWS Transform，請參閱 跨區域處理。如需處理期間資料儲存位置的相關資訊，請參閱資料保護。

Supported AWS 區域 （ 預設為啟用 ）

您可以在下列內容中建立 AWS Transform 工作區 AWS 區域。這些區域預設為啟用 - 您不需要在使用前啟用它們。如需詳細資訊，請參閱預設啟用的區域。

- 美國東部 (維吉尼亞北部)
- 歐洲 (法蘭克福)
- 亞太地區 (孟買)
- 亞太地區 (雪梨)
- 亞太地區 (東京)
- 歐洲 (倫敦)
- 亞太地區 (首爾)
- 加拿大 (中部)
- 南美洲 （ 聖保羅 ） - 僅限大型主機現代化代理程式

您在其中建立任務的工作區會決定任務 AWS 區域 的 。若要在不同區域中建立任務，您必須使用所需區域中的不同工作區。

對於 VMware 專案，工作區的區域用於探索。不過，您可以指定不同的區域做為遷移目標。該目標區域是在遷移完成時託管工作負載的位置。如需 VMware 遷移 AWS 區域 考量事項的詳細資訊，包括可能的目標區域清單，請參閱 the section called “支援的目標區域”。

AWS 的 支援 AWS Transform

AWS Transform 如果您在轉換任務期間遇到問題， 可讓您透過聊天建立和管理 AWS 支援案例。您的案例會自動充實任務內容，並路由至適當的支援團隊。如果您是作用中的 Countdown Premium 客戶，您的指定工程師將與您聯絡以管理問題解決。在 AWS Countdown Premium 中進一步了解。否則，支援團隊會在其 AWS Transform 支援佇列中調查您的案例。

先決條件

在使用支援案例管理之前，您需要：

- 作用中的 AWS 支援計劃 - Business、Enterprise On-Ramp 或 Enterprise
- 現有的 AWS Transform 應用程式

啟用支援案例管理

1. 開啟 AWS Transform 主控台。
2. 在導覽窗格中，選擇設定。
3. 在支援下，選擇啟用支援案例管理。
4. 選擇儲存變更。

AWS Transform 使用服務連結角色 (SLR) 代表您建立和管理支援案例。不需要額外的 IAM 許可。

建立支援案例

若要建立支援案例，請使用聊天介面：

1. 要求 建立支援案例。例如：
    - 「為失敗的轉換任務建立支援案例」
    - 「我需要任務錯誤、建立案例的說明」
2. 聊天會提示您提供必要資訊：
    - 您問題的簡短描述

- 詳細說明

3. 出現提示時確認案例建立。

案例會自動填入轉換任務的內容，包括：

- 任務 ID 和狀態
- 任務中繼資料
- 任務執行日誌（任務日誌）
- 任務計畫

案例會根據您的任務類型和問題類別自動指派。

檢視支援案例

若要檢視您的支援案例，請提示聊天：

- 「列出我的支援案例」
- 「顯示開啟的支援案例」
- 「我的案例的狀態為何？」

聊天將顯示：

- 案例 ID
- 主旨
- 狀態，例如開啟、待定、已解決或已關閉
- 上次更新日期
- 關聯的任務 ID

若要檢視特定案例的詳細資訊：

- 「顯示案例 【case-id】 的詳細資訊」
- 「案例 【case-id】 的最新更新是什麼？」

將通訊新增至案例

若要將訊息新增至現有案例：

1. 詢問聊天：「新增訊息至案例 【case-id】」
2. 出現提示時提供您的訊息。
3. 聊天將確認訊息已新增。

當 AWS Support 回應您的案例時，您會收到通知。

解決案例

若要解決支援案例：

1. 詢問聊天：「解決案例 【case-id】」
2. 出現提示時確認解析度。

> **Note**
>
> 您只能解決 AWS Support 已解決的案例。

停用支援案例管理

1. 開啟 AWS Transform 主控台。
2. 在導覽窗格中，選擇設定。
3. 在支援下，選擇停用支援案例管理。
4. 選擇儲存變更。

> **Note**
>
> 停用支援案例管理會移除以聊天為基礎的案例管理界面，但不會關閉現有的案例。您仍然可以透過 AWS 支援中心存取您的案例。

用量遙測

根據預設， AWS 轉換 IDE 外掛程式、 AWS 轉換代理程式技能和 AWS 轉換 Kiro Power 在轉換執行期間收集用量遙測。遙測由不同的資料點組成，例如 IDE 名稱 （例如 VS Code 或 Kiro)、AI 代理器名稱 （例如 Claude Code 或 OpenAI Codex) 和執行模式 （本機或遠端）。 AWS Transform 使用此資料來排定相容性測試的優先順序，以及延遲和可靠性。

若要停用遙測，請在聊天工作階段期間告知客服人員您不想發出遙測。此選擇退出僅適用於目前的聊天工作階段，而且必須針對每個新工作階段重複執行。如果您直接執行 AWS 轉換 CLI，請設定`ATX_DISABLE_TELEMETRY=true`環境變數。

操作資料

我們可能會根據您自然語言的意見回饋（例如您是否核准繼續進行轉換計畫，或提供在提議的計畫上迭代的指示），收集有關您使用 AWS 轉換的操作訊號，例如您使用的功能、錯誤日誌和指標，以提供服務和評估服務效能。

變更日誌

下表說明 AWS 轉換的顯著版本和更新。

日期	Title	說明	連結
2026-08-16	AWS 遷移轉換新增過時的安全群組規則移除	AWS 遷移的轉換現在可識別從內部部署環境遷移的未使用傳入防火牆規則，並建議將其移除作為引導式網路建議的一部分。這可協助您避免轉發不再提供目的的安全暴露，例如開放傳入存取。移除僅限於未使用的輸入規則，其中沒有觀察到的流量是規則未使用的可靠訊號。	文件
2026-07-29	AWS VMware 以外的遷移轉換 VMware	AWS 遷移的轉換現在支援從幾乎任何來源遷移虛擬和裸機伺服器環境，包括 VMware、Hyper-V 和其他平台。無論您的來源基礎設施為何，都可以使用遷移功能：探索、遷移規劃、建立登陸區域、網路遷移和伺服器重新託管。Web 應用程式工作流程已從 'VMware Migrations'	文件

日期	Title	說明	連結
		重新命名為 'Migrations （包括 VMware)'。	
2026-07-29	AWS 遷移的轉換新增了啟動後動作的支援	AWS 遷移的轉換現在支援啟動後動作，可在做為測試或切換執行個體啟動後，自動在每個伺服器上進行現代化和驗證任務。代理程式會使用 代表您建議、設定和執行動作 AWS Systems Manager。動作可以預先定義或自訂，在帳戶層級定義，或為每個伺服器自訂。	文件

日期	Title	說明	連結
2026-07-03	AWS 轉換探索工具新增 Oracle 資料庫支援	AWS 轉換探索工具現在會直接從 VMware、Hyper-V 和裸機伺服器的資料庫收集詳細的 Oracle 中繼資料。您可以透過直接 SQL 連線探索 Oracle 執行個體。此工具會收集容器資料庫/可插入資料庫 (CDB/PDB) 列舉、元件庫存和資料檔案大小。它也會擷取 Real Application Cluster (RAC)、Data Guard 和多租戶架構的拓撲旗標。如果您尚未設定資料庫登入資料，工具會回到作業系統層級偵測。支援所有 Oracle 版本。	Oracle 資料庫探索
2026-06-22	南美洲（聖保羅）區域支援大型主機現代化代理程式	AWS 大型主機現代化代理程式的轉換現在可在南美洲（聖保羅）區域 (sa-east-1) 使用。已將 sa-east-1 新增至支援的區域和跨區域推論資料表。	支援的區域、跨區域推論

日期	Title	說明	連結
2026-06-22	AWS 遷移的轉換支援當地語系化	AWS 遷移的轉換現在支援當地語系化。您可以在使用 VMware 遷移工作流程時，選擇設定圖示並選擇您偏好的語言，以變更 Web 應用程式的顯示語言。	當地語系化設定
2026-06-18	AWS 遷移的轉換支援所有 AWS 商業區域做為遷移目標	AWS 遷移的轉換支援所有 AWS 商業區域做為遷移目標，中東（巴林）和中東（阿拉伯聯合大公國）除外。遷移目標區域是部署遷移資源 AWS 的區域，包括登陸區域、網路基礎設施和伺服器重新託管。	支援的遷移目標區域
2026-06-18	AWS 遷移轉換可讓您將現有的 ENIs 連接至啟動範本	AWS 轉換可讓您將現有的彈性網路界面 (ENIs) 連接至您的啟動範本以進行遷移。AWS 轉換會顯示目標帳戶中找到的所有現有 ENIs，而且您可以標記它們，以便在執行個體啟動時透過啟動組態使用。	遷移的 ENI 資源標記

日期	Title	說明	連結
2026-06-18	AWS 遷移轉換可讓您設定複寫和啟動設定	AWS 轉換可讓您為遷移設定複寫設定和啟動設定。您可以根據目標帳戶或跨特定來源伺服器設定組態。	複寫和啟動設定

日期	Title	說明	連結
2026-06-17	生成式 AI 工作負載的 Model-to-model遷移評估	AWS 轉換現在提供 model-to-model遷移自訂轉換。此轉換會評估您的生成式 AI 工作負載。它會產生從第三方供應商遷移到 Amazon Bedrock 的遷移計劃。AI 代理程式會掃描您的程式碼庫，以識別每個使用中的 AI 開發套件和模型。代理程式會透過互動式問題收集遷移需求。然後，它透過透明的成本比較和生產就緒的程式碼變更，將模型映射到 Amazon Bedrock 對等項目。支援透過 LiteLLM 或 Ollama 從 OpenAI、Google Gemini、直接 Anthropic SDK 用量和開放原始碼模型遷移。處理直接 SDK 整合和架構包裝模式，包括 LangChain、LlamaIndex、CrewAI 、LangGraph 和多供應商路由層。除了標準 AWS 轉換定價之外，可免費使用。	最新消息、自訂轉換

日期	Title	說明	連結
2026-06-16	AWS 大型主機的轉換提供可追蹤的重新構想工作流程	AWS 大型主機的轉換現在提供連線、可追蹤的重新構想體驗，從評估到程式碼產生。執行 z/OS COBOL 和 PL/I 工作負載的企業可以評估其產品組合，以識別離散的業務職能、擷取業務規則、產生可開發的需求，並在單一連線工作流程中產生可追蹤的雲端原生程式碼。每個需求都會追蹤回原始程式碼，以獲得完整的可稽核性。	最新消息、文件
2026-06-16	AWS 轉換現在支援 Amazon FSx for NetApp ONTAP 作為目標儲存體（公開預覽版）	除了 Amazon EBS 之外，您現在可以將區塊儲存工作負載遷移至 Amazon FSx for NetApp ONTAP，作為運算重新託管的一部分。 AWS Transform 會在處理運算和網路的相同遷移波動內，將區塊儲存資料直接複寫至 FSx for ONTAP 磁碟區。	最新消息、文件

日期	Title	說明	連結
2026-06-05	Amazon RDS for SQL Server TCO 評估支援	您現在可以在將內部部署 SQL Server 資料庫遷移至 Amazon RDS for SQL Server 時預估成本。使用 AWS Transform 中採用 AI 技術的 TCO 評估來分析您的環境，並取得最佳的資料庫執行個體建議。評估支援使用資料庫Savings Plans使用自有媒體 (BYOM) 和已包含授權 (LI) 選項，最多可節省 20%。	最新消息、文件
2026-06-04	AWS 轉換探索工具現在支援做為網路遷移輸入來源	您現在可以使用 AWS Transform 探索工具作為網路遷移的來源，並搭配 modelizeIT，為同時執行 VMware 和非 VMware 工作負載的環境啟用混合網路遷移。	使用者指南
2026-05-27	AWS 轉換自訂文件新增用戶端技能範例和最佳實務	用戶端技能文件現在包含 Dockerfile 合規、資料庫遷移安全、Terraform 政策強制執行和 API 棄用協助程式的實際範例，以及建置和共用技能的最佳實務。	文件

日期	Title	說明	連結
2026-05-22	新的代理遷移評估功能現在可搭配 AWS Transform 使用	AWS 轉換現在提供進階遷移評估功能，包括假設案例、可自訂假設、靈活的檔案格式支援，以及多個新的總體擁有成本 (TCO) 評估功能。	最新消息、文件
2026-05-20	AWS 轉換會在網路遷移檢閱期間偵測現有的 VPCs	AWS 轉換現在會在網路遷移檢閱期間偵測目標帳戶中VPCs。您可以在映射VPCs 旁查看現有的 VPCs、識別 CIDR 衝突，並在部署之前解決它們。	文件
2026-05-14	AWS 轉換代理程式現在可在 Kiro、Claude、Cursor 和 Codex 中使用	AWS 轉換代理程式現在可以透過 Kiro 電源、代理程式外掛程式和 AWS 轉換 MCP 伺服器存取，讓開發人員直接從他們偏好的開發環境使用轉換功能。	最新消息
2026-05-14	AWS Transform 推出用於建置自訂轉換代理程式的代理程式建置器工具組	合作夥伴和客戶現在可以使用代理程式建置器工具組 Kiro Power 來建置、共用和註冊專用轉換代理程式，並將自訂工具和工作流程與 AWS Transform 整合。	最新消息

日期	Title	說明	連結
2026-05-14	AWS Transform 將代理式 AI 助理新增至 AWS Toolkit for Visual Studio	.NET 開發人員現在可以直接在 Visual Studio 中透過對話 step-by-step引導體驗來現代化應用程式，並在 IDE 和 Web 主控台中保留完整內容。	最新消息
2026-05-14	AWS 轉換現在支援客戶擁有的成品存放區	您可以設定自己的 Amazon S3 儲存貯體，並選擇性地使用自己的 AWS KMS 金鑰加密成品，以完全控制轉換成品的存放位置。	最新消息、使用者指南
2026-05-14	AWS 轉換新增遷移策略 (7R) 建議	透過 AWS 轉換，您現在可以分析探索到的庫存，並取得每個伺服器和應用程式的遷移策略建議。建議遵循業界標準的七種遷移策略 (7R)。每個建議都包含建議 AWS 的目標服務、可信度分數，以及背後的推理。您可以產生互動式 HTML 儀表板、PDF 或 Microsoft PowerPoint 輸出。	7Rs 建議

日期	Title	說明	連結
2026-05-11	AWS 轉換會在遷移期間新增容器化功能	AWS 轉換現在支援在遷移期間將應用程式轉換至容器、自動化 Dockerfile 產生、使用 CVE 掃描建置容器映像，以及部署至 Amazon ECS 或 Amazon EKS。	最新消息、使用者指南
2026-05-01	AWS Transform 現在為 Power BI 和 Tableau 提供快速的 BI 遷移代理程式	Wavicle Data Solutions 的合作夥伴建置代理程式會將 Power BI 和 Tableau 儀表板轉換為 AWS 轉換工作流程中的快速資產。	最新消息
2026-04-21	AWS 轉換自訂現在可在六個其他 AWS 區域中使用	AWS 轉換自訂擴展到亞太區域、加拿大和歐洲（倫敦），總共達到八個 AWS 區域。	最新消息
2026-04-15	AWS 轉換會在遷移工作流程中新增登陸區域建立	直接在遷移工作流程中新增了登陸區域建立。 AWS 轉換現有基礎的檢查、建議組織單位 (OU) 結構和目標帳戶，並提供全自動化部署或基礎設施即程式碼 (IaC) 輸出 (CloudFormation、AWS CDK 或登陸區域加速器 (LZA) 格式）。	最新消息、文件

日期	Title	說明	連結
2026-04-15	AWS 轉換新增遷移規劃圖表和報告	您現在可以在遷移規劃期間產生互動式圖表和分析報告。圖表類型包括網路拓撲貼圖、應用程式相依性圖表、波浪 Gantt 圖表和一般圖表。報告類型包括風險評估、7Rs 建議和自訂分析報告。輸出提供互動式 HTML、PDF 或 Microsoft PowerPoint (.pptx) 檔案。	圖表和報告
2026-04-14	AWS 轉換現在可在 Kiro 和 VS 程式碼中使用	AWS 轉換自訂轉換現在可從 Kiro 和 VS Code 存取，並在 IDE、CLI 和 Web 主控台表面共用任務狀態。	最新消息
2026-04-10	AWS 轉換為網路遷移新增具有安全群組映射的 DHCP	在網路遷移期間新增對具有安全群組映射的 DHCP 的支援。如果您有啟用 DHCP 的遷移工作負載，您現在可以確保您的安全規則在遷移後保持有效。這適用於透過 Transit Gateway 參考的 VPC 內安全群組，以及跨 VPC 和跨帳戶傳出規則。	文件

日期	Title	說明	連結
2026-03-31	AWS 轉換自訂 宣布自動化程式碼庫分析的一般可用性	全方位的程式碼庫分析轉換可達到一般可用性、產生架構文件、技術債務報告，以及任何語言的現代化建議。	最新消息
2026-03-31	AWS 轉換自訂引入新的受管轉換，大規模現代化程式碼	新增七種新的受管轉換，包括 Node.js 升級（一般可用性）、Java 最佳化、Log4j 遷移、Angular-to-React、Angular 升級和 Vue 升級（早期存取）。	最新消息
2026-03-20	AWS 轉換會新增公有APIs以進行網路遷移	新增用於網路遷移的公APIs，讓合作夥伴和程式設計存取網路遷移功能。	API 參考
2026-01-14	AWS 轉換自訂 add AWS PrivateLink 支援並擴展至歐洲（法蘭克福）	AWS 轉換自訂現在支援透過 AWS PrivateLink 的私有 VPC 存取，除了美國東部（維吉尼亞北部）之外，也在歐洲（法蘭克福）提供。	最新消息

日期	Title	說明	連結
2025-12-23	AWS 轉換可讓混合式資料中心遷移進行網路轉換	AWS 適用於 VMware 的轉換會自動將混合資料中心網路組態 (VLANs、IP 範圍） 轉換為 AWS VPCs、子網路和安全群組，無需手動映射。	最新消息
2025-12-01	AWS 啟動 AWS 轉換自訂以加速整個組織的現代化	AWS 轉換自訂達到一般可用性，讓組織能夠透過單一 CLI 命令大規模自動化可重複的程式碼轉換。	最新消息
2025-12-01	AWS Transform 為企業 VMware 遷移新增了代理程式 AI 功能	AWS Transform 的 VMware 代理程式現在可探索內部部署環境、映射相依性、產生遷移波動計畫，以及跨 HyperV、Nutanix、KVM 和裸機目標遷移。	最新消息
2025-12-01	AWS 轉換會啟動 AI 代理器以進行全堆疊 Windows 現代化	新的完整堆疊 Windows 代理程式會自動將 .NET 應用程式和 SQL Server 資料庫轉換為 Aurora PostgreSQL，並部署到 Amazon ECS 或 EC2 Linux 上的容器。	最新消息

日期	Title	說明	連結
2025-12-01	AWS 轉換可擴展 .NET 轉換功能，並增強開發人員體驗	AWS Transform 新增了 .NET 10 支援、ASP.NET Web Forms 到 Blazor 移植，以及透過 AWS Toolkit for Visual Studio 增強的互動式 IDE 體驗。	最新消息
2025-12-01	AWS 大型主機的轉換提供新的測試自動化功能	AWS 大型主機的轉換引入自動化測試計畫產生、測試資料收集指令碼和測試案例自動化，以加速大型主機現代化測試。	最新消息
2025-12-01	AWS 大型主機的轉換現在支援應用程式重新構想	新的資料和活動分析加上商業邏輯擷取功能，可將舊版大型主機應用程式分解為雲端原生架構。	最新消息
2025-11-13	AWS Transform 自動化登陸區域加速器網路組態	AWS 遷移的轉換會自動產生與 LZA 相容的網路 YAML 檔案，簡化 VMware 環境的多帳戶雲端基礎設施設定。	最新消息

日期	Title	說明	連結
2025-07-16	AWS 大型主機的轉換引進增強型程式碼重構和商業邏輯功能	AWS 大型主機的轉換新增了重新建構（程式碼重組）的一般可用性，並擴展了應用程式層級的商業邏輯擷取，以改善程式碼品質。	最新消息
2025-05-15	AWS VMware 的 轉換現已正式推出	AWS Transform for VMware 是一種代理式 AI 服務，可自動化從探索到部署的完整 VMware 現代化生命週期，達到一般可用性。	最新消息
2025-05-15	AWS 大型主機的轉換現已正式推出	AWS 大型主機的轉換是第一個大規模現代化 IBM z/OS 應用程式的代理式 AI 服務，可透過新的分析、分解和任務管理功能達到一般可用性。	最新消息

下載此資料。

AWS 轉換使用者指南的文件歷史記錄

下表說明 AWS 轉換使用者指南的文件歷史記錄。

變更	描述	日期
網路遷移新增過時的安全群組規則移除	引導式網路建議現在可以識別從內部部署環境遷移的未使用傳入防火牆規則，並建議將其移除。請參閱引導式網路建議。	2026 年 8 月 16 日
連接器主題已移至入門	連接器主題已從頂層導覽移至入門區段。請參閱 連接器。	2026 年 8 月 8 日
持續現代化新增 AWS 轉換受管遠端執行	持續現代化現在可以使用 ，在 AWS 轉換受管基礎設施上執行分析，無需在帳戶中佈建任何內容`atx ct remote analysis --mode aws-managed` 。您也可以排程在沒有 Amazon EventBridge 的 AWS 轉換受管基礎設施上執行的週期性分析。請參閱運算選項。	2026 年 8 月 7 日
持續現代化新增遠端執行、排程和標記	持續現代化現在包括在 Amazon EC2 或 AWS Batch 上佈建和執行分析和修復的`atx ct remote`命令、使用 Amazon EventBridge Scheduler 執行週期性分析的`atx ct schedule`命令，以及屬性型存取控制 (ABAC) 的資源標記。新的 AWS 受管政策支援最低權限的遠端和安全代理程式執行。`atx ct`	2026 年 7 月 28 日

	`server` 命令已棄用。請參閱使用持續現代化。	
持續現代化產品組合分析和修復	新增章節，記錄自動化程式碼分析和修復的 AWS 轉換持續現代化功能 (`atx ct` 子命令）。請參閱持續現代化。	2026 年 6 月 3 日
布朗菲爾德網路：現有的 VPCs可見性	在網路遷移檢閱期間新增了現有的 VPC 偵測。 AWS Transform 會自動偵測VPCs，並標記 CIDR 與映射 VPCs衝突。請參閱目標帳戶中VPCs。	2026 年 5 月 18 日
新增 AWS 轉換自訂的技能格式、用戶端技能和子代理程式日誌	轉換定義現在使用技能格式 (`SKILL.md` 搭配 YAML 前端和選用`references/` 資料夾）。新增了用戶端技能，以使用其他功能擴展代理程式，以及子代理程式日誌來改善偵錯。需要 CLI 2.0 版或更新版本。請參閱轉換定義和用戶端技能。	2026 年 5 月 11 日
新增來源碼容器化	AWS 轉換現在可以使用生成式 AI 將應用程式容器化。從 Git 儲存庫或 zip 上傳提供您的原始程式碼，而 AWS Transform 會對其進行分析、產生 Docker 成品、將容器映像發佈至 Amazon ECR、產生基礎設施做為程式碼，以及部署至 Amazon Elastic Container Service 或 Amazon Elastic Kubernetes Service。請參閱原始程式碼容器化。	2026 年 5 月 7 日

新增網路最佳化操作和引導建議	新增了步驟 5：檢閱和最佳化網路，其中包含 VPC 和子網路操作（刪除、排除、合併、分割、調整大小、重新命名、變更 IP 地址），以及命名標準化、範圍檢閱、容量正確調整大小、安全性檢閱和 VPC 整合的引導建議。請參閱檢閱和最佳化網路。	2026 年 4 月 27 日
AWS 轉換 6 個新區域中可用的自訂	在AWS 轉換自訂中新增對 ca-central-1、eu-west-2、ap-northeast-1、ap-northeast-2、ap-southeast-2 和 ap-south-1 的支援。	2026 年 4 月 21 日
已更新連接器許可文件	新增目標 AWS 帳戶 連接器的詳細許可明細，涵蓋 S3、GN、Migration Hub 許可、工作負載遷移和登陸區域基礎設施佈建。請參閱連線目標 AWS 帳戶。	2026 年 4 月 19 日
已更新 VMware 遷移任務類型	新增探索和遷移規劃、登陸區域和登陸區域、網路和伺服器遷移任務類型。已將網路遷移重新命名為僅網路遷移和遷移規劃，以建置遷移計劃。請參閱 VMware 遷移任務類型。	2026 年 4 月 19 日
Restructured Connect AWS 帳戶目標	將連接器設定重組為三個步驟：遷移類型選擇、MAP 協議和連接器組態，包括支援的目標區域、帳戶角色、委派管理員指導和 IAM 角色。請參閱連線目標 AWS 帳戶。	2026 年 4 月 19 日

新增其他server-migration-only的目標區域	記錄了 14 個額外的商業區域，可用於沒有網路遷移的伺服器遷移任務，並要求允許清單，直到 2026 年第 Q3。請參閱支援的目標區域。	2026 年 4 月 19 日
新增遷移伺服器章節	新增遷移伺服器章節，涵蓋完整的重新託管工作流程，包括帳戶結構、IAM 角色、委派管理員設定、複寫代理程式部署、測試和切換。	2026 年 4 月 19 日
新增建置登陸區域章節	新增了組建登陸區域章節，其中包含登陸區域佈建的連接器許可詳細資訊。	2026 年 4 月 19 日
安全群組映射和參考	新增安全群組映射策略 (MAP、MAP_DHCP、SKIP) 和參考文件以遷移網路的安全群組。	2026 年 4 月 13 日
不支援的網路檔案類型自動轉換	新增支援在遷移網路中自動轉換不支援的網路組態檔案類型。	2026 年 4 月 6 日
新增資料庫遷移的 KMS 金鑰政策	已新增資料庫遷移的加密區段。	2026 年 3 月 26 日
記錄的新 AWS 受管政策	新增 DBModProvisioningAndMigration 區段。	2026 年 3 月 24 日
記錄的新 AWS 受管政策	新增 DBModDiscoveryAndAssessment 區段。	2026 年 3 月 24 日
產生網路圖表	新增選用的網路圖表產生 (Mermaid 和 PNG 格式） 以遷移網路。	2026 年 3 月 18 日

防火牆和 SDN 組態檔案支援	新增對遷移網路中網路遷移的 Palo Alto Networks、Fortinet FortiGate 和 Cisco ACI 組態檔案的支援。	2026 年 2 月 11 日
網路資源的自訂標記	新增遷移網路中網路遷移的任務層級和 VPC 層級自訂標記支援https://docs.aws.amazon.com/transform/latest/userguide/transform-vmware-migrate-network.html。	2026 年 1 月 28 日
新增支援文件	新增對 章節AWS 的支援。	2025 年 12 月 23 日
記錄新的 AWS 受管政策	新增 AWSTransformCustomFullAccess、AWSTransformCustomExecuteTransformations 和 AWSTransformCustomManageTransformations 區段。	2025 年 12 月 7 日
VMware 遷移	更新 VMware 遷移章節。	2025 年 12 月 1 日
更新 AWS 受管政策	更新 AWSServiceRoleForAWSTransform 文件以反映新增的許可。	2025 年 12 月 1 日
支援的區域	更新支援的區域主題。	2025 年 12 月 1 日
大型主機現代化	更新大型主機現代化章節。	2025 年 12 月 1 日
入門	已更新入門主題。	2025 年 12 月 1 日
全堆疊 Windows 現代化	新增了全堆疊 Windows 現代化主題，其中包含更新的 .NET 區段和新的 SQL Server 現代化區段。	2025 年 12 月 1 日
探索工具	新增探索工具區段。	2025 年 12 月 1 日

更新 AWS 受管政策	已更新 AWSTransformApplicationECSDeploymentPolicy，具有擴展的 IAM 角色檢查許可、建立 ECS 服務連結角色，以及支援 ECR 加密的 KMS 許可。	2025 年 11 月 22 日
更新 AWS 受管政策	使用額外的 EC2 網路、IAM 角色檢查、S3 儲存貯體管理和 KMS 加密許可更新 AWSTransformApplicationDeploymentPolicy。	2025 年 11 月 22 日
探索收集器	新增AWS 轉換探索工具> 文件。	2025 年 10 月 31 日
已新增 VMware 遷移架構圖	在遷移網路中新增 VMware 遷移架構圖。 https://docs.aws.amazon.com/transform/latest/userguide/transform-vmware-migrate-network.html	2025 年 10 月 23 日
VMware 遷移結果更新	已更新遷移結果資訊在遷移網路中。	2025 年 10 月 12 日
VMware 遷移結果更新	已更新遷移結果資訊在遷移網路中。	2025 年 10 月 12 日
S3 連接器文件	新增 .NET Web 應用程式的 S3 連接器文件。	2025 年 10 月 8 日
新使用者連接器主題	新增使用者連接器主題。	2025 年 9 月 21 日
更新 AWS 受管政策	已更新 AWSServiceRoleForAWSTransform 文件。	2025 年 9 月 17 日
儲存體評估支援	新增儲存體評估的 NetApp Data Infrastructure Insights (DII) 檔案支援。	2025 年 9 月 2 日

目標區域更新	新增三個支援的目標區域。	2025 年 8 月 31 日
受管政策更新	新增 AWSServiceRoleForAWSTransform 要使用的 IAM Identity Center 唯讀權限。	2025 年 8 月 29 日
記錄的新 AWS 受管政策	新增 AWSTransformApplicationDeploymentPolicy 區段。	2025 年 8 月 28 日
介面端點	新增界面端點主題。	2025 年 7 月 9 日
初始版本	AWS 轉換使用者指南的初始版本。	2025 年 5 月 15 日

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。