使用者指南

AWS 應用程式探索服務

AWS 應用程式探索服務: 使用者指南

Table of Contents

什麼是 AWS Application Discovery Service？

AWS Application Discovery Service 透過收集內部部署伺服器和資料庫的使用和組態資料，協助您規劃遷移至 AWS 雲端。Application Discovery Service 已與 AWS Migration Hub 和 AWS Database Migration Service Fleet Advisor 整合。Migration Hub 會將遷移狀態資訊彙總到單一主控台，簡化遷移追蹤。您可以檢視探索的伺服器，將它們分組到應用程式，然後從您主要區域的 Migration Hub 主控台追蹤每個應用程式的遷移狀態。您可以使用 DMS Fleet Advisor 來評估資料庫工作負載的遷移選項。

所有探索到的資料都存放在您的 AWS Migration Hub 主區域。因此，您必須先在 Migration Hub 主控台或使用 CLI 命令設定主區域，才能執行任何探索和遷移活動。您的資料可以在 Microsoft Excel 或 AWS 分析工具中匯出以供分析，例如 Amazon Athena 和 Amazon QuickSight。

使用 Application Discovery Service APIs，您可以匯出所發現伺服器的系統效能和使用率資料。將此資料輸入您的成本模型，以計算在其中執行這些伺服器的成本 AWS。此外，您可以匯出伺服器之間存在的網路連線相關資料。此資訊有助於您判斷網路伺服器之間的相依性，並將這些伺服器分組至應用程式以利遷移規劃。

> **Note**
>
> 開始探索程序 AWS Migration Hub 之前，您的主要區域必須設定在 中，因為您的資料將存放在您的主要區域。如需使用主要區域的詳細資訊，請參閱主要區域。

Application Discovery Service 提供三種方式來執行探索和收集內部部署伺服器的資料：

- 透過 VMware vCenter 部署 Application Discovery Service Agentless Collector (Agentless Collector) (OVA 檔案），即可執行無代理程式探索。設定 Agentless Collector 之後，它會識別虛擬機器 VMs) 和與 vCenter 相關聯的主機。Agentless Collector 會收集下列靜態組態資料：伺服器主機名稱、IP 地址、MAC 地址、磁碟資源配置、資料庫引擎版本和資料庫結構描述。此外，它會收集每個 VM 和資料庫的使用率資料，為 CPU、RAM 和磁碟 I/O 等指標提供平均和尖峰使用率。
- 代理程式型探索可以透過在每個 VMs 和實體伺服器上部署 AWS 應用程式探索代理程式 （探索代理程式） 來執行。代理程式安裝程式適用於 Windows 和 Linux 作業系統。它會收集靜態組態資料、詳細的時間序列系統效能資訊、傳入和傳出網路連線，以及執行中的處理程序。
- 檔案型匯入可讓您直接將內部部署環境的詳細資訊匯入 Migration Hub，而無需使用 Agentless Collector 或 Discovery Agent，因此您可以直接從匯入的資料執行遷移評估和規劃。擷取的資料取決於提供的資料。

Application Discovery Service 與 AWS Partner Network (APN) 合作夥伴的應用程式探索解決方案整合。這些第三方解決方案可協助您將內部部署環境的詳細資訊直接匯入 Migration Hub，而無需使用任何無代理程式收集器或探索代理程式。第三方應用程式探索工具可以查詢 AWS Application Discovery Service，而且可以使用公有 API 寫入 Application Discovery Service 資料庫。如此一來，您就可以將資料匯入 Migration Hub，並加以檢視，以便可將應用程式與伺服器建立關聯並追蹤遷移。

VMware Discovery

如果您的虛擬機器 (VMs) 在 VMware vCenter 環境中執行，您可以使用 Agentless Collector 收集系統資訊，而不必在每個 VM 上安裝代理程式。而是改為將此現場部署設備載入到 vCenter 並允許它探索所有主機和 VM。

Agentless Collector 會擷取在 vCenter 中執行之每個 VM 的系統效能資訊和資源使用率，無論使用何種作業系統。不過，它無法查看每個 VM 內部，因此，無法找出每個 VM 上執行哪些處理程序，以及存在哪些網路連線。因此，如果您需要此層級的詳細資訊，並想要仔細查看一些現有的 VMs，以協助規劃遷移，您可以視需要安裝 Discovery Agent。

此外，對於託管在 VMware 上的 VMs，您可以使用 Agentless Collector 和 Discovery Agent 同時執行探索。如需每個探索工具將收集的資料確切類型的詳細資訊，請參閱 使用 VMware vCenter Agentless Collector 資料收集模組。

資料庫探索

如果您的內部部署環境中有資料庫和分析伺服器，則可以使用 Agentless Collector 來探索和清查這些伺服器。然後，您可以收集每個資料庫伺服器的效能指標，而無需在環境中的每部電腦上安裝 Agentless Collector。

Agentless Collector 資料庫和分析資料收集模組會擷取中繼資料和效能指標，讓您深入了解資料基礎設施。資料庫和分析資料收集模組使用 Microsoft Active Directory 中的 LDAP 來收集您網路中作業系統、資料庫和分析伺服器的相關資訊。然後，資料收集模組會定期執行查詢，以收集資料庫和分析伺服器 CPU、記憶體和磁碟容量的實際使用率指標。如需收集指標的詳細資訊，請參閱 資料庫和分析模組收集的資料。

在 Agentless Collector 完成您環境的資料收集後，您可以使用 AWS DMS 主控台進行進一步分析和規劃遷移。例如，若要在 中選擇最佳遷移目標 AWS 雲端，您可以為來源資料庫產生目標建議。如需詳細資訊，請參閱使用資料庫和分析資料收集模組。

比較 Agentless Collector 和 Discovery Agent

下表提供 Application Discovery Service 支援的資料收集方法的快速比較。

	無代理程式收集器	探索代理程式	Migration Hub 範本	RVTools 匯出
Supported server types				
VMware 虛擬機器	是	是	Yes	Yes
實體伺服器	否	是	Yes	Yes
Deployment				
每個伺服器	否	是	N/A	No
每個 vCenter	是	否	N/A	Yes
相同網路上的每個資料中心	否	否	不適用	否
Collected data				
伺服器設定檔（靜態組態）資料	Yes	Yes	Yes	Yes
Hypervisor 的伺服器使用率指標 (CPU、RAM 等)	Yes	Yes	Yes	No
伺服器使用率指標來自伺服器 (CPU、RAM 等)	Yes	Yes	Yes	No

	無代理程式收集器	探索代理程式	Migration Hub 範本	RVTools 匯出
伺服器網路連線（僅限 TCP)	Yes	Yes	No	No
執行中的程序	No	Yes	No	No
收集間隔	-60 minutes	-15 seconds	Single snapshot	Single snapshot
Server data use cases				
在 Migration Hub 中檢視伺服器資料	Yes	Yes	Profile only	No
根據伺服器設定檔產生 Amazon EC2 建議	Yes	Yes	Yes	Yes
根據使用率資料產生 Amazon EC2 建議	Yes	Yes	Yes	No
匯出最新的使用率快照資料	Yes	Yes	Yes	No
匯出時間序列使用率資料	No	Yes	No	No
Network data use cases				
遷移中樞中的視覺化	Yes	Yes	No	No
匯出至 Amazon Athena 以進行進一步探索	No	Yes	No	No
匯出至 CSV 檔案	No	Yes	No	No

	無代理程式收集器	探索代理程式	Migration Hub 範本	RVTools 匯出
Database use cases				
資料庫伺服器設定檔（靜態組態）資料	Yes	No	No	No
支援的資料庫引擎	Oracle、SQL Server、MySQL、PostgreSQL	None	None	None
資料庫結構描述複雜性和重複項目	Yes	No	No	No
資料庫結構描述物件	Yes	No	No	No
Platform support				
支援的作業系統	在 VMware 中心 v5.5 或更新版本中執行的任何作業系統	任何 Linux 或 Windows 伺服器	任何 Linux 或 Windows 伺服器	任何 Linux 伺服器、Windows 伺服器或 VMware v5.5 或更新版本

前提

若要使用 Application Discovery Service，會假設下列項目：

- 您已註冊 AWS。如需詳細資訊，請參閱設定 Application Discovery Service。
- 您已選取 Migration Hub 主區域。如需詳細資訊，請參閱有關主要區域的文件。

以下是可以預期的情況：

- Migration Hub 主區域是唯一一個 Application Discovery Service 存放您探索和規劃資料的 區域。

- 探索代理程式、連接器和匯入只能用於您選取的 Migration Hub 主區域。
- 如需您可以使用 Application Discovery Service AWS 的區域清單，請參閱 Amazon Web Services 一般參考。

設定 Application Discovery Service

AWS Application Discovery Service 第一次使用 之前，請先完成下列任務：

- 註冊 Amazon Web Services
- 建立 IAM 使用者
- 登入 Migration Hub 主控台並選擇主要區域

註冊 Amazon Web Services

如果您沒有 AWS 帳戶，請完成下列步驟來建立一個。

註冊 AWS 帳戶

1. 開啟 https://portal.aws.amazon.com/billing/signup。
2. 請遵循線上指示進行。

   註冊程序的一部分包括接聽電話或文字訊息，以及在電話鍵盤上輸入驗證碼。

   當您註冊 時 AWS 帳戶，AWS 帳戶根使用者會建立 。根使用者有權存取該帳戶中的所有 AWS 服務 和資源。作為安全最佳實務，請將管理存取權指派給使用者，並且僅使用根使用者來執行需要根使用者存取權的任務。

建立 IAM 使用者

建立 AWS 帳戶時，您會取得單一登入身分，該身分可完整存取帳戶中的所有 AWS 服務和資源。此身分稱為 AWS 帳戶根使用者。 AWS Management Console 使用您用來建立帳戶的電子郵件地址和密碼登入 ，可讓您完整存取帳戶中的所有 AWS 資源。

強烈建議您不要以根使用者處理日常任務，即使是管理作業。相反地，請遵循安全最佳實務建立個別 IAM 使用者並建立 AWS Identity and Access Management (IAM) 管理員使用者。接著請妥善鎖定根使用者憑證，只用來執行少數的帳戶與服務管理任務。

除了建立管理使用者之外，您還需要建立非管理 IAM 使用者。下列主題說明如何建立這兩種類型的 IAM 使用者。

主題

建立 IAM 管理使用者

根據預設，管理員帳戶會繼承存取 Application Discovery Service 所需的所有政策。

建立管理員使用者

- 在 AWS 帳戶中建立管理員使用者。如需說明，請前往《IAM 使用者指南》中的建立第一個 IAM 使用者與管理員群組。

建立 IAM 非管理使用者

建立非管理 IAM 使用者時，請遵循安全最佳實務授予最低權限，授予使用者最低許可。

使用 IAM 受管政策來定義非管理 IAM 使用者對 Application Discovery Service 的存取層級。如需 Application Discovery Service 受管政策的相關資訊，請參閱 AWS 的 受管政策 AWS Application Discovery Service。

建立非管理員 IAM 使用者

1. 在 中 AWS Management Console，導覽至 IAM 主控台。
2. 依照《IAM 使用者指南》中的在 AWS 帳戶中建立 IAM 使用者所述，使用主控台建立使用者的指示來建立非管理員 IAM 使用者。

   遵循 IAM 使用者指南中的指示：

   - 在選取存取類型的步驟中，選取程式設計存取。請注意，雖然不建議，但只有在您計劃使用相同的 IAM 使用者登入資料來AWS 存取主控台時，才選取管理 AWS 主控台存取。
   - 在設定許可頁面的步驟中，選擇將現有政策直接連接至使用者的選項。然後從政策清單中選擇 Application Discovery Service 的受管 IAM 政策。如需 Application Discovery Service 受管政策的相關資訊，請參閱 AWS 的 受管政策 AWS Application Discovery Service。
   - 在檢視使用者存取金鑰 （ 存取金鑰 IDs和私密存取金鑰 ） 的步驟中，請遵循有關將使用者的新存取金鑰 ID 和私密存取金鑰儲存在安全的地方的重要注意事項中的指導。

登入 Migration Hub 主控台並選擇主要區域

您需要在用於 AWS 的帳戶中選擇 AWS Migration Hub 主區域 AWS Application Discovery Service。

選擇主要區域

1. 使用 AWS 您的帳戶登入 AWS Management Console ，並在 https：//https://console.aws.amazon.com/migrationhub/ 開啟 Migration Hub 主控台。
2. 在 Migration Hub 主控台導覽窗格中，選擇設定，然後選擇主要區域。

   您的 Migration Hub 資料會存放在您的主要區域，以用於探索、規劃和遷移追蹤。如需詳細資訊，請參閱 Migration Hub 主區域。

AWS 應用程式探索代理程式

AWS Application Discovery Agent (Discovery Agent) 是您安裝在內部部署伺服器和VMs上的軟體，目標為探索和遷移。代理程式會擷取系統組態、系統效能、執行程序，以及系統與系統之間網路連線的詳細資訊。代理程式支援大多數 Linux 和 Windows 作業系統，您可以在實體現場部署伺服器、Amazon EC2 執行個體和虛擬機器上部署這些作業系統。

> **Note**
>
> 部署 Discovery Agent 之前，您必須選擇 Migration Hub 主區域。您必須在主要區域中註冊您的代理程式。

Discovery Agent 會在您的本機環境中執行，且需要根權限。當您啟動 Discovery Agent 時，它會安全地與您的主區域連線，並向 Application Discovery Service 註冊。

- 例如，如果 `eu-central-1`是您的主區域，它會`arsenal-discovery.eu-central-1.amazonaws.com`向 Application Discovery Service 註冊。
- 或視需要將主區域替換為所有其他區域，但 us-west-2 除外。
- 如果 `us-west-2`是您的主要區域，則會`arsenal.us-west-2.amazonaws.com`向 Application Discovery Service 註冊。

運作方式

註冊後，代理程式會開始收集其所在主機或 VM 的資料。代理程式會每隔 15 分鐘 Ping Application Discovery Service 以取得組態資訊。

收集的資料包含系統規格、時間序列使用率或效能資料、網路連線及處理程序資料。您可以使用此資訊來對應您的 IT 資產及其網路相依性。所有這些資料點都可協助您判斷在 中執行這些伺服器的成本 AWS ，並規劃遷移。

Discovery Agents 會使用 Transport Layer Security (TLS) 加密，將資料安全地傳輸至 Application Discovery Service。代理程式設定為當有新版可用時即自動升級。您可視需要變更此組態設定。

> **Tip**
>
> 在下載並開始 Discovery Agent 安裝之前，請務必先閱讀 中所有必要的先決條件 Discovery Agent 的先決條件

Discovery Agent 收集的資料

AWS Application Discovery Agent (Discovery Agent) 是您在內部部署伺服器和 VMs 上安裝的軟體。Discovery Agent 會收集系統組態、序列使用率或效能資料的時間、程序資料和傳輸控制通訊協定 (TCP) 網路連線。本節說明收集的資料。

Discovery Agent 收集資料的資料表圖例：

- 「主機」一詞是指實體伺服器或 VM。
- 收集的資料是以千位元組 (KB) 為單位 (除非另有指明)。
- Migration Hub 主控台中的同等資料會以 MB (MB) 為單位報告。
- 輪詢期間間隔約 15 秒，每 15 分鐘會傳送至 AWS 。
- 以星號 (*) 表示的資料欄位僅適用於從代理程式的 API 匯出函數產生的 `.csv` 檔案。

資料欄位	描述
agentAssignedProcessId*	代理程式所探索處理程序的處理程序 ID
agentId	代理程式的唯一 ID
agentProvidedTimeStamp*	代理程式觀察的日期和時間 (mm/dd/yyyy hh:mm:ss am/pm)
cmdLine*	在命令列輸入的處理程序
cpuType	主機所用的 CPU (中央處理單元) 類型
destinationIp*	封包傳送目標的裝置 IP 地址
destinationPort*	資料/請求傳送目標的連接埠號碼
family*	路由系列的通訊協定

資料欄位	描述
freeRAM (MB)	可立即提供給應用程式使用的可用 RAM 和快取 RAM，以 MB 表示
gateway*	網路的節點地址
hostName	在其上收集資料的主機名稱
hypervisor	Hypervisor 的類型
ipAddress	主機的 IP 地址
ipVersion*	IP 版本編號
isSystem*	布林值屬性，指出處理程序是否屬於作業系統
macAddress	主機的 MAC 地址
name*	對其收集資料之主機、網路、指標等的名稱
netMask*	網路主機所屬的 IP 地址字首
osName	主機上的作業系統名稱
osVersion	主機上的作業系統版本
路徑	源自命令列的命令路徑
sourceIp*	傳送 IP 封包的裝置 IP 地址
sourcePort*	資料/請求來源的連接埠號碼
timestamp*	代理程式記錄回報屬性的日期和時間
totalCpuUsagePct	輪詢期間主機上的 CPU 使用量百分比
totalDiskBytesReadPerSecond (Kbps)	所有磁碟每秒讀取的總千位元數
totalDiskBytesWrittenPerSecond (Kbps)	所有磁碟每秒寫入的總千位元數
totalDiskFreeSize (GB)	可用磁碟空間，以 GB 表示

資料欄位	描述
totalDiskReadOpsPerSecond	每秒讀取 I/O 操作的總數
totalDiskSize (GB)	磁碟總容量，以 GB 表示
totalDiskWriteOpsPerSecond	每秒寫入 I/O 操作的總數
totalNetworkBytesReadPerSecond (Kbps)	每秒讀取位元組總輸送量
totalNetworkBytesWrittenPerSecond (Kbps)	每秒寫入位元組總輸送量
totalNumCores	CPU 中的獨立處理單元總數
totalNumCpus	中央處理單元總數
totalNumDisks	主機上的實體硬碟數量
totalNumLogicalProcessors*	實體核心總數乘以每個核心上可執行的執行緒數目
totalNumNetworkCards	伺服器上的網路卡總數
totalRAM (MB)	主機上可用的 RAM 總數
transportProtocol*	使用的傳輸通訊協定類型

Discovery Agent 的先決條件

以下是您必須先執行的先決條件和任務，才能成功安裝 AWS Application Discovery Agent (Discovery Agent)。

- 您必須先設定AWS Migration Hub 主區域，才能開始安裝 Discovery Agent。
- 如果您安裝了 1.x 版本的代理程式，必須移除後才能安裝最新的版本。
- 如果正在安裝代理程式的主機執行 Linux，請確認主機至少支援 Intel i686 CPU 架構 （ 也稱為 P6 micro 架構 ）。
- 確認支援您的作業系統 (OS) 環境：

  Linux

Amazon Linux 2012.03、2015.03

Amazon Linux 2 (9/25/2018 更新和以後)

Ubuntu 12.04、14.04、16.04、18.04、20.04

Red Hat Enterprise Linux 5.11、6.10、7.3、7.7、8.1

CentOS 5.11、6.9、7.3

SUSE 11 SP4、12 SP5、15 SP5

Windows

Windows Server 2003 R2 SP2

Windows Server 2008 R1 SP2、2008 R2 SP1

Windows Server 2012 R1、2012 R2

Windows Server 2016

Windows Server 2019

Windows Server 2022

- 如果您的網路限制對外連線，您需更新防火牆設定。代理程式需要透過 TCP 連接埠 443 存取 `arsenal`。它們不需要開啟任何傳入連接埠。

  例如，如果您的主區域是 `eu-central-1`，您將使用 `https://arsenal-discovery.eu-central-1.amazonaws.com:443`
- 需要存取您主區域的 Amazon S3，才能自動升級運作。
- 在主控台中建立 AWS Identity and Access Management (IAM) 使用者，並連接現有的 IAM `AWSApplicationDiscoveryAgentAccess` 受管政策。此政策可讓使用者代表您執行必要的代理程式動作。如需受管政策的詳細資訊，請參閱 AWS 的 受管政策 AWS Application Discovery Service。
- 檢查您的網路時間協定 (NTP) 伺服器時間偏移，並在有需要時予以更正。不正確的時間同步會造成代理程式註冊呼叫失敗。

> **Note**
>
> Discovery Agent 具有 32 位元代理程式可執行檔，可在 32 位元和 64 位元作業系統上執行。透過使用單一可執行檔能減少需部署的安裝套件數量。此可執行代理程式適用於 Linux 和 Windows 作業系統。並在以下各別安裝章節中說明。

安裝 Discovery Agent

此頁面說明如何在 Linux 和 Microsoft Windows 上安裝 Discovery Agent。

在 Linux 上安裝 Discovery Agent

在 Linux 上完成下列程序。開始此程序之前，請確定您的 Migration Hub 主區域已設定完成。

> **Note**
>
> 如果您使用的不是目前的 Linux 版本，請參閱舊版 Linux 平台的考量事項。

在資料中心安裝 AWS Application Discovery Agent

1. 登入 Linux 伺服器或 VM，並建立新的目錄以包含您的代理程式元件。
2. 切換到新的目錄並從命令列或主控台下載安裝指令碼。
   a. 若要從命令列下載，請執行以下命令。

      ```
      curl -o ./aws-discovery-agent.tar.gz https://s3-region.amazonaws.com/aws-discovery-agent.region/linux/latest/aws-discovery-agent.tar.gz
      ```

   b. 若要從 Migration Hub 主控台下載 ，請執行下列動作：
      i. 登入 AWS Management Console ，並在 https：//https://console.aws.amazon.com/migrationhub/ 開啟 Migration Hub 主控台。
      ii. 在左側導覽頁面的探索下，選擇工具。
      iii. 在AWS 探索代理程式方塊中，選擇下載代理程式，然後選擇下載 Linux。您的下載會立即開始。
3. 使用下列三個命令，驗證安裝套件的密碼編譯簽章：

   ```
   curl -o ./agent.sig https://s3.region.amazonaws.com/aws-discovery-agent.region/linux/latest/aws-discovery-agent.tar.gz.sig
   ```

   ```
   curl -o ./discovery.gpg https://s3.region.amazonaws.com/aws-discovery-agent.region/linux/latest/discovery.gpg
   ```

```
gpg --no-default-keyring --keyring ./discovery.gpg --verify agent.sig aws-discovery-agent.tar.gz
```

代理程式公開金鑰 (discovery.gpg) 指紋是 7638 F24C 6717 F97C 4F1B 3BC0 5133 255E 4DF4 2DA2。

4. 解壓縮 tarball，如下所示。

```
tar -xzf aws-discovery-agent.tar.gz
```

5. 若要安裝代理程式，請選擇下列其中一種安裝方法。

若要...	執行此作業...
安裝 Discovery Agent	若要安裝代理程式，請執行代理程式安裝命令，如下列範例所示。在此範例中，*your-home-region* 取代為您的主區域名稱、將 *aws-access-key-id* 取代為您的存取金鑰 ID，並將 *aws-secret-access-key* 取代為您的私密存取金鑰。 `sudo bash install -r your-home-region -k aws-access-key-id -s aws-secret-access-key` 根據預設，客服人員會在更新可供使用時自動下載和套用更新。 我們建議您使用此預設組態。 不過，如果您不希望客服人員自動下載和套用更新，請在執行客服人員安裝命令時包含 `-u false` 參數。
（選用）安裝 Discovery Agent 並設定不透明的代理	若要設定不透明代理，請將下列參數新增至代理程式安裝命令： • -e 代理密碼。

若要...	執行此作業...
	• -f 代理連接埠號碼。 • -g 代理結構描述。 • -i 代理使用者名稱。 以下是使用非透明代理參數的代理程式安裝命令範例。 `sudo bash install -r your-home-region -k aws-access-key-id -s aws-secret-access-key -d myproxy.mycompany.com -e mypassword -f proxy-port-number -g https -i myusername` 如果您的代理不需要身分驗證，請退出 -e和 -i 參數。 安裝命令範例使用 https，如果您的代理使用 HTTP，http請為 -g 參數值指定 。

6. 如果您的網路限制對外連線，您需更新防火牆設定。代理程式需要透過 TCP 連接埠 443 存取 arsenal。它們不需要開啟任何傳入連接埠。

   例如，如果您的主區域是 eu-central-1，您將使用 https://arsenal-discovery.*eu-central-1*.amazonaws.com:443

舊版 Linux 平台的考量事項

有些舊版的 Linux 平台，例如 SUSE 10、CentOS 5 和 RHEL 5，已終止服務，或僅提供基本支援。這些平台可能受到out-of-date的密碼套件的影響，導致代理程式更新指令碼無法下載安裝套件。

Curl

Application Discovery 代理程式需要 curl才能與 AWS 伺服器進行安全通訊。有些舊版的 curl 無法安全地與現代 Web 服務進行通訊。

若要使用 Application Discovery 代理程式內含的 `curl` 版本處理所有操作，請搭配 `-c true` 參數執行安裝指令碼。

憑證授權機構套件組合

舊版的 Linux 系統可能有過期的憑證授權機構 (CA) 套件組合，它對保護網際網路通訊安全非常重要。

若要使用 Application Discovery 代理程式內含的 CA 套件組合處理所有操作，請搭配 `-b true` 參數執行安裝指令碼。

這些安裝指令碼選項可以一起使用。在下列範例命令中，兩個指令碼參數都會傳遞至安裝指令碼：

```
sudo bash install -r your-home_region -k aws-access-key-id -s aws-secret-access-key -c
 true -b true
```

在 Microsoft Windows 上安裝 Discovery Agent

請完成下列程序，在 Microsoft Windows 上安裝 代理程式。在開始此程序之前，請確定您的 Migration Hub 主區域已設定。

在資料中心安裝 AWS Application Discovery Agent

1. 下載 Windows 代理程式安裝程式，但不要按兩下在 Windows 中執行安裝程式。

   > **Important**
   >
   > 請勿按兩下在 Windows 中執行安裝程式，因為它將無法安裝。代理程式安裝僅可從命令提示字元執行。(如果您已經連按兩下安裝程式，則必須移至新增/移除程式並解除安裝代理程式，然後再繼續進行其餘的安裝步驟。)
   > 如果 Windows 代理程式安裝程式在主機上未偵測到任何版本的 Visual C++ x86 執行期，則其會在安裝代理程式軟體之前自動安裝 Visual C++ x86 2015–2019 執行期。

2. 以管理員身分開啟命令提示字元，並導覽至您儲存安裝套件的位置。
3. 若要安裝代理程式，請選擇下列其中一種安裝方法。

若要...	執行此作業...
安裝 Discovery Agent	若要安裝代理程式，請執行代理程式安裝命令，如下列範例所示。在此範例中，將 取代*your-home-region* 為您主要區域的名稱、將 *aws-access-key-id* 取代為您的存取金鑰 ID，並將 *aws-secret-access-key* 取代為您的私密存取金鑰。 或者，您也可以指定 INSTALLLOCATION 參數*C:\install-location* 的資料夾路徑，以設定代理程式安裝位置。例如：INSTALLLOCATION=" *C:\install-location* "。產生的資料夾階層將為 【INSTALLLOCATION 路徑】\AWS Discovery。根據預設，安裝位置為 Program Files 資料夾。 或者，您可以使用 LOGANDCONFIGLOCATION 來覆寫代理程式日誌資料夾和組態檔案的預設目錄 (ProgramData)。產生的資料夾階層為 [*LOGANDCONFIGLOCATION path*]\AWS Discovery 。 `.\AWSDiscoveryAgentInstaller.exe REGION=" your-home-region " KEY_ID="aws-access-key-id " KEY_SECRET=" aws-secret-access-key " /quiet` 根據預設，客服人員會在更新可供使用時自動下載和套用更新。 我們建議您使用此預設組態。

若要...	執行此作業...
	不過，如果您不希望客服人員自動下載和套用更新，請在執行代理程式安裝命令時包含下列參數： `AUTO_UPDATE=false` **Warning** 停用自動升級可防止安裝最新的安全性修補程式。

若要...	執行此作業...
（選用）安裝 Discovery Agent 並設定不透明的代理	若要設定不透明代理，請將下列公有屬性新增至代理程式安裝命令： • PROXY_HOST – 代理主機的名稱 • PROXY_SCHEME – 代理結構描述 • PROXY_PORT – 代理連接埠號碼 • PROXY_USER – 代理使用者名稱 • PROXY_PASSWORD – 代理使用者密碼 以下是使用非透明代理屬性的代理程式安裝命令範例。 `.\AWSDiscoveryAgentInstaller.exe REGION=" your-home-region " KEY_ID="aws-access-key-id " KEY_SECRET=" aws-secret-access-key " PROXY_HOST=" myproxy.mycompany.com " PROXY_SCHEME="https" PROXY_PORT=" proxy-port-number " PROXY_USER=" myusername " PROXY_PASSWORD=" mypassword " /quiet` 如果您的代理不需要身分驗證，請省略 PROXY_USER 和 PROXY_PASSWORD 屬性。安裝命令範例使用 https。如果您的代理使用 HTTP，http請為 PROXY_SCHEME 值指定。

4. 如果來自您網路的傳出連線受到限制，您必須更新防火牆設定。代理程式需要透過 TCP 連接埠 443 存取 arsenal。它們不需要開啟任何傳入連接埠。

   例如，如果您的所在區域是 eu-central-1，您將使用下列項目： https://arsenal-discovery.*eu-central-1*.amazonaws.com:443

套件簽署和自動升級

對於 Windows Server 2008 和更新版本，Amazon 會以密碼編譯方式使用 SHA256 憑證簽署 Application Discovery Service 代理程式安裝套件。對於 Windows Server SHA2-signed的自動更新，請確保主機已安裝 Hotfix 以支援 SHA2 簽章身分驗證。 SP2 Microsoft 的最新支援 Hotfix 有助於在 Windows Server 2008 SP2 上支援 SHA2 身分驗證。 SP2

> **Note**
>
> Microsoft 不再公開提供 SHA256 支援 Windows 2003 的修正程式。如果這些修正尚未安裝在 Windows 2003 主機中，則需要手動升級。

手動執行升級

1. 下載 Windows Agent Updater。
2. 以管理員身分開啟命令提示。
3. 導覽至儲存更新程式的位置。
4. 執行下列命令。

```
AWSDiscoveryAgentUpdater.exe /Q
```

管理 Discovery Agent 程序

此頁面說明如何在 Linux 和 Microsoft Windows 上管理 Discovery Agent。

在 Linux 上管理 Discovery Agent 程序

您可以使用 `Upstart`、 或 `System V init`工具，在系統層級管理 Discovery Agent `systemd`的行為。以下標籤概述在每個個別的工具中支援任務的命令。

systemd

管理 Application Discovery 代理程式的命令

任務	Command
驗證代理程式是否執行中	`sudo systemctl status aws-discovery-daemon.service`
啟動代理程式	`sudo systemctl start aws-discovery-daemon.service`
停止代理程式	`sudo systemctl stop aws-discovery-daemon.service`
重新啟動代理程式	`sudo systemctl restart aws-discovery-daemon.service`

Upstart

Application Discovery Agent 的管理命令

任務	Command
驗證代理程式是否執行中	`sudo initctl status aws-discovery-daemon`
啟動代理程式	`sudo initctl start aws-discovery-daemon`
停止代理程式	`sudo initctl stop aws-discovery-daemon`
重新啟動代理程式	`sudo initctl restart aws-discovery-daemon`

System V init

Application Discovery Agent 的管理命令

任務	Command
驗證代理程式是否執行中	`sudo /etc/init.d/aws-discovery-daemon status`
啟動代理程式	`sudo /etc/init.d/aws-discovery-daemon start`
停止代理程式	`sudo /etc/init.d/aws-discovery-daemon stop`
重新啟動代理程式	`sudo /etc/init.d/aws-discovery-daemon restart`

在 Microsoft Windows 上管理 Discovery Agent 程序

您可以透過 Windows Server Manager Services 主控台，在系統層級管理 Discovery Agent 的行為。下表說明執行方法。

任務	服務名稱	服務狀態/動作
驗證代理程式是否執行中	AWS 探索代理程式 AWS 探索更新程式	已開始
啟動代理程式	AWS 探索代理程式 AWS 探索更新程式	選擇 Start (啟動)。
停止代理程式	AWS 探索代理程式 AWS 探索更新程式	選擇 Stop (停止)。
重新啟動代理程式	AWS 探索代理程式 AWS 探索更新程式	選擇 Restart (重新啟動)。

解除安裝 Discovery Agent

此頁面說明如何解除安裝 Linux 和 Microsoft Windows 上的 Discovery Agent。

在 Linux 上解除安裝 Discovery Agent

本節說明如何解除安裝 Linux 上的 Discovery Agent。

如果您使用的是 yum 套件管理員，請解除安裝 代理程式

- 如果使用 yum，請使用下列命令解除安裝代理程式。

```
rpm -e --nodeps aws-discovery-agent
```

如果您使用的是 apt-get 套件管理員，請解除安裝 代理程式

- 如果使用 apt-get，請使用下列命令解除安裝代理程式。

```
apt-get remove aws-discovery-agent:i386
```

如果您使用的是 zypper 套件管理員，請解除安裝代理程式

- 如果使用 zypper，請使用下列命令解除安裝代理程式。

```
zypper remove aws-discovery-agent
```

在 Microsoft Windows 上解除安裝 Discovery Agent

本節說明如何解除安裝 Microsoft Windows 上的 Discovery Agent。

若要解除安裝 Windows 上的探索代理程式

1. 在 Windows 中開啟控制面板。
2. 選擇程式集。
3. 選擇程式和功能。
4. 選取AWS 探索代理程式。

5. 選擇解除安裝。

> **Note**
>
> 如果您選擇在解除安裝代理程式之後重新安裝代理程式，請使用 /repair和 /norestart選項執行下列命令。
>
> ```
> .\AWSDiscoveryAgentInstaller.exe REGION="your-home-region" KEY_ID="aws-access-key-id" KEY_SECRET="aws-secret-access-key" /quiet /repair /norestart
> ```

使用命令列在 Windows 上解除安裝探索代理程式

1. 以滑鼠右鍵按一下開始。
2. 選擇命令提示字元。
3. 使用以下命令在 Windows 上解除安裝探索代理程式。

```
wmic product where name='AWS Discovery Agent' call uninstall
```

> **Note**
>
> 如果.exe檔案存在於伺服器上，您可以使用下列命令，從伺服器完全解除安裝代理程式。如果您使用此命令解除安裝 ，則重新安裝代理程式時不需要使用 /repair和 /norestart選項。
>
> ```
> .\AWSDiscoveryAgentInstaller.exe /quiet /uninstall
> ```

啟動和停止 Discovery Agent 資料收集

部署和設定 Discovery Agent 之後，如果資料收集停止，您可以重新啟動它。您可以透過 中的步驟，或透過 進行 API 呼叫在 AWS Migration Hub 主控台中啟動和停止資料收集器，透過 主控台啟動或停止資料收集 AWS CLI。

安裝 AWS CLI 並啟動或停止資料收集

1. 如果您尚未這麼做，請安裝 AWS CLI 適合您作業系統類型的 (Windows 或 Mac/Linux)。如需說明，請參閱 AWS Command Line Interface 使用者指南。
2. 開啟命令提示字元 (Windows) 或終端機 (MAC/Linux)。
   a. 輸入 `aws configure` 然後按 Enter 鍵。
   b. 輸入您的 AWS 存取金鑰 ID 和 AWS 私密存取金鑰。
   c. 輸入您預設區域名稱的主區域，例如 *us-west-2*。（在此範例中，我們假設 us-west-2是您的主要區域。）
   d. 輸入預設輸出格式的 `text`。
3. 若要尋找您要停止或啟動資料收集之代理程式的 ID，請輸入下列命令：

```
aws discovery describe-agents
```

4. 若要由代理程式開始資料收集，請輸入下列命令：

```
aws discovery start-data-collection-by-agent-ids --agent-ids <agent ID>
```

若要停止代理程式的資料收集，請輸入下列命令：

```
aws discovery stop-data-collection-by-agent-ids --agent-ids <agent ID>
```

探索代理程式疑難排解

此頁面涵蓋 Linux 和 Microsoft Windows 上的 Discovery Agent 故障診斷。

Linux 上的 Discovery Agent 故障診斷

如果您在 Linux 上安裝或使用 Discovery Agent 時遇到問題，請參閱下列有關記錄和組態的指引。協助疑難排解代理程式或其與 Application Discovery Service 連線的潛在問題時， AWS Support 通常會請求這些檔案。

- 日誌檔

  Discovery Agent 的日誌檔案位於下列目錄中。

```
/var/log/aws/discovery/
```

日誌檔案會命名為 ，以指出它們是由主要協助程式、自動升級程式或安裝程式產生。

- 組態檔案

  Discovery Agent 2.0.1617.0 版或更新版本的組態檔案位於下列目錄中。

  ```
  /etc/opt/aws/discovery/
  ```

  2.0.1617.0 之前的 Discovery Agent 版本組態檔案位於下列目錄中。

  ```
  /var/opt/aws/discovery/
  ```

- 如需如何移除舊版 Discovery Agent 的說明，請參閱 Discovery Agent 的先決條件。

對 Microsoft Windows 上的 Discovery Agent 進行故障診斷

如果您在 Microsoft Windows 上安裝或使用 AWS Application Discovery Agent 時遇到問題，請參閱下列有關記錄和組態的指導。 AWS 支援通常會在協助疑難排解代理程式或其與 Application Discovery Service 的連線時請求這些檔案。

- 安裝記錄

  在某些情況下，代理程式安裝命令似乎失敗。例如，當 Windows Services Manager 顯示探索服務尚未建立，便可能會發生失敗。在這種情況下，新增 /log install.log 至命令來產生詳細資訊安裝日誌。

- 營運記錄

  在 Windows Server 2008 和更新版本中，代理程式日誌檔位於下列目錄。

  ```
  C:\ProgramData\AWS\AWS Discovery\Logs
  ```

  在 Windows Server 2003 中，代理程式日誌檔位於下列目錄。

  ```
  C:\Documents and Settings\All Users\Application Data\AWS\AWS Discovery\Logs
  ```

日誌檔案會命名為 ，以指出是由主要服務、自動升級或安裝程式產生。

- 組態檔案

  在 Windows Server 2008 和更新版本中，代理程式組態檔案位於下列位置。

  ```
  C:\ProgramData\AWS\AWS Discovery\config
  ```

  在 Windows Server 2003 中，代理程式組態檔案位於下列位置。

  ```
  C:\Documents and Settings\All Users\Application Data\AWS\AWS Discovery\config
  ```

- 如需如何移除舊版 Discovery Agent 的說明，請參閱 Discovery Agent 的先決條件。

Application Discovery Service 無代理程式收集器

Application Discovery Service 無代理程式收集器 (Agentless Collector) 是一種內部部署應用程式，透過無代理程式方法來收集有關內部部署環境的資訊，包括伺服器設定檔資訊（例如，作業系統、CPUs 數量、RAM 數量）、資料庫中繼資料、使用率指標，以及內部部署伺服器之間網路流量的資料。您會使用開放式虛擬封存 (OVA) 檔案在您的 VMware vCenter Server 環境中安裝 Agentless Collector 做為虛擬機器 (VM)。

Agentless Collector 具有模組化架構，允許使用多個 Agentless 收集方法。Agentless Collector 提供從 VMware VMs 和分析伺服器收集資料的模組。它還提供一個模組，用於收集內部部署伺服器之間網路流量的資料。

Agentless Collector 透過收集內部部署伺服器和資料庫的使用和組態資料，以及內部部署伺服器之間的網路流量資料，來支援 AWS Application Discovery Service（應用程式探索服務）的資料收集。

Application Discovery Service 已與 整合 AWS Migration Hub，這項服務可在將您的遷移狀態資訊彙總到單一主控台時簡化遷移追蹤。您可以檢視探索到的伺服器、取得 Amazon EC2 建議、視覺化網路連線、將伺服器分組到應用程式中，然後從您主要區域的 Migration Hub 主控台追蹤每個應用程式的遷移狀態。

Agentless Collector 資料庫和分析資料收集模組已與 AWS Database Migration Service () 整合AWS DMS。此整合有助於規劃遷移至 AWS 雲端。您可以使用資料庫和分析資料收集模組來探索環境中的資料庫和分析伺服器，並建立您要遷移至 的伺服器庫存 AWS 雲端。此資料收集模組會收集 CPU、記憶體和磁碟容量的資料庫中繼資料和實際使用率指標。收集這些指標之後，您可以使用 AWS DMS 主控台來產生來源資料庫的目標建議。

Agentless Collector 的先決條件

以下是使用 Application Discovery Service Agentless Collector (Agentless Collector) 的先決條件：

- 一或多個 AWS 帳戶。
- 主 AWS Migration Hub 區域已設定的 AWS 帳戶，請參閱 登入 Migration Hub 主控台並選擇主要區域。您的 Migration Hub 資料會存放在您的主區域，以用於探索、規劃和遷移追蹤。
- 設定為使用 AWS 受管政策 AWS 的帳戶 IAM 使用者`AWSApplicationDiscoveryAgentlessCollectorAccess`。若要使用資料庫和分析資料收集模組，此 IAM 使用者也必須使用兩個客戶受管 IAM 政策和 `DMSCollectorPolicy` `FleetAdvisorS3Policy`。如需詳細資訊，請參閱部署 Application Discovery Service 無代理程式收集器。IAM 使用者必須在 Migration Hub 主區域中設定的 AWS 帳戶中建立。

- VMware vCenter Server V5.5、V6, V6.5、6.7 或 7.0。

> **Note**
>
> Agentless Collector 支援所有這些版本的 VMware，但我們目前針對 6.7 和 7.0 版進行測試。

- 對於 VMware vCenter Server 設定，請確定您可以為系統群組提供具有讀取和檢視許可設定的 vCenter 憑證。
- Agentless Collector 需要透過 TCP 連接埠 443 對多個 AWS 網域進行傳出存取。如需這些網域的清單，請參閱 設定防火牆以傳出存取 AWS 網域。
- 若要使用資料庫和分析資料收集模組，請在您設定為 Migration Hub 主區域的 中建立 AWS 區域 Amazon S3 儲存貯體。資料庫和分析資料收集模組會將庫存中繼資料存放在此 Amazon S3 儲存貯體中。如需詳細資訊，請參閱《Amazon S3 使用者指南》中的建立儲存貯體。
- Agentless Collector 第 2 版需要 ESXi 6.5 或更新版本。

設定防火牆以傳出存取 AWS 網域

如果來自您網路的傳出連線受到限制，您必須更新防火牆設定，以允許傳出存取 Agentless Collector 所需的 AWS 網域。哪些 AWS 網域需要傳出存取權取決於您的 Migration Hub 主區域是美國西部（奧勒岡）區域、us-west-2 或其他區域。

如果 AWS 您的帳戶主區域是 us-west-2，以下網域需要傳出存取權：

- `arsenal-discovery.us-west-2.amazonaws.com` – 收集器使用此網域來驗證其已設定所需的 IAM 使用者憑證。收集器也會使用它來傳送和儲存收集的資料，因為主要區域是 us-west-2。
- `migrationhub-config.us-west-2.amazonaws.com` – 收集器會使用此網域，根據提供的 IAM 使用者登入資料，判斷收集器將資料傳送至哪個主區域。
- `api.ecr-public.us-east-1.amazonaws.com` – 收集器會使用此網域來探索可用的更新。
- `public.ecr.aws` – 收集器使用此網域下載更新。
- dms.*`your-migrationhub-home-region`*.amazonaws.com – 收集器使用此網域連線至 AWS DMS 資料收集器。
- `s3.amazonaws.com` – 收集器會使用此網域，將資料庫和分析資料收集模組收集的資料上傳至您的 Amazon S3 儲存貯體。
- `sts.amazonaws.com` – 收集器使用此網域來了解收集器已設定的帳戶。

如果 AWS 您的帳戶所在區域不是 ，以下網域需要傳出存取權**us-west-2**：

- `arsenal-discovery.us-west-2.amazonaws.com` – 收集器使用此網域來驗證其已設定所需的 IAM 使用者憑證。
- `arsenal-discovery.`*`your-migrationhub-home-region`*`.amazonaws.com` – 收集器會使用此網域來傳送和儲存收集的資料。
- `migrationhub-config.us-west-2.amazonaws.com` – 收集器會使用此網域，根據提供的 IAM 使用者登入資料，判斷收集器應將資料傳送到哪個主區域。
- `api.ecr-public.us-east-1.amazonaws.com` – 收集器會使用此網域來探索可用的更新。
- `public.ecr.aws` – 收集器使用此網域下載更新。
- `dms.`*`your-migrationhub-home-region`*`.amazonaws.com` – 收集器使用此網域連線至 AWS DMS 資料收集器。
- `s3.amazonaws.com` – 收集器會使用此網域，將資料庫和分析資料收集模組收集的資料上傳至您的 Amazon S3 儲存貯體。
- `sts.amazonaws.com` – 收集器使用此網域來了解收集器已設定的帳戶。

設定 Agentless Collector 時，您可能會收到錯誤，例如設定失敗 – 請檢查您的登入資料，然後再試一次或AWS 無法連線。請確認網路設定。這些錯誤可能是因為 Agentless Collector 嘗試建立與其需要傳出存取的其中一個 AWS 網域的 HTTPS 連線失敗所造成。

如果 AWS 無法建立與 的連線，則 Agentless Collector 無法從您的內部部署環境收集資料。如需如何修正 連線的詳細資訊 AWS，請參閱 修正無代理程式收集器在設定 AWS 期間無法連線。

部署 Application Discovery Service 無代理程式收集器

若要部署 Application Discovery Service Agentless Collector，您必須先建立 IAM 使用者並下載收集器。此頁面會逐步引導您部署收集器所要採取的步驟。

為 Agentless Collector 建立 IAM 使用者

若要使用 Agentless Collector，登入 Migration Hub 主控台並選擇主要區域您必須在您在 中使用的 AWS 帳戶中建立 AWS Identity and Access Management (IAM) 使用者。然後，將此 IAM 使用者設定為使用以下 AWS 受管政策 AWSApplicationDiscoveryAgentlessCollectorAccess。您在建立 IAM 使用者時連接此 IAM 政策。

若要使用資料庫和分析資料收集模組，請建立兩個客戶受管 IAM 政策。這些政策可讓您存取 Amazon S3 儲存貯體 AWS DMS 和 API。如需詳細資訊，請參閱《IAM 使用者指南》中的建立客戶受管政策。

- 使用下列 JSON 程式碼來建立**DMSCollectorPolicy**政策。

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "dms:DescribeFleetAdvisorCollectors",
            "dms:ModifyFleetAdvisorCollectorStatuses",
            "dms:UploadFileMetadataList"
        ],
        "Resource": "*"
    }]
}
```

- 使用下列 JSON 程式碼來建立**FleetAdvisorS3Policy**政策。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject*",
                "s3:GetBucket*",
                "s3:List*",
                "s3:DeleteObject*",
                "s3:PutObject*"
            ],
            "Resource": [
                "arn:aws:s3:::bucket_name",
                "arn:aws:s3:::bucket_name/*"
            ]
        }
    ]
}
```

在上述範例中，將 *bucket_name*取代為您在先決條件步驟中建立的 Amazon S3 儲存貯體名稱。

我們建議您建立非管理 IAM 使用者以搭配 Agentless Collector 使用。建立非管理 IAM 使用者時，請遵循安全最佳實務授予最低權限，授予使用者最低許可。

建立非管理員 IAM 使用者以搭配 Agentless Collector 使用

1. 在 中 AWS Management Console，使用您用來在 中設定主區域的 AWS 帳戶，導覽至 IAM 主控台登入 Migration Hub 主控台並選擇主要區域。
2. 依照 IAM 使用者指南中在您的 AWS 帳戶中建立 IAM 使用者中所述，使用主控台建立使用者的指示來建立非管理員 IAM 使用者。

   遵循 IAM 使用者指南中的指示：

   - 在選取存取類型的步驟中，選取程式設計存取。請注意，雖然不建議，但只有在您計劃使用相同的 IAM 使用者登入資料來AWS 存取主控台時，才選取管理 AWS 主控台存取。
   - 在設定許可頁面的步驟中，選擇將現有政策直接連接至使用者的選項。然後從政策清單中選擇`AWSApplicationDiscoveryAgentlessCollectorAccess` AWS 受管政策。

     接著，選取 `DMSCollectorPolicy`和`FleetAdvisorS3Policy`客戶受管 IAM 政策。
   - 在檢視使用者存取金鑰 （ 存取金鑰 IDs和私密存取金鑰 ） 的步驟中，請遵循有關將使用者的新存取金鑰 ID 和私密存取金鑰儲存在安全的地方的重要注意事項中的指導。您將需要在 中使用這些存取金鑰設定無代理程式收集器。

     這是輪換存取金鑰 AWS 的安全最佳實務。如需輪換金鑰的資訊，請參閱《IAM 使用者指南》中的針對需要長期憑證的使用案例定期輪換存取金鑰。

下載 Agentless Collector

若要設定 Application Discovery Service Agentless Collector (Agentless Collector)，您必須下載並部署 Agentless Collector Open Virtualization Archive (OVA) 檔案。Agentless Collector 是您安裝在內部部署 VMware 環境中的虛擬設備。此步驟說明如何下載收集器 OVA 檔案，下一個步驟則說明如何部署該檔案。

下載收集器 OVA 檔案並驗證其檢查總和

1. 以 VMware 管理員身分登入 vCenter，並切換至您要下載 Agentless Collector OVA 檔案的目錄。
2. 從下列 URL 下載 OVA 檔案：

   無代理程式收集器 OVA

3. 根據您的系統環境中使用的雜湊演算法，下載 MD5 或 SHA256 以取得包含檢查總和值的檔案。使用下載的值來驗證在上述步驟中下載ApplicationDiscoveryServiceAgentlessCollector的檔案。
4. 根據您的 Linux 變化，執行版本適當的 MD5 命令或 SHA256 命令，來驗證 ApplicationDiscoveryServiceAgentlessCollector.ova 檔案的加密簽章是否與您下載的各自 MD5/SHA256 檔案中的值相符。

```
$ md5sum ApplicationDiscoveryServiceAgentlessCollector.ova
```

```
$ sha256sum ApplicationDiscoveryServiceAgentlessCollector.ova
```

部署 Agentless Collector

Application Discovery Service Agentless Collector (Agentless Collector) 是您在內部部署 VMware 環境中安裝的虛擬設備。本節說明如何部署您在 VMware 環境中下載的 Open Virtualization Archive (OVA) 檔案。

Agentless Collector 虛擬機器規格

Agentless Collector version 2

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

Agentless Collector version 1

- 作業系統 – Amazon Linux 2
- RAM – 16 GB
- CPU – 4 個核心

下列程序會逐步引導您在 VMware 環境中部署 Agentless Collector OVA 檔案。

部署 Agentless Collector

1. 以 VMware 管理員身分登入 vCenter。
2. 使用下列其中一種方法來安裝 OVA 檔案：
   - 使用 UI：選擇檔案，選擇部署 OVF 範本，選取您在上一節下載的收集器 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。
   - 使用命令列：若要從命令列安裝收集器 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。

     以下是使用 ovftool 命令列工具安裝收集器 OVA 檔案的範例。

     ```
     ovftool --acceptAllEulas --name=AgentlessCollector --datastore=datastore1
      -dm=thin ApplicationDiscoveryServiceAgentlessCollector.ova
      'vi://username:password@vcenterurl/Datacenter/host/esxi/'
     ```

     以下說明範例中***###***的值

     - 名稱是您要用於 Agentless Collector VM 的名稱。
     - 資料存放區是 vCenter 中資料存放區的名稱。
     - OVA 檔案名稱是下載的收集器 OVA 檔案名稱。
     - 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。
3. 在 vCenter 中尋找已部署的 Agentless Collector。在 VM 上按一下滑鼠右鍵，然後選擇開啟電源、開啟電源。
4. 幾分鐘後，收集器的 IP 地址會顯示在 vCenter 中。您可以使用此 IP 地址來連線至收集器。

存取 Agentless Collector 主控台

下列程序說明如何存取 Application Discovery Service Agentless Collector (Agentless Collector) 主控台。

存取 Agentless Collector 主控台

1. 開啟 Web 瀏覽器，然後在網址列中輸入下列 URL：**https://***<ip_address>***/**，其中 *<ip_address>* 是來自 的收集器 IP 地址部署 Agentless Collector。

2. 第一次存取 Agentless Collector 時，請選擇開始使用。之後，系統會要求您登入。

如果您是第一次存取 Agentless Collector 主控台，接下來您將 設定無代理程式收集器。否則，您會看到 Agentless Collector 儀表板。

設定無代理程式收集器

Application Discovery Service Agentless Collector (Agentless Collector) 是基於 Amazon Linux 2 的虛擬機器 (VM)。下一節說明如何在 Agentless Collector 主控台的設定 Agentless Collector 頁面上設定收集器 VM。

在設定無代理程式收集器頁面上設定收集器 VM

1. 對於收集器名稱，輸入收集器的名稱來識別它。名稱可以包含空格，但不能包含特殊字元。
2. 在資料同步下，輸入 AWS 帳戶 IAM 使用者的 AWS 存取金鑰和私密金鑰，以指定 做為目的地帳戶，以接收收集器探索到的資料。如需 IAM 使用者需求的相關資訊，請參閱 部署 Application Discovery Service 無代理程式收集器。

   a. 對於AWS 存取金鑰，輸入您指定為目的地 AWS 帳戶之帳戶 IAM 使用者的存取金鑰。
   b. 針對AWS 私密金鑰，輸入您要指定為目的地 AWS 帳戶之帳戶 IAM 使用者的私密金鑰。
   c. （選用）如果您的網路需要使用代理存取 AWS，請輸入代理主機、代理連接埠，以及選擇性使用現有代理伺服器進行身分驗證所需的登入資料。
3. 在 Agentless Collector 密碼下，設定用於驗證 Agentless Collector 存取權的密碼。

   - 密碼區分大小寫
   - 密碼長度必須介於 8 到 64 個字元之間
   - 密碼必須至少包含以下四個類別中的一個字元：
     - 小寫字母 (a-z)
     - 大寫字母 (A-Z)
     - 數字 (0-9)
     - 非英數字元 (@$！#%*？&)
   - 密碼不能包含下列字元以外的特殊字元：@$！#%*？&

   a. 針對 Agentless Collector 密碼，輸入用來驗證收集器存取權的密碼。
   b. 對於重新輸入 Agentless Collector 密碼，若要驗證，請再次輸入密碼。

4. 在其他設定下，閱讀授權合約。若您同意接受，請選取核取方塊。
5. 若要啟用 Agentless Collector 的自動更新，請在其他設定下，選取自動更新 Agentless Collector。如果您未選取此核取方塊，則需要手動更新 Agentless Collector，如 中所述手動更新 Application Discovery Service Agentless Collector。
6. 選擇儲存組態。

下列主題說明選用的收集器組態任務。

選用組態任務

- （選用）設定 Agentless Collector VM 的靜態 IP 地址
- （選用）使用 DHCP 將 Agentless Collector VM 重設回
- （選用）設定 Kerberos 身分驗證通訊協定

（選用）設定 Agentless Collector VM 的靜態 IP 地址

下列步驟說明如何設定 Application Discovery Service Agentless Collector (Agentless Collector) VM 的靜態 IP 地址。第一次安裝時，收集器 VM 會設定為使用動態主機組態通訊協定 (DHCP)。

> **Note**
>
> Agentless Collector 支援 IPv4。它不支援 IPv6。

Agentless Collector version 2

設定收集器 VM 的靜態 IP 地址

1. 從 VMware vCenter 收集下列網路資訊：
   - 靜態 IP 地址 – 子網路中未簽章的 IP 地址。例如，192.168.1.138。
   - CIDR 網路遮罩 – 若要取得 CIDR 網路遮罩，請檢查託管收集器 VM 的 VMware vCenter 主機的 IP 地址設定。例如，/24。
   - 預設閘道 – 若要取得預設閘道，請檢查託管收集器 VM 的 VMware vCenter 主機 IP 地址設定。例如，192.168.1.1。
   - 主要 DNS – 若要取得主要 DNS，請檢查託管收集器 VM 的 VMware vCenter 主機 IP 地址設定。例如，192.168.1.1。

- （選用）次要 DNS
- （選用）本機網域名稱 – 這可讓收集器到達沒有網域名稱的 vCenter 主機 URL。

2. 開啟收集器的 VM 主控台**ec2-user**，並使用密碼以 登入**collector**，如下列範例所示。

```
username: ec2-user
password: collector
```

3. 在遠端終端機中輸入下列命令來停用網路介面。

```
sudo ip link set ens192 down
```

4. 使用下列步驟更新介面組態。

   a. 使用下列命令，在 vi 編輯器中開啟 10-cloud-init-ens192.network。

   ```
   sudo vi /etc/systemd/network/10-cloud-init-ens192.network
   ```

   b. 使用您在收集網路資訊步驟中收集的資訊來更新值，如下列範例所示。

   ```
   [Match]
   Name=ens192

   [Network]
   DHCP=no
   Address=static-ip-value/CIDR-netmask
   Gateway=gateway-value
   DNS=dnsserver-value
   ```

5. 使用下列步驟更新網域名稱系統 (DNS)。

   a. 使用下列命令在 vi 中開啟 `resolv.conf` 檔案。

   ```
   sudo vi /etc/resolv.conf
   ```

   b. 使用下列命令更新 vi 中的`resolv.conf`檔案。

   ```
   search localdomain-name
   options timeout:2 attempts:5
   nameserver dnsserver-value
   ```

下列範例顯示已編輯resolv.conf的檔案。

```
search vsphere.local
options timeout:2 attempts:5
nameserver 192.168.1.1
```

6. 輸入下列命令來啟用網路界面。

```
sudo ip link set ens192 up
```

7. 重新啟動 VM，如下列範例所示。

```
sudo reboot
```

8. 使用下列步驟驗證您的網路設定。

   a. 輸入下列命令，檢查 IP 地址是否正確設定。

```
ifconfig
ip addr show
```

   b. 輸入下列命令，檢查閘道是否已正確新增。

```
route -n
```

   輸出應類似於下列範例。

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use
 Iface
0.0.0.0         192.168.1.1     0.0.0.0         UG    0      0        0 eth0
172.17.0.0      0.0.0.0         255.255.0.0     U     0      0        0
 docker0
192.168.1.0     0.0.0.0         255.255.255.0   U     0      0
```

   c. 輸入下列命令，確認您可以 ping 公有 URL。

```
ping www.google.com
```

   d. 確認您可以 ping vCenter IP 地址或主機名稱，如下列範例所示。

```
ping vcenter-host-url
```

Agentless Collector version 1

設定收集器 VM 的靜態 IP 地址

1. 從 VMware vCenter 收集下列網路資訊：
   - 靜態 IP 地址 – 子網路中未簽章的 IP 地址。例如，192.168.1.138。
   - 網路遮罩 – 若要取得網路遮罩，請檢查託管收集器 VM 的 VMware vCenter 主機 IP 地址設定。例如，255.255.255.0。
   - 預設閘道 – 若要取得預設閘道，請檢查託管收集器 VM 的 VMware vCenter 主機 IP 地址設定。例如，192.168.1.1。
   - 主要 DNS – 若要取得主要 DNS，請檢查託管收集器 VM 的 VMware vCenter 主機 IP 地址設定。例如，192.168.1.1。
   - （選用）次要 DNS
   - （選用）本機網域名稱 – 這可讓收集器到達沒有網域名稱的 vCenter 主機 URL。
2. 開啟收集器的 VM 主控台**ec2-user**，並使用密碼以 登入**collector**，如下列範例所示。

   ```
   username: ec2-user
   password: collector
   ```
3. 在遠端終端機中輸入下列命令來停用網路介面。

   ```
   sudo /sbin/ifdown eth0
   ```
4. 使用下列步驟更新界面 eth0 組態。

   a. 使用下列命令，在 vi 編輯器中開啟 ifcfg-eth0。

   ```
   sudo vi /etc/sysconfig/network-scripts/ifcfg-eth0
   ```

   b. 使用您在收集網路資訊步驟中收集的資訊來更新界面值，如下列範例所示。

   ```
   DEVICE=eth0
   BOOTPROTO=static
   ```

```
ONBOOT=yes
IPADDR=static-ip-value
NETMASK=netmask-value
GATEWAY=gateway-value
TYPE=Ethernet
USERCTL=yes
PEERDNS=no
RES_OPTIONS="timeout:2 attempts:5"
```

5. 使用下列步驟更新網域名稱系統 (DNS)。

   a. 使用下列命令在 vi 中開啟 `resolv.conf` 檔案。

   ```
   sudo vi /etc/resolv.conf
   ```

   b. 使用下列命令更新 vi 中的`resolv.conf`檔案。

   ```
   search localdomain-name
   options timeout:2 attempts:5
   nameserver dnsserver-value
   ```

   下列範例顯示已編輯`resolv.conf`的檔案。

   ```
   search vsphere.local
   options timeout:2 attempts:5
   nameserver 192.168.1.1
   ```

6. 輸入下列命令來啟用網路界面。

   ```
   sudo /sbin/ifup eth0
   ```

7. 重新啟動 VM，如下列範例所示。

   ```
   sudo reboot
   ```

8. 使用下列步驟驗證您的網路設定。

   a. 輸入下列命令，檢查 IP 地址是否正確設定。

   ```
   ifconfig
   ip addr show
   ```

b. 輸入下列命令，檢查閘道是否已正確新增。

```
route -n
```

輸出應類似於下列範例。

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use
 Iface
0.0.0.0         192.168.1.1     0.0.0.0         UG    0      0        0 eth0
172.17.0.0      0.0.0.0         255.255.0.0     U     0      0        0
 docker0
192.168.1.0     0.0.0.0         255.255.255.0   U     0      0
```

c. 輸入下列命令，確認您可以 ping 公有 URL。

```
ping www.google.com
```

d. 確認您可以 ping vCenter IP 地址或主機名稱，如下列範例所示。

```
ping vcenter-host-url
```

（選用）使用 DHCP 將 Agentless Collector VM 重設回

下列步驟說明如何重新設定 Agentless Collector VM 以使用 DHCP。

Agentless Collector version 2

設定收集器 VM 以使用 DHCP

1. 在遠端終端機中執行下列命令來停用網路介面。

```
sudo ip link set ens192 down
```

2. 使用下列步驟更新介面組態。

a. 使用下列命令，在 vi 編輯器中開啟 `10-cloud-init-ens192.network` 檔案。

```
sudo vi /etc/systemd/network/10-cloud-init-ens192.network
```

b. 更新值，如下列範例所示。

```
[Match]
Name=ens192

[Network]
DHCP=yes

[DHCP]
ClientIdentifier=mac
```

3. 輸入下列命令以重設 DNS 設定。

```
echo "" | sudo tee /etc/resolv.conf
```

4. 輸入下列命令來啟用網路界面。

```
sudo ip link set ens192 up
```

5. 重新啟動收集器 VM，如下列範例所示。

```
sudo reboot
```

Agentless Collector version 1

設定收集器 VM 以使用 DHCP

1. 在遠端終端機中執行下列命令來停用網路介面。

```
sudo /sbin/ifdown eth0
```

2. 使用下列步驟更新網路組態。

a. 使用下列命令在 vi 編輯器中開啟 `ifcfg-eth0` 檔案。

```
sudo /sbin/ifdown eth0
```

b. 更新 `ifcfg-eth0` 檔案中的值，如下列範例所示。

```
DEVICE=eth0
BOOTPROTO=dhcp
```

```
ONBOOT=yes
TYPE=Ethernet
USERCTL=yes
PEERDNS=yes
DHCPV6C=yes
DHCPV6C_OPTIONS=-nw
PERSISTENT_DHCLIENT=yes
RES_OPTIONS="timeout:2 attempts:5"
```

3. 輸入下列命令以重設 DNS 設定。

```
echo "" | sudo tee /etc/resolv.conf
```

4. 輸入下列命令來啟用網路界面。

```
sudo /sbin/ifup eth0
```

5. 重新啟動收集器 VM，如下列範例所示。

```
sudo reboot
```

（選用）設定 Kerberos 身分驗證通訊協定

如果您的作業系統伺服器支援 Kerberos 身分驗證通訊協定，則您可以使用此通訊協定連線到您的伺服器。若要這樣做，您必須設定 Application Discovery Service Agentless Collector VM。

下列步驟說明如何在 Application Discovery Service Agentless Collector VM 上設定 Kerberos 身分驗證通訊協定。

在收集器 VM 上設定 Kerberos 身分驗證通訊協定

1. 開啟收集器的 VM 主控台**ec2-user**，並使用密碼以 登入**collector**，如下列範例所示。

```
username: ec2-user
password: collector
```

2. 在 /etc 資料夾中開啟krb5.conf組態檔案。若要這麼做，您可以使用下列程式碼範例。

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

3. 使用下列資訊更新krb5.conf組態檔案。

```
[libdefaults]
    forwardable = true
    dns_lookup_realm = true
    dns_lookup_kdc = true
    ticket_lifetime = 24h
    renew_lifetime = 7d
    default_realm = default_Kerberos_realm

[realms]
 default_Kerberos_realm = {
     kdc = KDC_hostname
     server_name = server_hostname
     default_domain = domain_to_expand_hostnames
 }

[domain_realm]
 .domain_name = default_Kerberos_realm
 domain_name = default_Kerberos_realm
```

儲存檔案，然後結束文字編輯器。

4. 重新啟動收集器 VM，如下列範例所示。

```
sudo reboot
```

使用 Agentless Collector Network Data Collection 模組

網路資料收集模組可讓您探索現場部署資料中心伺服器之間的相依性。此網路資料可讓您了解應用程式如何跨伺服器通訊，進而加速遷移規劃。

網路資料收集模組會連線至 VMware vCenter 模組識別的伺服器，並分析來源 IP 到這些伺服器的目的地 IP/連接埠流量。

主題

- 設定網路資料收集模組
- 網路資料收集嘗試
- Network Data Collection 模組中的伺服器狀態

設定網路資料收集模組

網路資料收集模組會收集來自 VMware vCenter 模組之伺服器庫存的網路資料。因此，若要使用網路資料收集模組，請先設定 VMware vCenter 模組。如需指示，請遵循下列主題中的指引：

1. the section called “部署收集器”
2. the section called “存取收集器主控台”
3. the section called “設定收集器”
4. the section called “使用 VMware 資料收集模組”

設定網路資料收集模組

1. 在 Agentless Collector 儀表板的網路資料收集區段中，選擇檢視網路連線。
2. 在網路連線頁面上，選擇編輯收集器。
3. 在登入資料區段中，輸入至少一組登入資料。您最多可以輸入 10 組登入資料。模組第一次嘗試收集伺服器資料時，會嘗試所有登入資料，直到找到一組有效的登入資料為止；然後儲存該設定，並在後續嘗試中再次使用。如需設定登入資料的資訊，請參閱the section called “設定登入資料”。
4. 在資料收集偏好設定區段中，若要在伺服器重新啟動時自動開始收集資料，請選取自動開始資料收集。
5. 如果您尚未設定 WinRM 憑證，請選取停用 WinRM 憑證檢查。
6. 選擇 Save (儲存)。
7. 每 15 秒會在伺服器上進行收集。若要查看指定伺服器集合嘗試的詳細資訊，請選取伺服器資料表中伺服器左側的核取方塊。

設定登入資料

網路資料收集模組使用 WinRM 從 Windows 伺服器收集資料。它使用 SNMPv2 和 SNMPv3 從 Linux 伺服器收集資料。

WinRM 登入資料：

- 指定具有下列項目之 Windows 帳戶的使用者名稱和密碼：
  - `\root\standardcimv2` 對命名空間的讀取存取權
  - `MSFT_NetTCPConnection` 類別的讀取許可

  - 遠端 WMI 存取
- 我們建議您建立具有最少必要許可的專用服務帳戶。
- 避免使用網域管理員或本機管理員帳戶。
- 連接埠 5986 (HTTPS) 必須在收集器和目標伺服器之間開啟。
- 避免停用 WinRM 憑證檢查。如需設定 WinRM 憑證的詳細資訊，請參閱the section called “在設定 WinRM 憑證時解決自我簽署的憑證問題”。

SNMPv2 登入資料：

- 提供可存取 1.3.6.1.2.1.6.13 的唯讀社群字串。* OID
- SNMPv3 較 SNMPv2 為佳，因為 SNMPv3 的安全性有所提升
- 連接埠 161/UDP 必須在收集器和目標伺服器之間開啟
- 使用複雜的非預設社群字串
- 避免常見的字串，例如 "public" 或 "private"
- 將社群字串視為密碼

SNMPv3 登入資料

- 提供使用者名稱/密碼和身分驗證/隱私權詳細資訊，以及可存取 1.3.6.1.2.1.6.13 的唯讀許可。* OID。
- 連接埠 161/UDP 必須在收集器和目標伺服器之間開啟
- 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 (AES 優於 DES)
- 使用複雜的密碼進行身分驗證和隱私權
- 使用唯一的使用者名稱 （避免常用名稱）

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

網路資料收集嘗試

發現新的伺服器時，收集器會嘗試每個 IP 地址的每個已設定登入資料。收集器找到有效的登入資料後，只會使用該登入資料。連續兩次故障後，收集器會嘗試在 30 分鐘、2 小時、8 小時，然後 24 小時後收集伺服器的聯網資料。嘗試失敗 6 次後，收集器會繼續每天嘗試一次所有設定的登入資料。若要解決此問題，請選擇編輯收集器來編輯目前憑證或新增其他憑證，或變更要監控的目標伺服器。

Network Data Collection 模組中的伺服器狀態

下表說明集合狀態值。

Status	意義
收集或收集	上次嘗試收集網路連線成功。
發生錯誤或發生錯誤	由於聯網或許可問題，上次嘗試收集網路連線失敗。如需詳細資訊，請選取伺服器左側出現錯誤的核取方塊。
略過	未提供有效登入資料的伺服器。更新或設定其他伺服器登入資料。
無資料	伺服器的資料收集尚未啟動。若要開始收集資料，請選擇開始收集器。
待定	集合已開始，但尚未嘗試集合。等待幾分鐘，然後重新整理清單。

使用 VMware vCenter Agentless Collector 資料收集模組

本節說明 Application Discovery Service Agentless Collector (Agentless Collector) VMware vCenter 資料收集模組，用於從您的 VMware VMs 收集伺服器庫存、設定檔和使用率資料。

主題

- 設定 VMware vCenter 的 Agentless Collector 資料收集模組

- 檢視 VMware 資料收集詳細資訊
- 控制 vCenter 資料收集的範圍
- Agentless Collector VMware vCenter 資料收集模組收集的資料

設定 VMware vCenter 的 Agentless Collector 資料收集模組

本節說明如何設定 Agentless Collector VMware vCenter 資料收集模組，以從您的 VMware VMs 收集伺服器庫存、設定檔和使用率資料。

> **Note**
>
> 開始 vCenter 設定之前，請確定您可以使用系統群組的讀取和檢視許可集來提供 vCenter 憑證。

設定 VMware vCenter 資料收集模組

1. 在 Agentless Collector 儀表板頁面的資料收集下，選擇 VMware vCenter 區段中的設定。
2. 在設定 VMware vCenter 資料收集頁面上，執行下列動作：
   a. 在 vCenter 登入資料下：
      i. 針對 vCenter URL/IP，輸入 VMware vCenter Server 主機的 IP 地址。
      ii. 針對 vCenter 使用者名稱，輸入收集器用來與 vCenter 通訊的本機或網域使用者名稱。網域使用者使用的格式為 domain\username 或 username@domain。
      iii. 在 vCenter Password (vCenter 密碼) 中輸入本機或網域使用者的密碼。
   b. 在資料收集偏好設定下：
      - 若要在設定成功後立即自動開始收集資料，請選取自動開始資料收集。
   c. 選擇 Set up (設定)。

接下來，您將看到 VMware 資料收集詳細資訊頁面，如下一個主題所述。

檢視 VMware 資料收集詳細資訊

VMware 資料收集詳細資訊頁面會顯示您在 中設定的 vCenter 詳細資訊設定 VMware vCenter 的 Agentless Collector 資料收集模組。

在探索的 vCenter 伺服器下，您設定的 vCenter 會列出下列 vCenter 的相關資訊：

- vCenter 伺服器的 IP 地址。
- vCenter 中的伺服器數量。
- 資料收集的狀態。
- 自上次更新以來的時間長度。

選擇移除 vCenter 伺服器以移除顯示的 vCenter 伺服器，並返回設定 VMware vCenter 資料收集頁面。

如果您未選擇自動開始資料收集，您可以使用此頁面上的開始資料收集按鈕來開始資料收集。資料收集開始後，開始按鈕會變更為停止資料收集。

如果收集狀態欄顯示收集，表示資料收集已開始。

您可以在 AWS Migration Hub 主控台中檢視收集的資料。如果您要收集 VMware vCenter 伺服器清查的資料，您可以在開啟資料收集後約 15 分鐘存取主控台中顯示的資料。

如果您的網際網路存取未遭到封鎖，您可以在此頁面的 Migration Hub 中選擇檢視伺服器，以開啟 Migration Hub 主控台。無論您是否選擇此按鈕，如需如何存取 Migration Hub 主控台的資訊，請參閱檢視收集的資料。

以下是根據遷移規劃活動建議資料收集長度的指導方針：

- TCO （總擁有成本） - 2 到 4 週
- 遷移規劃 - 2 到 6 週

控制 vCenter 資料收集的範圍

vCenter 使用者需要每個 ESX 主機或 VM 的唯讀許可，才能使用 Application Discovery Service 清查。您可以使用許可設定，控制資料收集的範圍包括哪些主機和 VM。您可以允許清查目前 vCenter 下的所有主機和 VM，或逐案例授予許可。

> **Note**
>
> 作為安全最佳實務，我們建議不要將其他不需要的許可授予 Application Discovery Service 的 vCenter 使用者。

以下程序說明從最粗糙到最精細的組態案例。這些程序適用於 vSphere Client v6.7.0.2。其他版本的用戶端的程序可能不同，取決於您使用的 vSphere 用戶端版本。

探索目前 vCenter 下所有 ESX 主機和 VM 的相關資料

1. 在您的 VMware vSphere 用戶端中，選擇 vCenter，然後選擇 Hosts and Clusters (主機與叢集) 或 VMs and Templates (VM 與範本)。
2. 選擇資料中心資源，然後選擇許可。
3. 選擇 vCenter 使用者，然後選擇要新增、編輯或移除使用者角色的符號。
4. 從角色功能表中選擇唯讀。
5. 選擇傳播到子系，然後選擇確定。

探索特定 ESX 主機及其所有子物件的相關資料

1. 在您的 VMware vSphere 用戶端中，選擇 vCenter，然後選擇 Hosts and Clusters (主機與叢集) 或 VMs and Templates (VM 與範本)。
2. 依序選擇 Related Objects (相關物件) 和 Hosts (主機)。
3. 開啟內容 (按一下滑鼠右鍵) 選單取得主機名稱，並依序選擇 All vCenter Actions (所有 vCenter 動作) 和 Add Permission (新增許可)。
4. 在 Add Permission (新增許可) 下將 vCenter 使用者新增至主機。針對 Assigned Role (指派的角色) 選擇 Read-only (唯讀)。
5. 依序選擇 Propagate to children (向兒童傳播) 和 OK (確定)。

探索特定 ESX 主機或子 VM 的資料

1. 在您的 VMware vSphere 用戶端中，選擇 vCenter，然後選擇 Hosts and Clusters (主機與叢集) 或 VMs and Templates (VM 與範本)。
2. 依序選擇 Related Objects (相關物件)。
3. 選擇 Hosts (主機) (顯示 vCenter 已知的 ESX 主機清單) 或 Virtual Machines (虛擬機器) (顯示所有 ESX 主機上的 VM 清單)。
4. 開啟內容 (按一下滑鼠右鍵) 選單取得主機或 VM 名稱，並依序選擇 All vCenter Actions (所有 vCenter 動作) 和 Add Permission (新增許可)。
5. 在 Add Permission (新增許可) 下將 vCenter 使用者新增至主機或 VM。針對 Assigned Role (指派的角色) 選擇 Read-only (唯讀)。
6. 選擇確定。

> **Note**
>
> 如果您選擇 Propagate to children (向兒童傳播)，您仍然可以逐案例移除 ESX 主機和 VM 的唯讀許可。此選項不會影響套用到其他 ESX 主機和 VM 的已繼承許可。

Agentless Collector VMware vCenter 資料收集模組收集的資料

以下資訊說明 Application Discovery Service Agentless Collector (Agentless Collector) VMware vCenter 資料收集模組收集的資料。如需設定資料收集的詳細資訊，請參閱設定 VMware vCenter 的 Agentless Collector 資料收集模組。

Agentless Collector VMware vCenter 收集資料的資料表圖例：

- 收集的資料是以千位元組 (KB) 為單位 (除非另有指明)。
- Migration Hub 主控台中的同等資料會以 MB (MB) 為單位報告。
- 以星號 (*) 表示的資料欄位僅適用於從 Application Discovery Service API 匯出函數產生的 .csv 檔案。

  Agentless Collector 支援使用 CLI AWS 匯出資料。若要使用 AWS CLI 匯出收集的資料，請遵循 Application Discovery Service 使用者指南中 Export System Performance Data for All Servers 頁面中的指示。
- 輪詢期間大約為 60 分鐘間隔。
- 以雙星號 (**) 表示的資料欄位目前傳回 null 值。

資料欄位	描述
applicationConfigurationId*	VM 分組的遷移應用程式 ID。
avgCpuUsagePct	輪詢期間 CPU 使用率的平均百分比。
avgDiskBytesReadPerSecond	輪詢期間從磁碟讀取的平均位元組數。
avgDiskBytesWrittenPerSecond	輪詢期間寫入磁碟的平均位元組數。
avgDiskReadOpsPerSecond**	每秒讀取 I/O 操作的平均數量 null。
avgDiskWriteOpsPerSecond**	每秒寫入 I/O 操作的平均數量。

資料欄位	描述
avgFreeRAM	以 MB 表示的平均可用 RAM。
avgNetworkBytesReadPerSecond	每秒讀取位元組的平均輸送量。
avgNetworkBytesWrittenPerSecond	每秒寫入位元組的平均輸送量。
computerManufacturer	ESXi 主機報告的廠商。
computerModel	ESXi 主機報告的電腦模型。
configId	Application Discovery Service 指派給探索 VM 的 ID。
configType	發現的資源類型。
connectorId	虛擬設備的 ID。
cpuType	VM 的 vCPU，主機的實際模型。
datacenterId	vCenter 的 ID。
hostId*	VM 主機的 ID。
hostName	執行虛擬化軟體的主機名稱。
hypervisor	Hypervisor 的類型。
id	伺服器 ID。
lastModifiedTimeStamp*	資料匯出前資料收集的日期和時間。
macAddress	VM 的 MAC 地址。
manufacturer	虛擬化軟體的製造商。
maxCpuUsagePct	輪詢期間 CPU 用量的百分比上限。
maxDiskBytesReadPerSecond	輪詢期間從磁碟讀取的位元組數目上限。
maxDiskBytesWrittenPerSecond	輪詢期間寫入磁碟的位元組數目上限。

資料欄位	描述
maxDiskReadOpsPerSecond**	每秒讀取 I/O 操作的數量上限。
maxDiskWriteOpsPerSecond**	每秒寫入 I/O 操作的數量上限。
maxNetworkBytesReadPerSecond	每秒讀取位元組的最大輸送量。
maxNetworkBytesWrittenPerSecond	每秒寫入位元組的最大輸送量。
memoryReservation*	限制以避免 VM 上的記憶體過度遞交。
moRefId	唯一 vCenter 受管物件參考 ID。
name*	VM 或網路的名稱（使用者指定）。
numCores	指派給 VM 的 CPU 核心數量。
numCpus	ESXi 主機上的 CPU 通訊端數量。
numDisks**	VM 上的磁碟數量。
numNetworkCards**	VM 上的網路卡數量。
osName	VM 上的作業系統名稱。
osVersion	VM 上的作業系統版本。
portGroupId*	VLAN 的成員連接埠群組 ID。
portGroupName*	VLAN 的成員連接埠群組名稱。
powerState*	電源狀態。
serverId	Application Discovery Service 已將 ID 指派給探索的 VM。
smBiosId*	系統管理 BIOS 的 ID/版本。
state*	虛擬設備的狀態。
toolsStatus	VMware 工具的操作狀態

資料欄位	描述
totalDiskFreeSize	可用磁碟空間，以 MB 表示。適用於 vCenter Server 7.0 和更新版本。
totalDiskSize	磁碟的總容量，以 MB 表示。
totalRAM	VM 上可用的 RAM 總量，以 MB 為單位。
type	主機類型。
vCenterId	VM 的唯一 ID 號碼。
vCenterName*	vCenter 主機的名稱。
virtualSwitchName*	虛擬交換器的名稱。
vmFolderPath	VM 檔案的目錄路徑。
vmName	虛擬機器的名稱。

使用資料庫和分析資料收集模組

本節說明如何設定、設定和使用資料庫和分析資料收集模組。您可以使用此資料收集模組來連線至資料環境，並從內部部署資料庫和分析伺服器收集中繼資料和效能指標。如需有關您可以使用此模組收集之指標的資訊，請參閱 Agentless Collector 資料庫和分析資料收集模組收集的資料。

> **Important**
>
> 支援結束通知：2026 年 5 月 20 日， AWS 將結束對 AWS Database Migration Service Fleet Advisor 的支援。2026 年 5 月 20 日之後，您將無法再存取 AWS DMS Fleet Advisor 主控台或 AWS DMS Fleet Advisor 資源。如需詳細資訊，請參閱 AWS DMS Fleet Advisor 終止支援。

在高層級上，使用資料庫和分析資料收集模組時，您會採取下列步驟。

1. 完成先決條件步驟、設定 IAM 使用者，以及建立 AWS DMS 資料收集器。
2. 設定資料轉送，以確保您的資料收集模組可以將收集的中繼資料和效能指標傳送至其中 AWS。

3. 新增您的 LDAP 伺服器，並使用它們來探索資料環境中的作業系統伺服器。或者，手動新增作業系統伺服器或使用 使用 VMware 資料收集模組。
4. 設定作業系統伺服器的連線憑證，然後使用它們來探索資料庫伺服器。
5. 設定資料庫和分析伺服器的連線登入資料，然後執行資料收集。如需詳細資訊，請參閱資料庫和分析資料收集。
6. 在 AWS DMS 主控台中檢視收集的資料，並使用它來產生遷移到 的目標建議 AWS 雲端。如需詳細資訊，請參閱資料庫和分析資料收集。

主題

支援的作業系統、資料庫和分析伺服器

Agentless Collector 中的資料庫和分析資料收集模組支援 Microsoft Active Directory LDAP 伺服器。

此資料收集模組支援下列作業系統伺服器。

- Amazon Linux 2
- CentOS Linux 第 6 版及更新版本
- Debian 第 10 版及更新版本
- Red Hat Enterprise Linux 第 7 版及更新版本
- SUSE Linux Enterprise Server 第 12 版及更新版本
- Ubuntu 16.01 版及更新版本
- Windows Server 2012 及更高版本
- Windows XP 及更高版本

此外，資料庫和分析資料收集模組支援下列資料庫伺服器。

- Microsoft SQL Server 2012 版及最高至 2019 版
- MySQL 5.6 版，最高至 8 版
- Oracle 11g 版本 2 及最高至 12c、19c 和 21c
- PostgreSQL 9.6 版及最高至 13 版

建立 AWS DMS 資料收集器

您的資料庫和分析資料收集模組使用 AWS DMS 資料收集器與 AWS DMS 主控台互動。您可以在 AWS DMS 主控台中檢視收集的資料，或使用它來判斷大小正確的 AWS 目標引擎。如需詳細資訊，請參閱使用 AWS DMS Fleet Advisor 目標建議功能。

建立 AWS DMS 資料收集器之前，請先建立 AWS DMS 資料收集器用來存取 Amazon S3 儲存貯體的 IAM 角色。當您在 中完成先決條件時，已建立此 Amazon S3 儲存貯體Agentless Collector 的先決條件。

為您的 AWS DMS 資料收集器建立存取 Amazon S3 的 IAM 角色

1. 登入 AWS Management Console 並開啟位於 https：//https://console.aws.amazon.com/iam/ 的 IAM 主控台。
2. 在導覽窗格中，選擇角色，然後選擇建立角色。
3. 在選取受信任實體頁面上，針對信任的實體類型選擇 AWS 服務。針對其他服務的使用案例 AWS，選擇 DMS。
4. 選取 DMS 核取方塊，然後選擇下一步。
5. 在新增許可頁面上，選擇您之前建立的 FleetAdvisorS3Policy。選擇下一步。
6. 在命名、檢閱和建立頁面上的角色名稱輸入 **FleetAdvisorS3Role**，然後選擇建立角色。
7. 開啟您建立的角色，然後選擇信任關係索引標籤。選擇編輯信任政策。
8. 在編輯信任政策頁面上，將下列 JSON 貼到編輯器中，取代現有的程式碼。

```
{
 "Version": "2012-10-17",
 "Statement": [{
  "Sid": "",
  "Effect": "Allow",
  "Principal": {
   "Service": [
    "dms.amazonaws.com",
```

```
    "dms-fleet-advisor.amazonaws.com"
   ]
  },
  "Action": "sts:AssumeRole"
 }]
}
```

9. 選擇更新政策。

現在，在 AWS DMS 主控台中建立資料收集器。

建立 AWS DMS 資料收集器

1. 登入 AWS Management Console ，並在 https：//https://console.aws.amazon.com/dms/v2/ 開啟 AWS DMS 主控台。
2. 選擇 AWS 區域 您設定為 Migration Hub 主區域的 。如需詳細資訊，請參閱登入 Migration Hub 並選擇主要區域。
3. 在導覽窗格中，選擇探索底下的資料收集器。資料收集器頁面隨即開啟。
4. 選擇建立資料收集器。建立資料收集器頁面隨即開啟。
5. 在一般組態區段的名稱中，輸入資料收集器的名稱。
6. 在連線能力區段中，選擇 Browse S3。從清單中選擇您之前建立的 Amazon S3 儲存貯體。
7. 對於 IAM 角色，請選擇您之前建立`FleetAdvisorS3Role`的 。
8. 選擇建立資料收集器。

設定資料轉送

建立所需的 AWS 資源後，請設定從資料庫和分析資料收集模組轉送至 AWS DMS 收集器的資料。

設定資料轉送

1. 開啟 Agentless Collector 主控台。如需詳細資訊，請參閱存取收集器主控台。
2. 選擇檢視資料庫和分析收集器。
3. 在儀表板頁面上，選擇資料轉送區段中的設定資料轉送。
4. 對於 AWS 區域、IAM 存取金鑰 ID 和 IAM 私密存取金鑰，您的 Agentless Collector 會使用您之前設定的值。如需詳細資訊，請參閱登入 Migration Hub 並選擇主要區域及部署收集器。
5. 針對連線的 DMS 資料收集器，選擇您在 AWS DMS 主控台中建立的資料收集器。

6. 選擇儲存。

設定資料轉送之後，請檢查儀表板頁面上的資料轉送區段。請確定
您的資料庫和分析資料收集模組會顯
示 連
線以存取 DMS 和存取 S3。

新增您的 LDAP 和作業系統伺服器

資料庫和分析資料收集模組使用 Microsoft Active Directory 中的 LDAP 來收集您網路中作業系統、資料庫和分析伺服器的相關資訊。輕量型目錄存取通訊協定 (LDAP) 是開放的標準應用程式通訊協定，您可以使用此通訊協定，透過 IP 網路存取和維護分散式目錄資訊服務。

您可以將現有的 LDAP 伺服器新增至資料庫和分析資料收集模組，以自動探索網路中的作業系統伺服器。如果您不使用 LDAP，您可以手動新增作業系統伺服器。

將 LDAP 伺服器新增至資料庫和分析資料收集模組

1. 開啟 Agentless Collector 主控台。如需詳細資訊，請參閱存取收集器主控台。
2. 選擇檢視資料庫和分析收集器，然後在導覽窗格中的探索下選擇 LDAP 伺服器。
3. 選擇新增 LDAP 伺服器。新增 LDAP 伺服器頁面隨即開啟。
4. 針對主機名稱，輸入 LDAP 伺服器的主機名稱。
5. 針對連接埠，輸入用於 LDAP 請求的連接埠號碼。
6. 針對使用者名稱，輸入您用來連線至 LDAP 伺服器的使用者名稱。
7. 針對密碼，輸入您用來連線至 LDAP 伺服器的密碼。
8. （選用）選擇驗證連線，以確保您已正確新增 LDAP 伺服器登入資料。或者，您可以稍後從 LDAP 伺服器頁面上的清單驗證 LDAP 伺服器連線憑證。
9. 選擇新增 LDAP 伺服器。
10. 在 LDAP 伺服器頁面上，從清單中選擇 LDAP 伺服器，然後選擇探索作業系統伺服器。

> **Important**
>
> 對於作業系統探索，資料收集模組需要網域伺服器的登入資料，才能使用 LDAP 通訊協定執行請求。

資料庫和分析資料收集模組會連線至 LDAP 伺服器，並探索您的作業系統伺服器。資料收集模組完成作業系統伺服器探索後，您可以選擇檢視作業系統伺服器，以查看探索到的作業系統伺服器清單。

或者，您可以手動新增作業系統伺服器，或從逗號分隔值 (CSV) 檔案匯入伺服器清單。此外，您可以使用 VMware vCenter Agentless Collector 資料收集模組來探索您的作業系統伺服器。如需詳細資訊，請參閱使用 VMware 資料收集模組。

將作業系統伺服器新增至資料庫和分析資料收集模組

1. 在資料庫和分析收集器頁面上，選擇導覽窗格中探索下的作業系統伺服器。
2. 選擇新增作業系統伺服器。新增作業系統伺服器頁面隨即開啟。
3. 提供您的作業系統伺服器登入資料。

   a. 針對作業系統類型，選擇伺服器的作業系統。

   b. 針對主機名稱/IP，輸入作業系統伺服器的主機名稱或 IP 地址。

   c. 針對連接埠，輸入用於遠端查詢的連接埠號碼。

   d. 針對身分驗證類型，選擇作業系統伺服器使用的身分驗證類型。

   e. 針對使用者名稱，輸入您用來連線至作業系統伺服器的使用者名稱。

   f. 針對密碼，輸入您用來連線至作業系統伺服器的密碼。

   g. 選擇驗證，確認您已正確新增作業系統伺服器登入資料。
4. （選用）從 CSV 檔案新增多個作業系統伺服器。

   a. 選擇從 CSV 大量匯入作業系統伺服器。

   b. 選擇下載範本以儲存 CSV 檔案，其中包含您可以自訂的範本。

   c. 根據範本，將作業系統伺服器的連線登入資料輸入 檔案。下列範例顯示如何在 CSV 檔案中提供作業系統伺服器連線登入資料。

   ```
   OS type,Hostname/IP,Port,Authentication type,Username,Password
   Linux,192.0.2.0,22,Key-based authentication,USER-EXAMPLE,ANPAJ2UCCR6DPCEXAMPLE
   Windows,203.0.113.0,,NTLM,USER2-EXAMPLE,AKIAIOSFODNN7EXAMPLE
   ```

   新增所有作業系統伺服器的登入資料後，請儲存 CSV 檔案。

   d. 選擇瀏覽，然後選擇您的 CSV 檔案。
5. 選擇新增作業系統伺服器。
6. 新增所有作業系統伺服器的登入資料後，請選取您的作業系統伺服器，然後選擇探索資料庫伺服器。

探索您的資料庫伺服器

本節會引導您完成設定作業系統和資料庫伺服器時必須採取的步驟。然後，您將探索您的伺服器，並可以選擇手動新增資料庫或分析伺服器。

對於資料庫探索，您必須為來源資料庫建立具有資料收集模組所需最低許可的使用者。如需詳細資訊，請參閱AWS DMS 《 使用者指南》中的為 AWS DMS Fleet Advisor 建立資料庫使用者。

設定

若要探索在先前新增的作業系統伺服器上執行的資料庫，資料收集模組需要存取作業系統和資料庫伺服器。此頁面概述您需要採取的步驟，以確保您的資料庫可在連線設定中指定的連接埠存取。您也將在資料庫伺服器上開啟遠端身分驗證，並提供您的資料收集模組許可。

在 Linux 上設定

完成下列程序來設定 以探索 Linux 上的資料庫伺服器。

設定 Linux 以探索資料庫伺服器

1. 提供 `ss`和 `netstat`命令的 sudo 存取權。

   下列程式碼範例會授予 `ss`和 `netstat`命令的 sudo 存取權。

   ```
   sudo bash -c "cat << EOF >> /etc/sudoers.d/username
   username ALL=(ALL) NOPASSWD: /usr/bin/ss
   username ALL=(ALL) NOPASSWD: /usr/bin/netstat
   EOF"
   ```

   在上述範例中，將 *username*取代為您在作業系統伺服器連線登入資料中指定的 Linux 使用者名稱。

   上述範例使用 `ss`和 `netstat`命令的`/usr/bin/`路徑。此路徑在您的環境中可能不同。若要判斷 `ss`和 `netstat`命令的路徑，請執行 `which ss`和 `which netstat`命令。
2. 設定您的 Linux 伺服器以允許執行遠端 SSH 指令碼，並允許網際網路控制訊息通訊協定 (ICMP) 流量。

在 Microsoft Windows 上設定

完成下列程序來設定 以探索 Microsoft Windows 上的資料庫伺服器。

設定 Microsoft Windows 以探索資料庫伺服器

1. 提供憑證與授權，以執行 Windows Management Instrumentation (WMI) 和 WMI Query Language (WQL) 查詢並讀取登錄檔。
2. 將您在作業系統伺服器連線登入資料中指定的 Windows 使用者新增至下列群組：分散式 COM 使用者、效能日誌使用者、效能監視器使用者和事件日誌讀取器。若要這樣做，請使用下列程式碼範例。

```
net localgroup "Distributed COM Users" username /ADD
net localgroup "Performance Log Users" username /ADD
net localgroup "Performance Monitor Users" username /ADD
net localgroup "Event Log Readers" username /ADD
```

   在上述範例中，將 *username*取代為您在作業系統伺服器連線登入資料中指定的 Windows 使用者名稱。
3. 為您在作業系統伺服器連線登入資料中指定的 Windows 使用者授予必要的許可。
   - 針對 Windows 管理和檢測屬性，選擇本機啟動和遠端啟用。
   - 對於 WMI 控制，選擇 、、 DEFAULT和 WMI 命名空間的執行方法CIMV2、啟用帳戶StandartCimv2、遠端啟用和讀取安全許可。
   - 對於 WMI 外掛程式，執行 `winrm configsddl default` ，然後選擇讀取和執行。
4. 使用以下程式碼範例來設定您的 Windows 主機。

```
netsh advfirewall firewall add rule name="Open Ports for WinRM incoming traffic"
 dir=in action=allow protocol=TCP localport=5985, 5986 # Opens ports for WinRM
netsh advfirewall firewall add rule name="All ICMP V4" protocol=icmpv4:any,any
 dir=in action=allow # Allows ICPM traffic

Enable-PSRemoting -Force # Enables WinRM
Set-Service WinRM -StartMode Automatic # Allows WinRM service to run on host
 startup
Set-Item WSMan:\localhost\Client\TrustedHosts -Value {IP} -Force # Sets the
 specific IP from which the access to WinRM is allowed

winrm set winrm/config/service '@{Negotiation="true"}' # Allow Negosiate auth usage
winrm set winrm/config/service '@{AllowUnencrypted="true"}' # Allow unencrypted
 connection
```

探索資料庫伺服器

完成以下一組任務，以在 主控台上探索和新增資料庫伺服器。

開始探索資料庫伺服器

1. 在資料庫和分析收集器頁面上，選擇導覽窗格中探索下的作業系統伺服器。
2. 選取包含資料庫和分析伺服器的作業系統伺服器，然後在動作功能表上選擇驗證連線。
3. 對於連線狀態為失敗的伺服器，請編輯連線憑證。
    a. 選取具有相同登入資料的單一伺服器或多部伺服器，然後在動作功能表上選擇編輯。編輯作業系統伺服器頁面隨即開啟。
    b. 針對連接埠，輸入用於遠端查詢的連接埠號碼。
    c. 針對身分驗證類型，選擇作業系統伺服器使用的身分驗證類型。
    d. 針對使用者名稱，輸入您用來連線至作業系統伺服器的使用者名稱。
    e. 針對密碼，輸入您用來連線至作業系統伺服器的密碼。
    f. 選擇驗證連線，以確保您正確更新作業系統伺服器登入資料。接著，選擇儲存。
4. 更新所有作業系統伺服器的登入資料後，請選取您的作業系統伺服器，然後選擇探索資料庫伺服器。

資料庫和分析資料收集模組會連線至您的作業系統伺服器，並探索支援的資料庫和分析伺服器。資料收集模組完成探索後，您可以選擇檢視資料庫伺服器，以查看探索到的資料庫和分析伺服器清單。

或者，您可以手動將資料庫和分析伺服器新增至庫存。此外，您可以從 CSV 檔案匯入伺服器清單。如果您已將所有資料庫和分析伺服器新增至庫存，則可以略過此步驟。

手動新增資料庫或分析伺服器

1. 在資料庫和分析收集器頁面上，選擇導覽窗格中的資料收集。
2. 選擇新增資料庫伺服器。新增資料庫伺服器頁面隨即開啟。
3. 提供您的資料庫伺服器登入資料。
    a. 針對資料庫引擎，選擇您伺服器的資料庫引擎。如需詳細資訊，請參閱支援的作業系統、資料庫和分析伺服器。
    b. 針對主機名稱/IP，輸入資料庫或分析伺服器的主機名稱或 IP 地址。
    c. 在連接埠中，輸入伺服器執行所在的連接埠。

d. 針對身分驗證類型，選擇資料庫或分析伺服器使用的身分驗證類型。

e. 針對使用者名稱，輸入您用來連線至伺服器的使用者名稱。

f. 針對密碼，輸入您用來連線至伺服器的密碼。

g. 選擇驗證以確保您已正確新增資料庫或分析伺服器登入資料。

4. （選用）從 CSV 檔案新增多個伺服器。

a. 選擇從 CSV 大量匯入資料庫伺服器。

b. 選擇下載範本以儲存 CSV 檔案，其中包含您可以自訂的範本。

c. 根據範本，將資料庫和分析伺服器的連線登入資料輸入 檔案。下列範例顯示如何在 CSV 檔案中提供資料庫或分析伺服器連線憑證。

```
Database engine,Hostname/IP,Port,Authentication type,Username,Password,Oracle
 service name,Database,Allow public key retrieval,Use SSL,Trust server
 certificate
Oracle,192.0.2.1,1521,Login/Password authentication,USER-
EXAMPLE,AKIAI44QH8DHBEXAMPLE,orcl,,,,
PostgreSQL,198.51.100.1,1533,Login/Password authentication,USER2-
EXAMPLE,bPxRfiCYEXAMPLE,,postgre,,TRUE,
MSSQL,203.0.113.1,1433,Login/Password authentication,USER3-
EXAMPLE,h3yCo8nvbEXAMPLE,,,,,TRUE
MySQL,2001:db8:4006:812:ffff:200e,8080,Login/Password authentication,USER4-
EXAMPLE,APKAEIVFHP46CEXAMPLE,,mysql,TRUE,TRUE,
```

新增所有資料庫和分析伺服器的登入資料後，請儲存 CSV 檔案。

d. 選擇瀏覽，然後選擇您的 CSV 檔案。

5. 選擇新增資料庫伺服器。

6. 新增所有作業系統伺服器的登入資料後，請選取您的作業系統伺服器，然後選擇探索資料庫伺服器。

將所有資料庫和分析伺服器新增至資料收集模組後，請將它們新增至清查。資料庫和分析資料收集模組可以從庫存連線至伺服器，並收集中繼資料和效能指標。

將資料庫和分析伺服器新增至庫存

1. 在資料庫和分析收集器頁面上，選擇導覽窗格中探索下的資料庫伺服器。

2. 選取您要收集中繼資料和效能指標的資料庫和分析伺服器。

3. 選擇新增至庫存。

將所有資料庫和分析伺服器新增至庫存後，您可以開始收集中繼資料和效能指標。如需詳細資訊，請參閱資料庫和分析資料收集。

Agentless Collector 資料庫和分析資料收集模組收集的資料

Application Discovery Service Agentless Collector (Agentless Collector) 資料庫和分析資料收集模組會從資料環境收集下列指標。如需有關設定資料收集的資訊，請參閱使用資料庫和分析資料收集模組。

當您使用資料庫和分析資料收集模組收集中繼資料和資料庫容量時，它會擷取下列指標。

- 作業系統伺服器的可用記憶體
- 作業系統伺服器的可用儲存空間
- 資料庫版本與版次
- 作業系統伺服器的 CPU 數量
- 結構描述數目
- 預存程序數目
- 資料表數目
- 觸發程序數目
- 檢視數目
- 結構描述架構

在 AWS DMS 主控台中啟動結構描述分析後，資料收集模組會分析並顯示下列指標。

- 資料庫支援日期
- 程式碼的行數
- 結構描述複雜性
- 結構描述相似性

當您使用資料庫和分析資料收集模組收集中繼資料、資料庫容量和資源使用率時，它會擷取下列指標。

- 資料庫伺服器的 I/O 輸送量
- 資料庫伺服器的每秒讀寫次數 (IOPS)
- 作業系統伺服器使用的 CPU 數量

- 作業系統伺服器的記憶體使用量
- 作業系統伺服器的儲存空間使用量

您可以使用資料庫和分析資料收集模組，從您的 Oracle 和 SQL Server 資料庫收集中繼資料、容量和使用率指標。同時，對於 PostgreSQL 和 MySQL 資料庫，資料收集模組只能收集中繼資料。

檢視收集的資料

> **Important**
>
> 終止支援通知：2026 年 5 月 20 日， AWS 將終止對 AWS Database Migration Service Fleet Advisor 的支援。2026 年 5 月 20 日之後，您將無法再存取 AWS DMS Fleet Advisor 主控台或 AWS DMS Fleet Advisor 資源。如需詳細資訊，請參閱 AWS DMS Fleet Advisor 終止支援。

您可以依照中的步驟，在 Migration Hub 主控台中檢視 Application Discovery Service Agentless Collector (Agentless Collector) 收集的資料在 AWS Migration Hub 主控台中檢視伺服器。

您也可以執行下列步驟，在 AWS DMS 主控台中檢視資料庫和分析伺服器的收集指標。

在 AWS DMS 主控台中檢視資料庫和分析資料收集模組探索到的資料

1. 登入 AWS Management Console ，並在 https：//https://console.aws.amazon.com/dms/v2/ 開啟 AWS DMS 主控台。
2. 在探索下選擇庫存。詳細目錄頁面隨即開啟。
3. 選擇分析庫存以判斷資料庫結構描述屬性，例如相似性和複雜性。
4. 選擇結構描述索引標籤以查看分析結果。

您可以使用 AWS DMS 主控台來識別重複的結構描述、判斷遷移複雜性，以及匯出庫存資訊以供未來分析。如需詳細資訊，請參閱 Fleet Advisor 中的 AWS DMS 使用庫存進行分析。

存取 Agentless Collector

本節說明如何使用 Application Discovery Service Agentless Collector (Agentless Collector)。

主題

- Agentless Collector 儀表板

- 編輯 Agentless Collector 設定
- 編輯 VMware vCenter 登入資料

Agentless Collector 儀表板

在 Application Discovery Service Agentless Collector (Agentless Collector) 儀表板頁面上，您可以查看收集器的狀態，並選擇資料收集方法，如下列主題所述。

主題

- 收集器狀態
- 資料收集

收集器狀態

收集器狀態為您提供收集器的狀態資訊。收集器名稱、收集器與 AWS 的連線狀態、Migration Hub 主區域和版本。

如果您有 AWS 連線問題，您可能需要編輯 Agentless Collector 組態設定。

若要編輯收集器組態設定，請選擇編輯收集器設定，並遵循中所述的指示編輯 Agentless Collector 設定。

資料收集

在資料收集下，您可以選擇資料收集方法。Application Discovery Service Agentless Collector (Agentless Collector) 目前支援從 VMware VMs和資料庫和分析伺服器收集資料。未來的模組將支援其他虛擬化平台的集合，以及作業系統層級集合。

主題

- VMware vCenter 資料收集
- 資料庫和分析資料收集

VMware vCenter 資料收集

若要從 VMware VMs 收集伺服器庫存、設定檔和使用率資料，請設定與 vCenter 伺服器的連線。若要設定連線，請選擇 VMware vCenter 區段中的設定，並遵循中所述的指示使用 VMware vCenter Agentless Collector 資料收集模組。

設定 vCenter 資料收集之後，您可以從儀表板執行下列動作：

- 檢視資料收集狀態
- 開始資料收集
- 停止資料收集

> **Note**
>
> 在儀表板頁面上，設定 vCenter 資料收集之後，VMware vCenter 區段中的設定按鈕會取代為資料收集狀態資訊、停止資料收集按鈕，以及檢視和編輯按鈕。

資料庫和分析資料收集

您可以在下列兩種模式中執行資料庫和分析資料收集模組。

中繼資料和資料庫容量

資料收集模組會從資料庫和分析伺服器收集結構描述、版本、版本、CPU、記憶體和磁碟容量等資訊。您可以使用此收集的資訊，在 AWS DMS 主控台中運算目標建議。如果您的來源資料庫過度佈建或佈建不足，則目標建議也會過度佈建或佈建不足。

此為預設模式。

中繼資料、資料庫容量和資源使用率

除了中繼資料和資料庫容量資訊之外，資料收集模組還會收集資料庫和分析伺服器 CPU、記憶體和磁碟容量的實際使用率指標。此模式提供比預設模式更準確的目標建議，因為建議是以實際資料庫工作負載為基礎。在此模式中，資料收集模組每分鐘收集一次效能指標。

從資料庫和分析伺服器開始收集中繼資料和效能指標

1. 在資料庫和分析收集器頁面上，選擇導覽窗格中的資料收集。
2. 從資料庫清查清單中，選取要收集中繼資料和效能指標的資料庫和分析伺服器。
3. 選擇執行資料收集。資料收集類型對話方塊隨即開啟。
4. 選擇如何收集資料進行分析。

   如果您選擇中繼資料、資料庫容量和資源使用率選項，則請設定資料收集期間。您可以將資料收集期間設為未來 7 天，或使用 1-60 天的自訂範圍設定。

5. 選擇執行資料收集。資料收集頁面隨即開啟。
6. 選擇收集運作狀態索引標籤，以查看資料收集的狀態。

完成資料收集後，您的資料收集模組會將收集的資料上傳至您的 Amazon S3 儲存貯體。然後，您可以檢視此收集的資料，如 中所述檢視收集的資料。

編輯 Agentless Collector 設定

您在第一次設定 Application Discovery Service Agentless Collector (Agentless Collector) 時設定了收集器，如 中所述設定無代理程式收集器。下列程序說明如何編輯 Agentless Collector 組態設定。

編輯收集器組態設定

- 選擇 Agentless Collector 儀表板上的編輯收集器設定按鈕。

  在編輯收集器設定頁面上，執行下列動作：

  a. 針對收集器名稱，輸入名稱以識別收集器。名稱可以包含空格，但不能包含特殊字元。
  b. 在探索資料的目的地 AWS 帳戶下，輸入 AWS 要指定為目的地帳戶的 AWS 存取金鑰和私密金鑰，以接收收集器探索的資料。如需 IAM 使用者需求的相關資訊，請參閱部署 Application Discovery Service 無代理程式收集器。
     i. 對於AWS 存取金鑰，輸入您指定為目的地 AWS 帳戶之帳戶 IAM 使用者的存取金鑰。
     ii. 對於AWS 私密金鑰，輸入您指定為目的地 AWS 帳戶之帳戶 IAM 使用者的私密金鑰。
  c. 在 Agentless Collector 密碼下，變更密碼以用來驗證對 Agentless Collector 的存取。
     i. 針對 Agentless Collector 密碼，輸入用來驗證 Agentless Collector 存取的密碼。
     ii. 對於重新輸入 Agentless Collector 密碼，請再次輸入密碼以進行驗證。
  d. 選擇儲存組態。

接下來，您將看到 Agentless Collector 儀表板。

編輯 VMware vCenter 登入資料

若要從 VMware VMs 收集伺服器庫存、設定檔和使用率資料，請設定與 vCenter 伺服器的連線。如需有關設定 VMware vCenter 連線的資訊，請參閱 使用 VMware vCenter Agentless Collector 資料收集模組。

本節說明如何編輯 vCenter 憑證。

> **Note**
>
> 在編輯 vCenter 登入資料之前，請確定您可以使用系統群組的讀取和檢視許可集來提供 vCenter 登入資料。

編輯 VMware vCenter 登入資料

在頁面上檢視 VMware 資料收集詳細資訊，選擇編輯 vCenter 伺服器。

- 在編輯 vCenter 頁面上，執行下列動作：
  a. 在 vCenter 登入資料下：
     i. 針對 vCenter URL/IP，輸入 VMware vCenter Server 主機的 IP 地址。
     ii. 在 vCenter Username (vCenter 使用者名稱) 中輸入連接器用來與 vCenter 通訊的本機或網域使用者的名稱。網域使用者使用的格式為 domain\username 或 username@domain。
     iii. 在 vCenter Password (vCenter 密碼) 中輸入本機或網域使用者的密碼。
  b. 選擇 Save (儲存)。

手動更新 Application Discovery Service Agentless Collector

當您設定 Application Discovery Service Agentless Collector (Agentless Collector) 時，您可以選擇啟用自動更新，如 中所述設定無代理程式收集器。如果您未啟用自動更新，則需要手動更新 Agentless Collector。

下列程序說明如何手動更新 Agentless Collector。

手動更新 Agentless Collector

1. 取得最新的 Agentless Collector Open Virtualization Archive (OVA) 檔案。
2. （選用）建議您先刪除先前的 Agentless Collector OVA 檔案，再部署最新的檔案。
3. 請遵循 中的步驟部署 Agentless Collector。

先前的程序只會更新 Agentless Collector。您有責任將作業系統保持在最新狀態。

更新您的 Amazon EC2 執行個體

1. 從 VMware vCenter 取得 Agentless Collector 的 IP 地址。
2. 開啟收集器的 VM 主控台**ec2-user**，並使用密碼以 登入**collector**，如下列範例所示。

```
username: ec2-user
password: collector
```

3. 請遵循 Amazon Linux AL2 使用者指南中 AL2 執行個體上的更新執行個體軟體中的指示。

核心即時修補

Agentless Collector version 2

Agentless Collector 第 2 版虛擬機器使用 Amazon Linux 2023，如中所述部署 Agentless Collector。

若要啟用和使用適用於 Amazon Linux 2023 的即時修補，請參閱《Amazon EC2 使用者指南》中的 AL2023 上的核心即時修補。 Amazon EC2

Agentless Collector version 1

Agentless Collector 第 1 版虛擬機器使用 Amazon Linux 2，如中所述部署 Agentless Collector。

若要啟用和使用適用於 Amazon Linux 2 的即時修補，請參閱《Amazon EC2 使用者指南》中的 AL2 上的核心即時修補。 Amazon EC2

從 Agentless Collector 第 1 版升級至第 2 版

1. 使用最新的映像安裝新的 Agentless Collector OVA。
2. 設定登入資料。
3. 刪除舊的虛擬設備。

對 Agentless Collector 進行故障診斷

本節包含的主題可協助您疑難排解 Application Discovery Service Agentless Collector (Agentless Collector) 的已知問題。

主題

修正 **Unable to retrieve manifest or certificate file error**

如果您在 VMware vCenter UI 中嘗試從 Amazon S3 URL 部署 OVA 時收到此錯誤，請確定您的 vCenter 伺服器符合下列要求：

- VMware vCenter Server 8.0 版更新 1 或更新版本
- VMware vCenter Server 7.0 Update 3q (ISO Build 23788036) 或更新版本

在設定 WinRM 憑證時解決自我簽署的憑證問題

如果您啟用 WinRM 憑證檢查，您可能需要將自我簽署的憑證授權機構匯入無代理程式收集器。

匯入自我簽署憑證授權機構

1. 在 VMware vCenter 中開啟收集器的 VM Web 主控台`ec2-user`，並以密碼登入`collector`，如下列範例所示。

   ```
   username: ec2-user
   password: collector
   ```

2. 確定用於簽署 WinRM 憑證的每個自我簽署 CA 憑證都位於目錄 下`/etc/pki/ca-trust/source/anchors`。例如：

```
/etc/pki/ca-trust/source/anchors/https-winrm-ca-1.pem
```

3. 若要安裝新的憑證，請執行下列命令。

```
sudo update-ca-trust
```

4. 執行下列命令以重新啟動 Agentless Collector

```
sudo shutdown -r now
```

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 | less
```

修正無代理程式收集器在設定 AWS 期間無法連線

Agentless Collector 需要透過 TCP 連接埠 443 對多個 AWS 網域進行傳出存取。在主控台中設定 Agentless Collector 時，您可能會收到下列錯誤訊息。

> 無法連線 AWS
>
> AWS 無法連線。請確認網路設定。

發生此錯誤是因為 Agentless Collector 在設定程序期間嘗試建立 HTTPS 連線到收集器需要與之通訊的 AWS 網域失敗。如果無法建立連線， Agentless Collector 組態會失敗。

修正 的連線 AWS

1. 請洽詢您的 IT 管理員，了解貴公司防火牆是否封鎖連接埠 443 上需要傳出存取的任何 AWS 網域的傳出流量。哪些 AWS 網域需要傳出存取權取決於您的主區域是美國西部（奧勒岡）區域、us-west-2 還是某些其他區域。

   如果 AWS 您的帳戶主區域是 us-west-2，以下網域需要傳出存取權：

   - `arsenal-discovery.us-west-2.amazonaws.com`
   - `migrationhub-config.us-west-2.amazonaws.com`
   - `api.ecr-public.us-east-1.amazonaws.com`

- public.ecr.aws

如果 AWS 您的帳戶主區域不是 ，則下列網域需要傳出存取權**us-west-2**：

- arsenal-discovery.us-west-2.amazonaws.com
- arsenal-discovery.*your-home-region*.amazonaws.com
- migrationhub-config.us-west-2.amazonaws.com
- api.ecr-public.us-east-1.amazonaws.com
- public.ecr.aws

如果您的防火牆封鎖對 Agentless Collector 需要與之通訊的 AWS 網域的傳出存取，請在收集器組態下的資料同步區段中設定代理主機。

2. 如果更新防火牆無法解決連線問題，請使用下列步驟，以確保收集器虛擬機器與上一個步驟中列出的網域具有傳出網路連線。

   a. 從 VMware vCenter 取得 Agentless Collector 的 IP 地址。

   b. 開啟收集器的 VM Web 主控台**ec2-user**，並使用密碼以 登入**collector**，如下列範例所示。

   ```
   username: ec2-user
   password: collector
   ```

   c. 在連接埠 443 上執行 telnet 來測試與所列網域的連線，如下列範例所示。

   ```
   telnet migrationhub-config.us-west-2.amazonaws.com 443
   ```

3. 如果 telnet 無法解析網域，請嘗試使用 Amazon Linux 2 的指示來設定靜態 DNS 伺服器。
4. 如果錯誤持續發生，如需進一步支援，請參閱聯絡 AWS Support for Agentless Collector 問題。

修正連線至代理主機時的自我簽署憑證問題

如果與選擇性提供的代理通訊是透過 HTTPS 進行，且代理具有自我簽署憑證，您可能需要提供憑證。

1. 從 VMware vCenter 取得 Agentless Collector 的 IP 地址。
2. 開啟收集器的 VM Web 主控台ec2-user，並使用密碼登入collector，如下列範例所示。

```
username: ec2-user
password: collector
```

3. 將與安全代理相關聯的憑證內文，包括 -----BEGIN CERTIFICATE-----和 -----END CERTIFICATE-----，貼到下列檔案中：

```
/etc/pki/ca-trust/source/anchors/https-proxy-ca.pem
```

4. 若要安裝新憑證，請執行下列命令：

```
sudo update-ca-trust
```

5. 執行下列命令以重新啟動 Agentless Collector：

```
sudo shutdown -r now
```

尋找運作狀態不佳的收集器

您可以在 AWS Migration Hub （遷移中樞） 主控台的資料收集器頁面上找到每個收集器的狀態資訊。您可以透過尋找狀態為需要注意的任何收集器來識別具有問題的收集器。

下列程序說明如何存取 Agentless Collector 主控台來識別運作狀態問題。

存取 Agentless Collector 主控台

1. 使用 AWS 您的帳戶登入 ， AWS Management Console 並在 https：//https://console.aws.amazon.com/migrationhub/ 開啟 Migration Hub 主控台。
2. 在遷移中樞主控台導覽窗格的探索下，選擇資料收集器。
3. 從 Agentless 收集器索引標籤中，記下狀態為 需要注意的每個連接器的 IP 地址。
4. 若要開啟 Agentless Collector 主控台，請開啟 Web 瀏覽器。然後在地址列中輸入下列 URL：**https://***<ip_address>***/**，其中 ip_address 是運作狀態不佳收集器的 IP 地址。
5. 選擇登入，然後輸入在 中設定收集器時所設定的無代理程式收集器密碼設定無代理程式收集器。
6. 在 Agentless Collector 儀表板頁面的資料收集下，選擇 VMware vCenter 區段中的檢視和編輯。
7. 請遵循 中的指示編輯 VMware vCenter 登入資料來更正 URL 和登入資料。

修正運作狀態問題後，收集器會重新建立與 vCenter 伺服器的連線，而收集器的狀態會變更為收集狀態。如果問題仍然存在，請參閱 聯絡 AWS Support for Agentless Collector 問題。

造成收集器運作狀態不佳的最常見原因是 IP 地址和登入資料問題。 修正 IP 地址問題 修正 vCenter 登入資料問題可協助您解決這些問題，並將收集器恢復為運作狀態。

修正 IP 地址問題

如果收集器設定期間提供的 vCenter 端點格式錯誤、無效，或 vCenter 伺服器目前已關閉且無法連線，收集器可能會進入運作狀態不良。在這種情況下，您會收到連線錯誤訊息 。

下列程序可協助您解決 IP 位址問題。

修正收集器 IP 地址問題

1. 從 VMware vCenter 取得 Agentless Collector 的 IP 地址。
2. 開啟 Web 瀏覽器來開啟 Agentless Collector 主控台，然後在地址列中輸入下列 URL：**`https://`***`<ip_address>`***`/`**，其中 ip_address 是來自 的收集器 IP 地址部署 Agentless Collector。
3. 選擇登入，然後輸入在 中設定收集器時所設定的無代理程式收集器密碼設定無代理程式收集器。
4. 在 Agentless Collector 儀表板頁面的資料收集下，選擇 VMware vCenter 區段中的檢視和編輯。
5. 在 VMware 資料收集詳細資訊頁面的探索 vCenter 伺服器下，記下 vCenter 欄中的 IP 地址。
6. 使用 `ping`或 等個別命令列工具`traceroute`，驗證相關聯的 vCenter 伺服器是否作用中，以及可從收集器 VM 連線 IP。

   - 如果 IP 地址不正確且 vCenter 服務處於作用中狀態，請在收集器主控台中更新 IP 地址，然後選擇下一步。
   - 如果 IP 位址正確，但 vCenter 伺服器處於非作用中狀態，請啟動伺服器。
   - 如果 IP 位址正確且 vCenter 伺服器處於作用中狀態，請檢查是否因為防火牆問題而封鎖連入網路連線。如果是，請更新您的防火牆設定，以允許來自收集器 VM 的傳入連線。

修正 vCenter 登入資料問題

如果設定收集器時提供的 vCenter 使用者憑證無效，或沒有 vCenter 讀取和檢視帳戶權限，收集器可能會進入運作狀態不良。

如果您遇到與 vCenter 登入資料相關的問題，請檢查 以確保您已為系統群組設定 vCenter 讀取和檢視許可。

如需有關編輯 vCenter 登入資料的資訊，請參閱 編輯 VMware vCenter 登入資料。

修正資料庫和分析資料收集模組中的資料轉送問題

Agentless Collector 中資料庫和分析資料收集模組的首頁會顯示存取 DMS 和存取 S3 的連線狀態。如果您看到無法存取 DMS 和存取 S3，請設定資料轉送。如需詳細資訊，請參閱設定資料轉送。

如果您在設定資料轉送之後遇到此問題，請檢查 ，以確定您的資料收集模組可以存取網際網路。然後，請確定您已將 DMSCollectorPolicy 和 FleetAdvisorS3Policy 政策新增至您的 IAM 使用者。如需詳細資訊，請參閱部署 Application Discovery Service 無代理程式收集器。

如果您的資料收集模組無法連線至 AWS，則 會提供對下列網域的傳出存取權。

- dms.*your-home-region*.amazonaws.com
- s3.amazonaws.com

修正資料庫和分析資料收集模組中的連線問題

Agentless Collector 中的資料庫和分析資料收集模組會連線至您的 LDAP 伺服器，以探索資料環境中的作業系統伺服器。然後，資料收集模組會連線至您的作業系統伺服器，以探索資料庫和分析伺服器。從這些資料庫伺服器，資料收集模組會收集容量和效能指標。如果您的資料收集模組無法連線至這些伺服器，請確認您可以連線至您的伺服器。

在下列範例中，將*###*的值取代為您的值。

- 若要驗證您可以連線至 LDAP 伺服器，請安裝 `ldap-util`套件。若要這麼做，請執行下列命令。

  ```
  sudo apt-get install ldap-util
  ```

  然後執行以下命令。

  ```
  ldapsearch -x -D "CN=user,CN=Users,DC=example,DC=com" -w "password" -b
   "dc=example,dc=com" -h
  ```

- 若要驗證您可以連線至 Linux 作業系統伺服器，請使用下列命令。

  ```
  ssh -i C:\Users\user\private_key.pem -p 22 username@my-linux-host.domain.com
  ```

  在 Windows 中以管理員身分執行先前的範例。

```
ssh username@my-linux-host.domain.com
```

在 Linux 中執行先前的範例。

- 若要驗證您可以連線至 Windows 作業系統伺服器，請使用下列命令。

```
winrs -r:[hostname or ip] -u:username -p:password cmd
```

在 Windows 中以管理員身分執行先前的範例。

```
sudo apt install -y winrm
winrm --user=username --password=password [http or https]://[hostname or ip]:[port]
 "[cmd.exe or any other CLI command]"
```

在 Linux 中執行先前的範例。

- 若要驗證您可以連線至 SQL Server 資料庫，請使用下列命令。

```
sqlcmd -S [hostname or IP] -U username -P 'password'
SELECT GETDATE() AS sysdate
```

- 若要驗證您可以連線至 MySQL 資料庫，請使用下列命令。

```
mysql -u username -p 'password' -h [hostname or IP] -P [port]
SELECT NOW() FROM DUAL
```

- 若要驗證您可以連線至 Oracle 資料庫，請使用下列命令。

```
sqlplus username/password@[hostname or IP]:port/servicename
SELECT SYSDATE FROM DUAL
```

- 若要驗證您可以連線至 PostgreSQL 資料庫，請使用下列命令。

```
psql -U username -h [hostname or IP] -p port -d database
SELECT CURRENT_TIMESTAMP AS sysdate
```

如果您無法連線至資料庫和分析伺服器，請確定您提供必要的許可。如需詳細資訊，請參閱探索您的資料庫伺服器。

獨立 ESX 主機支援

Agentless Collector 不支援獨立的 ESX 主機。ESX 主機必須屬於 vCenter Server 執行個體的一部分。

聯絡 AWS Support for Agentless Collector 問題

如果您遇到 Application Discovery Service Agentless Collector (Agentless Collector) 問題，且需要協助，請聯絡 AWS Support 系統會與您聯絡，並可能要求您傳送收集器日誌。

取得 Agentless Collector 日誌

1. 從 VMware vCenter 取得 Agentless Collector 的 IP 地址。
2. 開啟收集器的 VM Web 主控台**ec2-user**，並使用密碼以 登入**collector**，如下列範例所示。

```
username: ec2-user
password: collector
```

3. 使用以下命令導覽至日誌資料夾。

```
cd /var/log/aws/collector
```

4. 使用以下命令壓縮日誌檔案。

```
sudo cp /local/agentless_collector/compose.log .
docker inspect $(docker ps --format {{.Names}}) | sudo tee docker_inspect.log >/
dev/null
sudo tar czf logs_$(date '+%d-%m-%Y_%H.%M.%S').tar.gz --exclude='db.mv*' *
```

5. 從 Agentless Collector VM 複製日誌檔案。

```
scp logs*.tar.gz targetuser@targetaddress
```

6. 將tar.gz檔案提供給 AWS 企業支援。

將資料匯入 Migration Hub

AWS Migration Hub (Migration Hub) 匯入可讓您直接將內部部署環境的詳細資訊匯入 Migration Hub，而無需使用 Application Discovery Service Agentless Collector (Agentless Collector) 或 AWS Application Discovery Agent (Discovery Agent)，因此您可以直接從匯入的資料執行遷移評估和規劃。您也可以將裝置群組為應用程式並追蹤其遷移狀態。

此頁面說明完成匯入請求的步驟。首先，您可以使用下列兩個選項之一來準備您的現場部署伺服器資料。

- 使用常見的第三方工具來產生包含您內部部署伺服器資料的檔案。
- 下載逗號分隔值 (CSV) 匯入範本，並填入您的內部部署伺服器資料。

使用上述兩種方法來建立內部部署資料檔案之後，您可以使用 Migration Hub 主控台 AWS CLI或其中一個 AWS SDKs，將檔案上傳至 Migration Hub。如需兩個選項的詳細資訊，請參閱 the section called “支援的匯入格式”。

您可以提交多個匯入請求。每個請求都會循序處理。您可以透過主控台或匯入 API 隨時檢查匯入請求的狀態。

匯入請求完成後，您可以檢視個別匯入記錄的詳細資訊。直接從 Migration Hub 主控台檢視使用率資料、標籤和應用程式映射。如果匯入時遇到錯誤，您可以檢閱成功與失敗記錄的計數，以及查看各個失敗記錄的錯誤詳細資訊。

處理錯誤：已提供連結來下載錯誤日誌和失敗的記錄檔案，此檔案為 CSV 檔案的壓縮存檔。在修正錯誤之後，使用這些檔案重新提交匯入請求。

數量限制適用於匯入的記錄、匯入的伺服器和可保留的刪除記錄。如需詳細資訊，請參閱AWS Application Discovery Service 配額。

支援的匯入格式

Migration Hub 支援下列匯入格式。

- RVTools
- Migration Hub 匯入範本

RVTools

Migration Hub 支援透過 RVTools 匯入 VMware vSphere 的匯出。從 RVTools 儲存資料時，請先選擇全部匯出至 csv 選項或全部匯出至 Excel 選項，然後 ZIP 資料夾，然後將 ZIP 檔案匯入 Migration Hub。ZIP 中需要下列檔案：vInfo、vNetwork、vCpu、vMemory、vDisk、vPartition、vSource、vTools、vHost、vNic、vSC_VMK。

Migration Hub 匯入範本

Migration Hub 匯入可讓您從任何來源匯入資料。提供的資料必須是 CSV 檔案支援的格式，而且資料必須只包含支援的欄位以及這些欄位支援的範圍。

下表中匯入欄位名稱旁的星號 (*) 表示它是必要欄位。您的匯入檔案的每個記錄皆至少必須填入一或多個這些必要欄位，以唯一識別伺服器或應用程式。否則，沒有任何必要欄位的記錄將無法匯入。

下表中匯入存檔名稱旁的插入符號 (^) 表示如果提供 serverId，則它是唯讀的。

> **Note**
>
> 如果您是使用 VMware.MoRefId 或 VMWare.VCenterId 來識別記錄，您必須在相同的記錄中有這兩個欄位。

匯入欄位名稱	描述	範例
ExternalId*^	自訂的識別符，可讓您將每個記錄標示為唯一。例如，ExternalId (ExternalId) 可以是您資料中心伺服器的庫存 ID。	Inventory Id 1 Server 2 CMBD Id 3
SMBiosId^	系統管理 BIOS (SMBIOS) ID。	
IPAddress*^	以逗號分隔的伺服器 IP 地址清單，以引號括住。	192.0.0.2 "10.12.31.233, 10.12.32.11"
MACAddress*^	以逗號分隔的伺服器 MAC 地址清單，以引號括住。	00:1B:44:11:3A:B7

匯入欄位名稱	描述	範例
		"00-15-E9-2B-99-3C, 00-14-22-01-23-45"
HostName*^	伺服器的主機名稱。我們建議此值應使用完整網域名稱 (FQDN)。	ip-1-2-3-4 localhost.domain
VMware.MoRefId*^	受管物件參考 ID。必須以 VMware.VCenterId 提供。	
VMware.VCenterId*^	虛擬機器唯一識別符。必須以 VMware.MoRefId 提供。	
CPU.NumberOfProcessors^	CPU 的數量。	4
CPU.NumberOfCores^	實體核心總數。	8
CPU.NumberOfLogicalCores^	可在伺服器中所有 CPUs 同時執行的執行緒總數。部分 CPU 可在單一 CPU 核心上同時執行多個執行緒。在這些情況下，此值會大於實體 (或虛擬) 核心的數量。	16
OS.Name^	作業系統的名稱。	Linux Windows.Hat
OS.Version^	作業系統的版本。	16.04.3 NT 6.2.8
VMware.VMName^	虛擬機器的名稱。	Corp1
RAM.TotalSizeInMB^	伺服器上可用的 RAM 總量，以 MB 為單位。	64 128

匯入欄位名稱	描述	範例
RAM.UsedSizeInMB.Avg^	伺服器上已用記憶體的平均數量，以 MB 為單位。	64 128
RAM.UsedSizeInMB.Max^	伺服器上可用的已用 RAM 數量上限，以 MB 為單位。	64 128
CPU.UsagePct.Avg^	當探索工具收集資料時的平均 CPU 使用率。	45 23.9
CPU.UsagePct.Max^	當探索工具收集資料時的最大 CPU 使用率。	55.34 24
DiskReadsPerSecondInKB.Avg^	磁碟平均每秒讀取的數目，以 KB 為單位。	1159 84506
DiskWritesPerSecondInKB.Avg^	磁碟平均每秒寫入的數目，以 KB 為單位。	199 6197
DiskReadsPerSecondInKB.Max^	磁碟最大每秒讀取的數目，以 KB 為單位。	37892 869962
DiskWritesPerSecondInKB.Max^	磁碟最大每秒寫入的數目，以 KB 為單位。	18436 1808
DiskReadsOpsPerSecond.Avg^	每秒磁碟讀取操作的平均數目。	45 28
DiskWritesOpsPerSecond.Avg^	磁碟寫入 操作的每秒平均次數。	8 3

匯入欄位名稱	描述	範例
DiskReadsOpsPerSecond.Max^	磁碟每秒讀取操作的最大數目。	1083 176
DiskWritesOpsPerSecond.Max^	磁碟寫入操作的每秒最大次數。	535 71
NetworkReadsPerSecondInKB.Avg^	網路讀取操作的每秒平均數量，以 KB 為單位。	45 28
NetworkWritesPerSecondInKB.Avg^	網路寫入操作的每秒平均數量，以 KB 為單位。	8 3
NetworkReadsPerSecondInKB.Max^	網路讀取操作的每秒最大數量，以 KB 為單位。	1083 176
NetworkWritesPerSecondInKB.Max^	網路寫入操作的每秒最大數量，以 KB 為單位。	535 71
應用程式	以逗號分隔之包含此伺服器的應用程式清單，以引號括住。此值可包含現有應用程式和/或匯入時建立的新應用程式。	Application1 "Application2, Application3"
ApplicationWave	此伺服器的遷移波動。	

匯入欄位名稱	描述	範例
標籤^	以逗號分隔的標籤清單，格式為「名稱:值」。 **Important** 請不要將敏感資訊 (例如個人資料) 儲存在標籤中。	"zone:1, critical:yes" "zone:3, critical:no, zone:1"
ServerId	如 Migration Hub 伺服器清單中顯示的伺服器識別符。	`d-server-01kk9i6ywwaxmp`

您可以匯入資料，即使您沒有將資料填入匯入範本中定義的所有欄位，只要每個記錄中至少有一個必要的欄位即可。透過使用外部或內部相符金鑰，以管理多個匯入請求中的重複項目。如果您填入自己的相符金鑰 `External ID`，此欄位將用於唯一識別和匯入記錄。若未指定相符金鑰，匯入作業將使用內部產生的相符金鑰，它來自於匯入範本的一些資料欄。如需此比對的詳細資訊，請參閱[將邏輯與探索的伺服器和應用程式配對]。

Note

Migration Hub 匯入不支援匯入範本中定義欄位以外的任何欄位。任何自訂的欄位都將被忽略，因此不會匯入。

設定匯入許可

在您可以匯入資料之前，請確定您的 IAM 使用者具有必要的 Amazon S3 許可，可將您的匯入檔案上傳 (`s3:PutObject`) 至 Amazon S3，以及讀取物件 (`s3:GetObject`)。您也必須建立 IAM 政策，並將其連接至在您 AWS 帳戶中執行匯入的 IAM 使用者，以建立程式設計存取 （ 適用於 AWS CLI) 或主控台存取。

Console Permissions

使用下列程序來編輯 IAM 使用者的許可政策，該使用者將使用 主控台在您的 AWS 帳戶中提出匯入請求。

編輯使用者連接的受管政策

1. 登入 AWS Management Console ，並在 https://console.aws.amazon.com/iam/：//www. 開啟 IAM 主控台。
2. 在導覽窗格中，選擇 Users (使用者)。
3. 選擇您想要為其變更許可政策的使用者名稱。
4. 選擇 Permissions (許可) 索引標籤，然後選擇 Add permissions (新增許可)。
5. 選擇 Attach existing policies directly (直接連接現有政策)，然後選擇 Create policy (建立政策)。

   a. 在開啟的 Create policy (建立政策) 頁面上，選擇 JSON (JSON) 並貼上以下政策。請記得將您儲存貯體的名稱，更換為 IAM 使用者將上傳檔案之儲存貯體的實際名稱。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": ["s3:ListBucket"],
      "Resource": ["arn:aws:s3:::importBucket"]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource": ["arn:aws:s3:::importBucket/*"]
    }
  ]
}
```

b. 選擇檢閱政策。

c. 為您的政策指定新的 Name (名稱) 和選用描述，然後檢閱政策的摘要。

d. 選擇建立政策。

6. 返回授予許可 IAM 主控台頁面，供將在您的帳戶 AWS 中提出匯入請求的使用者使用。
7. 重新整理政策表，並搜尋您剛建立的政策名稱。
8. 選擇下一步：檢閱。
9. 選擇新增許可。

現在您已將政策新增至 IAM 使用者，即可開始匯入程序。

AWS CLI Permissions

使用下列程序建立必要的受管政策，以授予 IAM 使用者使用 提出匯入資料請求的許可 AWS CLI。

建立和連接 受管政策

1. 使用 `aws iam create-policy` AWS CLI 命令建立具有下列許可的 IAM 政策。請記得將您儲存貯體的名稱，更換為 IAM 使用者將上傳檔案之儲存貯體的實際名稱。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["s3:ListBucket"],
      "Resource": ["arn:aws:s3:::importBucket"]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource": ["arn:aws:s3:::importBucket/*"]
    }
  ]
}
```

如需使用此命令的詳細資訊，請參閱《 AWS CLI 命令參考》中的 create-policy。

2. 使用 `aws iam create-policy` AWS CLI 命令建立具有下列許可的其他 IAM 政策。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "discovery:ListConfigurations",
                "discovery:CreateApplication",
                "discovery:UpdateApplication",
                "discovery:AssociateConfigurationItemsToApplication",
                "discovery:DisassociateConfigurationItemsFromApplication",
                "discovery:GetDiscoverySummary",
                "discovery:StartImportTask",
                "discovery:DescribeImportTasks",
                "discovery:BatchDeleteImportData"
            ],
            "Resource": "*"
        }
    ]
}
```

3. 使用 `aws iam attach-user-policy` AWS CLI 命令，將您在前兩個步驟中建立的政策連接到將使用 在您的 AWS 帳戶中執行匯入請求的 IAM 使用者 AWS CLI。如需使用此命令的詳細資訊，請參閱《 AWS CLI 命令參考》中的 attach-user-policy。

現在您已將政策新增至 IAM 使用者，即可開始匯入程序。

請記住，當 IAM 使用者將物件上傳到您指定的 Amazon S3 儲存貯體時，他們必須保留物件的預設許可集，以便使用者可以讀取物件。

將匯入檔案上傳至 Amazon S3

接下來，您必須將 CSV 格式的匯入檔案上傳至 Amazon S3，以便匯入檔案。開始之前，您應該有一個 Amazon S3 儲存貯體，該儲存貯體會事先建立和/或選擇匯入檔案。

Console S3 Upload

將匯入檔案上傳至 Amazon S3

1. 登入 AWS Management Console ，並在 https：//Amazon S3 主控台開啟 https：//https://console.aws.amazon.com/s3/。
2. 在 Bucket name (儲存貯體名稱) 清單中，選擇您要上傳物件的目標儲存貯體名稱。
3. 選擇上傳。
4. 在 Upload (上傳) 對話方塊中，選擇 Add files (新增檔案) 來選擇要上傳的檔案。
5. 選擇要上傳的檔案，然後選擇 Open (開啟)。
6. 選擇上傳。
7. 上傳您的檔案之後，請從您的儲存貯體儀表板選擇資料檔案物件的名稱。
8. 從物件詳細資訊頁面的 Overview (概觀) 索引標籤，複製 Object URL (物件 URL)。您在建立匯入請求時，將需要用到此 URL。
9. 前往 Migration Hub 主控台中的匯入頁面，如 中所述匯入 資料。然後，將物件 URL 貼到 Amazon S3 物件 URL 欄位中。

AWS CLI S3 Upload

將匯入檔案上傳至 Amazon S3

1. 開啟終端機視窗並導覽至匯入檔案儲存的目標目錄。
2. 輸入以下命令：

```
aws s3 cp ImportFile.csv s3://BucketName/ImportFile.csv
```

3. 這會傳回下列結果：

```
upload: .\ImportFile.csv to s3://BucketName/ImportFile.csv
```

4. 複製傳回的完整 Amazon S3 物件路徑。建立匯入請求時，您將需要此項目。

匯入 資料

從 Migration Hub 主控台下載匯入範本，並填入現有的現場部署伺服器資料之後，您就可以開始將資料匯入 Migration Hub。下列指示說明兩種方法，使用 主控台或透過 進行 API 呼叫 AWS CLI。

Console Import

在 Migration Hub 主控台的工具頁面上開始資料匯入。

開始匯入資料

1. 在導覽窗格中的 Discover (探索) 下，選擇 Tools (工具)。
2. 如果您尚未填寫匯入範本，您可以在匯入方塊中選擇匯入範本來下載範本。開啟下載範本並填入您現有的現場部署伺服器資料。您也可以從 Amazon S3 儲存貯體下載匯入範本，網址為 https：//https：//https://s3.us-west-2.amazonaws.com/templates-7cffcf56-bd96-4b1c-b45b-a5b42f282e46/import_template.csv..
3. 若要開啟匯入頁面，請在匯入方塊中選擇匯入。
4. 在匯入名稱下，指定匯入的名稱。
5. 填寫 Amazon S3 物件 URL 欄位。若要執行此步驟，您需要將匯入資料檔案上傳至 Amazon S3。如需詳細資訊，請參閱將匯入檔案上傳至 Amazon S3。
6. 選擇右下區域中的 Import (匯入)。這將開啟 Imports (匯入) 頁面，您可在此查看以表格列出的您的匯入和其狀態。

按照前述程序開始匯入資料之後，Imports (匯入) 頁面會顯示每個匯入請求的詳細資訊，包括其進度狀態、完成時間，以及成功或失敗記錄的數量，並可下載這些記錄。在此畫面中，您也可以導覽至探索下的伺服器頁面，以查看實際匯入的資料。

在 Servers (伺服器) 頁面上，您可以查看所有已探索到的伺服器 (裝置) 及匯入名稱。當您選取名稱欄中列出的匯入名稱，從匯入 （ 匯入歷史記錄 ） 頁面導覽時，系統會將您導向伺服器頁面，其中會根據選取的匯入資料集套用篩選條件。然後，您只會看到屬於該特定匯入的資料。

詞存檔為 .zip 格式，並包含兩個檔案；`errors-file` 以及 `failed-entries-file`。此錯誤檔案包含與每個失敗行關聯的錯誤訊息，以及您匯入失敗的資料檔案的關聯欄位名稱。您可以使用此檔案快速識別哪裡發生問題。失敗的項目檔案包含失敗的每個行和所有提供的欄位。您可以在此檔案變更錯誤檔案中標示的部分，並再次嘗試匯入已修正資訊的檔案。

AWS CLI Import

若要從 開始資料匯入程序 AWS CLI， AWS CLI 必須先在您的環境中安裝 。如需詳細資訊，請參閱AWS Command Line Interface 《 使用者指南》中的安裝 AWS 命令列界面。

> **Note**
>
> 如果您尚未填寫匯入範本，您可以從我們的 Amazon S3 儲存貯體下載匯入範本，網址為：https：//https://s3.us-west-2.amazonaws.com/templates-7cffcf56-bd96-4b1c-b45b-a5b42f282e46/import_template.csv

開始匯入資料

1. 請開啟終端機視窗並輸入下列命令：

```
aws discovery start-import-task --import-url s3://BucketName/ImportFile.csv --
name ImportName
```

2. 這會建立匯入任務，並傳回以下狀態資訊：

```
{
    "task": {
        "status": "IMPORT_IN_PROGRESS",
        "applicationImportSuccess": 0,
        "serverImportFailure": 0,
        "serverImportSuccess": 0,
        "name": "ImportName",
        "importRequestTime": 1547682819.801,
        "applicationImportFailure": 0,
        "clientRequestToken": "EXAMPLE1-abcd-1234-abcd-EXAMPLE1234",
        "importUrl": "s3://BucketName/ImportFile.csv",
        "importTaskId": "import-task-EXAMPLE1229949eabfEXAMPLE03862c0"
    }
}
```

追蹤您的 Migration Hub 匯入請求

您可以使用 主控台 AWS CLI或其中一個 AWS SDKs 來追蹤 Migration Hub 匯入請求的狀態。

Console Tracking

從 Migration Hub 主控台的匯入儀表板，您會找到下列元素。

- 名稱 – 匯入請求的名稱。

- 匯入 ID – 匯入請求的唯一 ID。
- 匯入時間 – 建立匯入請求的日期和時間。
- 匯入狀態 – 匯入請求的狀態。這可以是下列其中一個值：
  - 匯入 – 目前正在匯入此資料檔案。
  - 已匯入 – 已成功匯入整個資料檔案。
  - 匯入時發生錯誤 – 資料檔案中的一或多個記錄無法匯入。若要解決您的失敗記錄，請為您的匯入任務選擇 Download failed records (下載失敗紀錄)，解決失敗項目 csv 檔案中的錯誤之後再次執行匯入。
  - 匯入失敗 – 匯入資料檔案中沒有記錄。若要解決您的失敗記錄，請為您的匯入任務選擇 Download failed records (下載失敗紀錄)，解決失敗項目 csv 檔案中的錯誤之後再次執行匯入。
- 匯入的記錄 – 特定資料檔案中已成功匯入的記錄數目。
- 失敗的記錄 – 未匯入的特定資料檔案中的記錄數目。

CLI Tracking

您可以使用 `aws discovery describe-import-tasks` AWS CLI 命令追蹤匯入任務的狀態。

1. 請開啟終端機視窗並輸入下列命令：

   ```
   aws discovery describe-import-tasks
   ```

2. 這將以 JSON 格式傳回您所有匯入任務的清單，並包含狀態和其他相關資訊。或者，您可以篩選結果以傳回部分的匯入任務。

在追蹤您的匯入任務時，您可能會發現傳回的 `serverImportFailure` 值大於 0。發生此情況時，表示您的匯入檔案有一或多個項目無法匯入。您可以下載失敗記錄存檔，檢閱其中的檔案，然後以修改後的 failed-entries.csv 檔案再次執行匯入請求，即可解決此問題。

建立匯入任務後，您可以執行其他動作，以協助管理和追蹤您的資料遷移。例如，您可以下載特定請求的失敗記錄存檔。如需有關使用失敗記錄存檔解決匯入問題的詳細資訊，請參閱對失敗的匯入記錄進行故障診斷。

檢視和探索探索探索的資料

Application Discovery Service Agentless Collector (Agentless Collector) 和 AWS Discovery Agent (Discovery Agent) 都會根據平均和尖峰使用率提供系統效能資料。您可以使用所收集的系統效能資料，來執行高階總擁有成本 (TCO)。Discovery Agents 會收集更詳細的資料，包括系統效能資訊的時間序列資料、傳入和傳出網路連線，以及在伺服器上執行的程序。您可以使用此資料來以了解伺服器之間的網路相依性，並將相關伺服器分組為應用程式以利遷移規劃。

在本節中，您將找到如何從主控台和 中檢視和使用 Agentless Collector 和 Discovery Agent 發現的資料的說明 AWS CLI。

主題

使用 Migration Hub 主控台檢視收集的資料

對於 Application Discovery Service Agentless Collector (Agentless Collector) 和 AWS Discovery Agent (Discovery Agent)，在資料收集程序開始之後，您可以使用 主控台檢視其收集的伺服器和VMs資料。資料收集開始後約 15 分鐘，資料會出現在主控台中。您也可以透過使用 匯出 API 呼叫，以 CSV 格式檢視此資料 AWS CLI。

若要在 主控台中檢視有關已發現伺服器所收集的資料，請遵循 中的步驟在 AWS Migration Hub 主控台中檢視伺服器。若要進一步了解如何使用主控台來檢視、排序和標記 Agentless Collector 或 Discovery Agents 發現的伺服器，請參閱 使用 AWS Migration Hub 主控台探索資料。

Agentless Collector 資料庫和分析資料收集模組會將收集的資料上傳至 Amazon S3 儲存貯體。您可以在 DMS AWS 主控台中檢視此儲存貯體的資料。若要檢視有關已探索資料庫和分析伺服器的收集資料，請遵循中的步驟檢視收集的資料。

將邏輯與探索的伺服器和應用程式配對

AWS Application Discovery Service （應用程式探索服務） 具有內建比對邏輯，可識別其探索的伺服器何時符合現有項目。當此邏輯找到相符的項目，它會以新的值更新現有已探索到的伺服器的資訊。

此比對邏輯處理來自多個來源的重複伺服器，包括 AWS Migration Hub （遷移中樞） 匯入、Application Discovery Service Agentless Collector (Agentless Collector)、 AWS Application

Discovery Agent (Discovery Agent) 和其他遷移工具。如需 Migration Hub 匯入的詳細資訊，請參閱 Migration Hub 匯入。

當伺服器探索時，每個項目都會與之前匯入的記錄進行交叉檢查，以確保匯入的伺服器尚不存在。如果找不到相符的項目，將會建立新的記錄並指派新的唯一伺服器識別符。如果找到相符的項目，仍然會建立新的項目，但會指派與現有伺服器相同的唯一伺服器識別符。在 Migration Hub 主控台中檢視此伺服器時，您只會找到一個伺服器的唯一項目。

與此項目相關聯的伺服器屬性已完成合併，並可顯示先前可用記錄的屬性值及新匯入記錄的屬性值。如果特定伺服器屬性有來自多個來源的多個值，例如，`Total RAM` 中兩個不同的值與使用匯入及探索代理程式探索到的特定伺服器有關聯，則最近更新的值將顯示於該伺服器的相符記錄中。

相符欄位

在使用探索工具時，以下欄位用於比對伺服器。

- ExternalId – 這是用於比對伺服器的主要欄位。如果此欄位中的值與另一個項目`ExternalId`中的另一個值相同，則 Application Discovery Service 會比對兩個項目，無論其他欄位是否相符。
- IPAddress
- HostName
- MacAddress
- VMware.MoRefId 和 VMware.vCenterId – 這兩個值必須與另一個項目中的個別欄位相同，Application Discovery Service 才能執行比對。

探索 Amazon Athena 中的資料

Amazon Athena 中的資料探索可讓您在一個位置分析 Discovery Agent 從所有探索到的內部部署伺服器收集的資料。一旦從 Migration Hub 主控台 （或使用 StartContinousExport API) 啟用 Amazon Athena 中的資料探勘，並開啟代理程式的資料收集，代理程式所收集的資料會自動定期儲存在 S3 儲存貯體中。如需詳細資訊，請參閱探索 Amazon Athena 中的資料。

Amazon Athena 中的資料探勘可讓您在一個位置分析 Discovery Agents 從所有探索到的內部部署伺服器收集的資料。一旦從 Migration Hub 主控台 （或使用 StartContinousExport API) 啟用 Amazon Athena 中的資料探勘，並開啟代理程式的資料收集，代理程式收集的資料會自動定期儲存在 S3 儲存貯體中。

然後，您可以造訪 Amazon Athena 執行預先定義的查詢，以分析每個伺服器的時間序列系統效能、每個伺服器上執行的程序類型，以及不同伺服器之間的網路相依性。此外，您可以使用 Amazon Athena

撰寫自己的自訂查詢、上傳其他現有資料來源，例如組態管理資料庫 (CMDB) 匯出，以及將探索到的伺服器與實際業務應用程式建立關聯。您也可以將 Athena 資料庫與 Amazon QuickSight 整合，以視覺化查詢輸出並執行其他分析。

本節中的主題說明您可以在 Athena 中使用資料來評估和規劃遷移本機環境的方式 AWS。

在 Amazon Athena 中開啟資料探勘

Amazon Athena 中的資料探索是透過使用 Migration Hub 主控台或從 進行 API 呼叫來開啟連續匯出來啟用 AWS CLI。您必須先開啟資料探索，才能在 Amazon Athena 中查看並開始探索探索到的資料。

當您開啟持續匯出時，您的 帳戶`AWSServiceRoleForApplicationDiscoveryServiceContinuousExport`會自動使用服務連結角色。如需此服務連結角色的詳細資訊，請參閱 Application Discovery Service 的服務連結角色許可。

下列指示說明如何使用 主控台和 在 Amazon Athena 中開啟資料探 AWS CLI勘。

Turn on with the console

當您選擇「開始資料收集」，或按一下 Migration Hub 主控台的資料收集器頁面上標記為「Amazon Athena 中的資料探勘」的切換開關時，會隱含開啟持續匯出，以 Amazon Athena 啟用 Amazon Athena 中的資料探勘。

從主控台開啟 Amazon Athena 中的資料探勘

1. 在導覽窗格中，選擇 Data Collectors (資料收集器)。
2. 選擇 Agents (代理程式) 索引標籤。
3. 選擇開始資料收集，或者如果您已開啟資料收集，請按一下 Amazon Athena 切換中的資料探勘。
4. 在上一步驟產生的對話方塊中，按一下核取方塊以同意相關成本並選擇 Continue (繼續) 或 Enable (啟用)。

> **Note**
>
> 您的代理程式現在以「持續匯出」模式執行，可讓您在 Amazon Athena 中查看和使用探索到的資料。第一次啟用此功能時，您的資料最多可能需要 30 分鐘才會出現在 Amazon Athena 中。

Enable with the AWS CLI

Amazon Athena 中的資料探勘是透過 API 呼叫從 明確開啟的 Continuous Export 來啟用 AWS CLI。若要這樣做， AWS CLI 必須先在您的環境中安裝 。

在 Amazon Athena 中安裝 AWS CLI 並開啟資料探勘

1. AWS CLI 為您的作業系統 (Linux、macOS 或 Windows) 安裝 。如需說明，請參閱 AWS Command Line Interface 使用者指南。
2. 開啟命令提示字元 (Windows) 或終端機 (Linux 或 macOS)。
   a. 輸入 `aws configure` 然後按 Enter 鍵。
   b. 輸入您的 AWS 存取金鑰 ID 和 AWS 私密存取金鑰。
   c. 輸入預設區域名稱的 `us-west-2`。
   d. 輸入預設輸出格式的 `text`。
3. 鍵入以下命令：

```
aws discovery start-continuous-export
```

> **Note**
>
> 您的代理程式現在以「持續匯出」模式執行，可讓您在 Amazon Athena 中查看和使用探索到的資料。第一次啟用此功能時，您的資料最多可能需要 30 分鐘才會出現在 Amazon Athena 中。

直接在 Amazon Athena 中探索資料

在 Amazon Athena 中開啟資料探勘之後，您可以直接在 Athena 中查詢資料，開始探索和使用代理程式探索到的詳細目前資料。您可以使用此資料來產生試算表、執行成本分析、將該查詢連接至視覺化程式，以圖表化網路相依性等作業。

下列指示說明如何直接在 Athena 主控台中探索您的代理程式資料。如果您在 Athena 中沒有任何資料，或尚未在 Amazon Athena 中啟用資料探勘，對話方塊會提示您在 Amazon Athena 中啟用資料探勘，如 中所述在 Amazon Athena 中開啟資料探勘。

直接在 Athena 中探索代理程式探索的資料

1. 在 AWS Migration Hub 主控台的導覽窗格中，選擇伺服器。
2. 若要開啟 Amazon Athena 主控台，請選擇在 Amazon Athena 中探索資料。
3. 在 Query Editor (查詢編輯器) 頁面上，Database (資料庫) 下的導覽窗格中，確定 application_discovery_service_database 為已選取的狀態。

> **Note**
>
> 在 Tables (資料表) 下，下列資料表代表依代理程式分組的資料集。
>
> - os_info_agent
> - network_interface_agent
> - sys_performance_agent
> - processes_agent
> - inbound_connection_agent
> - outbound_connection_agent
> - id_mapping_agent

4. 透過在 Athena 查詢編輯器中寫入和執行 SQL 查詢，在 Amazon Athena 主控台中查詢資料。例如，您可以使用下列查詢來查看所有探索到的伺服器 IP 地址。

```
SELECT * FROM network_interface_agent;
```

如需更多範例查詢，請參閱在 Amazon Athena 中使用預先定義的查詢。

視覺化 Amazon Athena 資料

若要視覺化您的資料，可以將查詢移植到視覺化程式，例如 Amazon QuickSight 或其他開放原始碼視覺化工具，例如 Cytoscape、yEd 或 Gelphi。使用這些工具來轉譯網路圖表、摘要圖表和其他圖形表示。使用此方法時，您可以透過視覺化程式連線到 Athena，讓它可以存取您收集的資料做為產生視覺化的來源。

使用 QuickSight 視覺化您的 Amazon Athena 資料

1. 登入 Amazon QuickSight。

2. 選擇 Connect to another data source or upload a file (連接到其他資料來源或上傳檔案)。
3. 選擇 Athena。隨即顯示新的 Athena 資料來源對話方塊。
4. 在 Data source name (資料來源名稱) 欄位中輸入名稱。
5. 選擇 Create data source (建立資料來源)。
6. 在 Choose your table (選取您的資料表) 對話方塊中選取 Agents-servers-os (Agents-servers-os) 資料表，並選取 Select (選擇)。
7. 在 Finish data set creation (完成資料集建立) 對話方塊中，選取 Import to SPICE for quicker analytics (匯入至 SPICE 以進行更快速的分析)，然後選擇 Visualize (視覺化)。

   即會轉譯您的視覺化。

在 Amazon Athena 中使用預先定義的查詢

本節包含一組預先定義的查詢，此查訊可執行典型使用案例，例如 TCO 分析和網路視覺化。您可以直接使用這些查詢，也可以進行修改以滿足您的需求。

使用預先定義的查詢

1. 在 AWS Migration Hub 主控台的導覽窗格中，選擇伺服器。
2. 若要開啟 Amazon Athena 主控台，請選擇在 Amazon Athena 中探索資料。
3. 在 Query Editor (查詢編輯器) 頁面上，Database (資料庫) 下的導覽窗格中，確定 application_discovery_service_database 為已選取的狀態。
4. 在查詢編輯器中選擇加號 (+)，以建立具有新查詢的標籤。
5. 從 預先定義的查詢 複製其中一個查詢。
6. 將查詢貼到您剛建立新查詢頁籤的查詢窗格中。
7. 選擇 Run Query (執行查詢)。

預先定義的查詢

選擇標題以查看有關查詢的資訊。

取得伺服器的 IP 地址和主機名稱

此協助程式函數會擷取指定伺服器的 IP 地址和主機名稱。您可以在其他查詢中使用此視圖。如需有關如何建立檢視的資訊，請參閱《Amazon Athena 使用者指南》中的 CREATE VIEW。

```
CREATE OR REPLACE VIEW hostname_ip_helper AS
SELECT DISTINCT
  "os"."host_name"
, "nic"."agent_id"
, "nic"."ip_address"
FROM
  os_info_agent os
, network_interface_agent nic
WHERE ("os"."agent_id" = "nic"."agent_id");
```

識別具有或沒有代理程式的伺服器

此查詢可協助您執行資料驗證。如果您已在您網路的多部伺服器上部署代理程式，您可以使用此查詢以了解您網路上是否有其他伺服器尚未部署代理程式。在此查詢中，我們可檢視傳入和傳出網路流量，並可篩選以僅檢視私有 IP 地址的流量。亦即，以 192、10 或 172 起始的 IP 地址。

```
SELECT DISTINCT "destination_ip" "IP Address" ,
         (CASE
    WHEN (
    (SELECT "count"(*)
    FROM network_interface_agent
    WHERE ("ip_address" = "destination_ip") ) = 0) THEN
        'no'
        WHEN (
        (SELECT "count"(*)
        FROM network_interface_agent
        WHERE ("ip_address" = "destination_ip") ) > 0) THEN
            'yes' END) "agent_running"
    FROM outbound_connection_agent
WHERE ((("destination_ip" LIKE '192.%')
        OR ("destination_ip" LIKE '10.%'))
        OR ("destination_ip" LIKE '172.%'))
UNION
SELECT DISTINCT "source_ip" "IP ADDRESS" ,
         (CASE
    WHEN (
    (SELECT "count"(*)
    FROM network_interface_agent
    WHERE ("ip_address" = "source_ip") ) = 0) THEN
        'no'
        WHEN (
        (SELECT "count"(*)
        FROM network_interface_agent
```

```
        WHERE ("ip_address" = "source_ip") ) > 0) THEN
            'yes' END) "agent_running"
    FROM inbound_connection_agent
WHERE ((("source_ip" LIKE '192.%')
        OR ("source_ip" LIKE '10.%'))
        OR ("source_ip" LIKE '172.%'));
```

使用代理程式分析伺服器的系統效能資料

您可以使用此查詢，為您已安裝代理程式的現場部署伺服器分析系統效能和使用率模式資料。此查詢結合 system_performance_agent 資料表與 os_info_agent 資料表，以識別各伺服器的主機名稱。此查詢傳回執行代理程式之所有伺服器的時間序列使用率資料 (以 15 分鐘為間隔)。

```
SELECT "OS"."os_name" "OS Name" ,
    "OS"."os_version" "OS Version" ,
    "OS"."host_name" "Host Name" ,
     "SP"."agent_id" ,
     "SP"."total_num_cores" "Number of Cores" ,
     "SP"."total_num_cpus" "Number of CPU" ,
     "SP"."total_cpu_usage_pct" "CPU Percentage" ,
     "SP"."total_disk_size_in_gb" "Total Storage (GB)" ,
     "SP"."total_disk_free_size_in_gb" "Free Storage (GB)" ,
     ("SP"."total_disk_size_in_gb" - "SP"."total_disk_free_size_in_gb") "Used
 Storage" ,
     "SP"."total_ram_in_mb" "Total RAM (MB)" ,
     ("SP"."total_ram_in_mb" - "SP"."free_ram_in_mb") "Used RAM (MB)" ,
     "SP"."free_ram_in_mb" "Free RAM (MB)" ,
     "SP"."total_disk_read_ops_per_sec" "Disk Read IOPS" ,
     "SP"."total_disk_bytes_written_per_sec_in_kbps" "Disk Write IOPS" ,
     "SP"."total_network_bytes_read_per_sec_in_kbps" "Network Reads (kbps)" ,
     "SP"."total_network_bytes_written_per_sec_in_kbps" "Network Write (kbps)"
FROM "sys_performance_agent" "SP" , "OS_INFO_agent" "OS"
WHERE ("SP"."agent_id" = "OS"."agent_id") limit 10;
```

根據連接埠號碼和程序詳細資訊，追蹤伺服器之間的傳出通訊

此查詢會取得每個服務之傳出流量的詳細資料，以及連接埠號碼和程序的詳細資料。

在執行查詢之前，如果您尚未執行此操作，則必須建立包含從 IANA 下載之 IANA 連接埠登錄資料庫的 iana_service_ports_import 資料表。如需如何建立此角色的資訊，請參閱建立 IANA 連接埠登錄檔匯入資料表。

建立 iana_service_ports_import 資料表之後，建立兩個視圖輔助函數來追蹤傳出流量。如需有關如何建立檢視的資訊，請參閱《Amazon Athena 使用者指南》中的 CREATE VIEW。

建立傳出追蹤協助程式函數

1. 前往 https://console.aws.amazon.com/athena/ 開啟 Athena 主控台。
2. 使用以下列出所有不同傳出目的地 IP 地址的協助程式函數建立valid_outbound_ips_helper檢視。

```
CREATE OR REPLACE VIEW valid_outbound_ips_helper AS
SELECT DISTINCT "destination_ip"
FROM outbound_connection_agent;
```

3. 使用下列輔助函數，決定傳出流量的通訊頻率以建立 outbound_query_helper 檢視。

```
CREATE OR REPLACE VIEW outbound_query_helper AS
SELECT "agent_id" ,
         "source_ip" ,
         "destination_ip" ,
         "destination_port" ,
         "agent_assigned_process_id" ,
         "count"(*) "frequency"
FROM outbound_connection_agent
WHERE (("ip_version" = 'IPv4')
        AND ("destination_ip" IN
    (SELECT *
    FROM valid_outbound_ips_helper )))
GROUP BY  "agent_id", "source_ip", "destination_ip", "destination_port",
 "agent_assigned_process_id";
```

4. 現在您已有 iana_service_ports_import 資料表和兩個輔助函數，您可執行以下查詢以獲得詳細資料，包括每個服務的傳出流量、連接埠號碼，以及程序的詳細資訊。

```
SELECT hip1.host_name "Source Host Name",
         outbound_connections_results0.source_ip "Source IP Address",
         hip2.host_name "Destination Host Name",
         outbound_connections_results0.destination_ip "Destination IP Address",
         outbound_connections_results0.frequency "Connection Frequency",
         outbound_connections_results0.destination_port "Destination Communication
 Port",
         outbound_connections_results0.servicename "Process Service Name",
         outbound_connections_results0.description "Process Service Description"
```

```
FROM
    (SELECT DISTINCT o.source_ip,
         o.destination_ip,
         o.frequency,
         o.destination_port,
         ianap.servicename,
         ianap.description
    FROM outbound_query_helper o, iana_service_ports_import ianap
    WHERE o.destination_port = TRY_CAST(ianap.portnumber AS integer)) AS
 outbound_connections_results0 LEFT OUTER
JOIN hostname_ip_helper hip1
    ON outbound_connections_results0.source_ip = hip1.ip_address LEFT OUTER
JOIN hostname_ip_helper hip2
    ON outbound_connections_results0.destination_ip = hip2.ip_address
```

根據連接埠號碼和程序詳細資訊，追蹤伺服器之間的傳入通訊

此查詢會取得每個服務之輸入流量的相關資訊，以及連接埠號碼和程序詳細資料。

在執行此查詢之前，如果您尚未執行此操作，則必須建立包含從 IANA 下載之 IANA 連接埠登錄資料庫的 `iana_service_ports_import` 資料表。如需如何建立此角色的資訊，請參閱建立 IANA 連接埠登錄檔匯入資料表。

建立 `iana_service_ports_import` 資料表之後，建立兩個視圖輔助函數函數來追蹤傳入流量。如需有關如何建立檢視的資訊，請參閱《Amazon Athena 使用者指南》中的 CREATE VIEW。

建立匯入追蹤協助程式函數

1. 前往 https://console.aws.amazon.com/athena/ 開啟 Athena 主控台。
2. 使用列出所有不同的傳入來源 IP 地址的以下輔助函數建立 `valid_inbound_ips_helper` 檢視。

```
CREATE OR REPLACE VIEW valid_inbound_ips_helper AS
SELECT DISTINCT "source_ip"
FROM inbound_connection_agent;
```

3. 使用以下輔助函數，確定輸入流量的通訊頻率以建立 `inbound_query_helper` 檢視。

```
CREATE OR REPLACE VIEW inbound_query_helper AS
SELECT "agent_id" ,
         "source_ip" ,
```

```
         "destination_ip" ,
         "destination_port" ,
         "agent_assigned_process_id" ,
         "count"(*) "frequency"
FROM inbound_connection_agent
WHERE (("ip_version" = 'IPv4')
        AND ("source_ip" IN
    (SELECT *
    FROM valid_inbound_ips_helper )))
GROUP BY  "agent_id", "source_ip", "destination_ip", "destination_port",
 "agent_assigned_process_id";
```

4. 現在您已有 iana_service_ports_import 資料表和兩個輔助函數，您可執行以下查詢以獲得詳細資料，包括每個服務的傳入流量、連接埠號碼，以及程序的詳細資訊。

```
SELECT hip1.host_name "Source Host Name",
         inbound_connections_results0.source_ip "Source IP Address",
         hip2.host_name "Destination Host Name",
         inbound_connections_results0.destination_ip "Destination IP Address",
         inbound_connections_results0.frequency "Connection Frequency",
         inbound_connections_results0.destination_port "Destination Communication
 Port",
         inbound_connections_results0.servicename "Process Service Name",
         inbound_connections_results0.description "Process Service Description"
FROM
    (SELECT DISTINCT i.source_ip,
         i.destination_ip,
         i.frequency,
         i.destination_port,
         ianap.servicename,
         ianap.description
    FROM inbound_query_helper i, iana_service_ports_import ianap
    WHERE i.destination_port = TRY_CAST(ianap.portnumber AS integer)) AS
 inbound_connections_results0 LEFT OUTER
JOIN hostname_ip_helper hip1
    ON inbound_connections_results0.source_ip = hip1.ip_address LEFT OUTER
JOIN hostname_ip_helper hip2
    ON inbound_connections_results0.destination_ip = hip2.ip_address
```

從連接埠號碼識別執行中的軟體

此查詢會根據連接埠號碼識別執行中的軟體。

在執行此查詢之前，如果您尚未執行此操作，則必須建立包含從 IANA 下載之 IANA 連接埠登錄資料庫的 iana_service_ports_import 資料表。如需如何建立此角色的資訊，請參閱建立 IANA 連接埠登錄檔匯入資料表。

執行以下查詢，可根據連接埠號碼識別執行中的軟體。

```
SELECT o.host_name "Host Name",
       ianap.servicename "Service",
       ianap.description "Description",
       con.destination_port,
       con.cnt_dest_port "Destination Port Count"
FROM   (SELECT agent_id,
               destination_ip,
               destination_port,
               Count(destination_port) cnt_dest_port
        FROM   inbound_connection_agent
        GROUP  BY agent_id,
                  destination_ip,
                  destination_port) con,
       (SELECT agent_id,
               host_name,
               Max("timestamp")
        FROM   os_info_agent
        GROUP  BY agent_id,
                  host_name) o,
       iana_service_ports_import ianap
WHERE  ianap.transportprotocol = 'tcp'
       AND con.destination_ip NOT LIKE '172%'
       AND con.destination_port = ianap.portnumber
       AND con.agent_id = o.agent_id
ORDER BY cnt_dest_port DESC;
```

建立 IANA 連接埠登錄檔匯入資料表

某些預先定義的查詢需要名為 iana_service_ports_import 的資料表，其中包含從網際網路指派號碼授權單位 (IANA) 下載的資訊。

建立 iana_service_ports_import 資料表

1. 從 https：//iana.org 上的服務名稱和傳輸協定連接埠號碼登錄檔下載 IANA 連接埠登錄資料庫 CSV 檔案。
2. 將檔案上傳至 Amazon S3。如需詳細資訊，請參閱如何將檔案與資料夾上傳到 S3 儲存貯體？

3. 在名為 的 Athena 中建立新的資料表`iana_service_ports_import`。如需說明，請參閱《Amazon Athena 使用者指南》中的建立資料表。在下列範例中，您需要使用在先前步驟中將 CSV 檔案上傳到的 S3 儲存貯體的名稱來取代 `my_bucket_name`。

```
CREATE EXTERNAL TABLE IF NOT EXISTS iana_service_ports_import (
         ServiceName STRING,
         PortNumber INT,
         TransportProtocol STRING,
         Description STRING,
         Assignee STRING,
         Contact STRING,
         RegistrationDate STRING,
         ModificationDate STRING,
         Reference STRING,
         ServiceCode STRING,
         UnauthorizedUseReported STRING,
         AssignmentNotes STRING
)
ROW FORMAT SERDE 'org.apache.hadoop.hive.serde2.lazy.LazySimpleSerDe'
WITH SERDEPROPERTIES (
  'serialization.format' = ',',
  'quoteChar' = '"',
  'field.delim' = ','
) LOCATION 's3://my_bucket_name/'
TBLPROPERTIES ('has_encrypted_data'='false',"skip.header.line.count"="1");
```

使用 AWS Migration Hub 主控台探索資料

AWS Application Discovery Service (Application Discovery Service) 已與 AWS Migration Hub (Migration Hub) 整合，客戶可以在 Migration Hub 中檢視和管理其資料收集器、伺服器和應用程式。當您使用 Application Discovery Service 主控台時，系統會將您重新導向至 Migration Hub 主控台。使用 Migration Hub 主控台不需要額外的步驟或設定。

在本節中，您可以了解如何使用主控台管理和監控 Application Discovery Service Agentless Collector (Agentless Collector) 和 AWS Application Discovery Agent (Discovery Agent)。

主題

在 AWS Migration Hub 主控台儀表板中檢視資料

若要檢視主要儀表板，請從 AWS Migration Hub （遷移中樞） 主控台導覽窗格中選擇儀表板。在 Migration Hub 主儀表板中，您可以檢視伺服器、應用程式和資料收集器的高階統計資料，例如 Application Discovery Service Agentless Collector (Agentless Collector) 和 AWS Application Discovery Agent (Discovery Agent)。

主要儀表板會從中心位置的 Discover (探索) 和 Migrate (遷移) 儀表板收集資料。它有四個狀態和資訊窗格，以及快速存取的連結清單。使用窗格，您可以查看最近更新之應用程式的摘要狀態。您也可以快速存取任何應用程式、取得在不同狀態之應用程式的概觀，以及追蹤隨時間的遷移進度。

若要檢視主要儀表板，請從導覽窗格選擇儀表板，該窗格位於 Migration Hub 主控台首頁的左側。

在 AWS Migration Hub 主控台中啟動和停止資料收集器

Application Discovery Service Agentless Collector (Agentless Collector) 和 AWS Application Discovery Agent (Discovery Agent) 是 AWS Application Discovery Service (Application Discovery Service) 用來協助您探索現有基礎設施的資料收集工具。下列步驟說明如何下載和部署這些探索資料收集工具，部署 Agentless Collector以及 AWS 應用程式探索代理程式。

這些資料收集工具會將其資料存放在 Application Discovery Service 的儲存庫中，提供每個伺服器的詳細資訊，以及在伺服器上執行的程序。部署這些工具時，您可以從 AWS Migration Hub （遷移中樞）主控台啟動、停止和檢視收集的資料。

部署 AWS Application Discovery Agent (Discovery Agent) 之後，您可以在 （遷移中樞） 主控台的 AWS Migration Hub 資料收集器頁面上啟動或停止資料收集程序。

若要開始或停止資料收集工具

1. 使用 AWS 您的帳戶登入 ， AWS Management Console 並在 https：//https://console.aws.amazon.com/migrationhub/ 開啟 Migration Hub 主控台。
2. 在遷移中樞主控台導覽窗格的探索下，選擇資料收集器。
3. 選擇 Agents (代理程式) 索引標籤。
4. 選取您想要開始或停止之收集工具的核取方塊。
5. 選擇 Start data collection (開始資料收集) 或 Stop data collection (停止資料收集)。

在主控台中 AWS Migration Hub 排序資料收集器

如果您部署了許多資料收集器，您可以在主控台的資料收集器頁面上排序已部署收集器的顯示清單。您可以在搜尋列中套用篩選條件來排序清單。您可以搜尋和篩選 Data Collectors (資料收集器) 清單中指定的大部分條件。

下表顯示可用於 代理程式的搜尋條件，包括運算子、值和值的定義。

搜尋條件	運算子	值：定義
Agent ID (代理程式 ID)	==	從安裝集合工具的預先填入清單中選取的任何代理程式 ID。

搜尋條件	運算子	值：定義
Hostname (主機名稱)	== !=	對於代理程式，此為從已安裝代理程式之預先填入主機清單中選擇的任何主機名稱。
Collection status (收集狀態)	== !=	已開始：正在收集資料並傳送至 Application Discovery Service Start scheduled (已排程開始)：資料收集已排程開始。下次 ping 時，資料將傳送至 Application Discovery Service，狀態將變更為已開始。 已停止：未收集或傳送至 Application Discovery Service 的資料。 Stop scheduled (已排程停止)：資料收集已排程停止。下次 ping 時，資料將停止傳送至 Application Discovery Service，且狀態將變更為已停止。

搜尋條件	運算子	值：定義
醫療保健	== !=	Healthy (正常)：資料收集未啟動。此工具運作正常。 Unhealthy (狀況不良)：此工具位於錯誤狀態。不會收集或報告資料。 Unknown (不明)：超過一小時未建立連線。 Shutdown (關機)：由於系統、服務或協助程式關機，上次通訊時工具「關機」。如果發生重新開機或工具升級，狀態將在第一個報告週期變更為另一個狀態。 Running (執行中)：資料收集處於啟動狀態。此工具運作正常。
IP 地址	== !=	從已安裝收集工具之預先填入清單中選擇的任何 IP 地址。

下表顯示可用於無代理程式收集器的搜尋條件，包括運算子、值和值的定義。

搜尋條件	運算子	值：定義
ID	==	從安裝集合工具的預先填入清單中選取的任何無代理程式收集器 ID。
Hostname (主機名稱)	== !=	對於無代理程式收集器，從安裝無代理程式收集器的主機預

搜尋條件	運算子	值：定義
		先填入清單中選取的任何主機名稱。
Status	== !=	收集資料：資料收集已開啟。此工具運作正常。 準備設定 - 未開啟資料收集。此工具運作正常。 需要注意 — 工具處於錯誤狀態且需要注意。 Unknown (不明)：超過一小時未建立連線。 關閉：工具上次因系統、服務或協助程式關閉而通訊的「關閉」。如果發生重新開機或工具升級，狀態將在第一個報告週期變更為另一個狀態。
IP 地址	== !=	從已安裝收集工具之預先填入清單中選擇的任何 IP 地址。

若要套用搜尋篩選條件來排序資料收集器

1. 使用 AWS 您的帳戶登入 ， AWS Management Console 並在 https：//https://console.aws.amazon.com/migrationhub/ 開啟 Migration Hub 主控台。
2. 在遷移中樞主控台導覽窗格的探索下，選擇資料收集器。
3. 選擇無代理程式收集器或代理程式索引標籤。
4. 在搜尋列中按一下，然後從清單中選擇搜尋條件。
5. 從下一個清單中選擇運算子。
6. 從最後一個清單中選擇值。

在 AWS Migration Hub 主控台中檢視伺服器

Servers (伺服器) 頁面提供資料收集工具所知之每個伺服器執行個體的相關系統組態與效能資料。您可以檢視伺服器資訊、使用篩選條件來排序伺服器、使用鍵值組標記伺服器，以及匯出詳細的伺服器和系統資訊。

您可以取得由資料收集工具探索而得的伺服器一般檢視和詳細檢視。

若要檢視探索到的伺服器

1. 使用 AWS 您的帳戶登入 ， AWS Management Console 並在 https：//https://console.aws.amazon.com/migrationhub/ 開啟 Migration Hub 主控台。
2. 在遷移中樞主控台導覽窗格的探索下，選擇伺服器。探索到的伺服器會出現在伺服器清單中。
3. 如需伺服器的詳細資訊，請在 Server info (伺服器資訊) 欄中選擇其伺服器連結。這麼做會顯示一個畫面，其中說明伺服器。

伺服器的詳細資訊畫面會顯示系統資訊和效能指標。您也可以找到一個按鈕，用以匯出網路相依性和處理程序資訊。若要匯出詳細的伺服器資訊，請參閱使用 AWS Migration Hub 匯出伺服器資料。

在 AWS Migration Hub 主控台中排序伺服器

若要輕鬆找到特定伺服器，請套用搜尋篩選條件來排序由資料收集工具探索而得的所有伺服器。您可以搜尋和篩選許多條件。

若要套用搜尋篩選條件來排序伺服器

1. 使用 AWS 您的帳戶登入 ， AWS Management Console 並在 https：//https://console.aws.amazon.com/migrationhub/ 開啟 Migration Hub 主控台。
2. 在遷移中樞主控台導覽窗格的探索下，選擇伺服器。
3. 在搜尋列中按一下，然後從清單中選擇搜尋條件。
4. 從下一個清單中選擇運算子。
5. 輸入您所選搜尋條件的區分大小寫值，並按 Enter 鍵。
6. 重複步驟 2 – 4 可套用多個篩選條件。

在 AWS Migration Hub 主控台中標記伺服器

為了協助規劃遷移和保持事物井然有序，您可以為每個伺服器建立多個標籤。標籤是使用者定義的鍵值對，可存放與伺服器相關的任何自訂資料或中繼資料。您可以在單一操作中標記個別伺服器或多個伺服器。 AWS Application Discovery Service (Application Discovery Service) 標籤類似於 AWS 標籤，但兩種類型的標籤無法互換使用。

您可以從主要 Servers (伺服器) 頁面，為一或多個伺服器新增或移除多個標籤。在伺服器的詳細資訊頁面上，則只能為選取的伺服器新增或移除一或多個標籤。您可以在單一操作中，執行與多個伺服器或標籤相關的任何標記工作類型。您也可以移除標籤。

若要將標籤新增到一或多個伺服器

1. 使用 AWS 您的帳戶登入 ， AWS Management Console 並在 https：//https://console.aws.amazon.com/migrationhub/ 開啟 Migration Hub 主控台。
2. 在遷移中樞主控台導覽窗格的探索下，選擇伺服器。
3. 在 Server info (伺服器資訊) 欄中，選擇您要為其新增標籤的伺服器連結。若要一次將標籤新增到多個伺服器，請按一下多個伺服器的核取方塊。
4. 選擇新增標籤，然後選擇新增標籤。
5. 在對話方塊中，在金鑰欄位中輸入金鑰，然後在值欄位中輸入選擇性的值。

   選擇新增標籤並新增詳細資訊，以新增更多標籤。
6. 選擇 Save (儲存)。

若要從一或多個伺服器移除標籤

1. 使用 AWS 您的帳戶登入 ， AWS Management Console 並在 https：//https://console.aws.amazon.com/migrationhub/ 開啟 Migration Hub 主控台。
2. 在遷移中樞主控台導覽窗格的探索下，選擇伺服器。
3. 在 Server info (伺服器資訊) 欄中，選擇您要從中移除標籤的伺服器連結。選取多個伺服器的核取方塊，一次從多個伺服器移除標籤。
4. 選擇移除標籤。
5. 選取您要移除的每個標籤。
6. 選擇確認。

使用 AWS Migration Hub 匯出伺服器資料

本主題說明如何使用 AWS Management Console、 AWS Command Line Interface或 API 匯出伺服器資料。

使用 AWS Management Console 匯出所有伺服器的伺服器資料

1. 登入 AWS Management Console ，並在 https：//https://console.aws.amazon.com/migrationhub/ 開啟 Migration Hub 主控台。
2. 在探索下方的左側導覽窗格中，選擇伺服器。
3. 選擇動作，然後選擇匯出探索資料。
4. 在畫面下方的 Exports (匯出) 區段中，選擇 Export server details (匯出伺服器詳細資訊)。此動作會產生 .zip 檔案，其中包含下表所述的 .csv 檔案。

檔案名稱	描述
{account_id}_Application.csv	每個應用程式的詳細資訊，包括伺服器計數、名稱和描述。
{account_id}_ApplicationResourceAssociation.csv	伺服器與應用程式之間的關係。
{account_id}_ImportTemplate	每個伺服器應用程式和標籤的摘要。您可以修改並重新匯入此檔案，以更新與伺服器相關聯的應用程式。
{account_id}_NetworkInterface.csv	每個網路介面的詳細資訊，包括相關聯的伺服器、地址和交換器。
{account_id}_Server.csv	每個伺服器的詳細資訊，包括作業系統、主機名稱和 Hypervisor。
{account_id}_SystemPerformance.csv	每個伺服器的詳細資訊，包括 CPU、記憶體和儲存組態，以及效能。
{account_id}_Tags.csv	與伺服器相關聯的每個標籤的詳細資訊。

檔案名稱	描述
{account_id}_VMwareInfo.csv	每個 VMware 組態的詳細資訊，包括 moRef、vmName 和 vCenter。

使用 AWS Management Console 匯出特定伺服器的客服人員資料

1. 登入 AWS Management Console ，並在 https：//https://console.aws.amazon.com/migrationhub/ 開啟 Migration Hub 主控台。
2. 在探索下方的左側導覽窗格中，選擇伺服器。
3. 將游標放在伺服器下的搜尋欄位中。下拉式清單隨即出現。在該清單中，在屬性下，選擇來源，然後選擇 = 運算子，然後選擇來源 = 代理程式。
4. 在搜尋結果中，選擇要匯出資料的伺服器名稱。此動作會帶您前往該伺服器的詳細資訊頁面。
5. 輸入開始時間和結束時間，然後選擇匯出。匯出的 .zip 檔案包含下表所述的 .csv 檔案。

{account_id}_destinationProcessConnection.csv	傳入伺服器連線的詳細資訊。
{account_id}_networkInterface.csv	每個網路界面的詳細資訊，包括地址、遮罩和名稱
{account_id}_osInfo.csv	作業系統的詳細資訊，包括 CPU 類型、Hypervisor 和作業系統名稱。
{account_id}_process.csv	在伺服器上執行之程序的詳細資訊。
{account_id}_sourceProcessConnection.csv	源自伺服器的傳出連線詳細資訊。
{account_id}_systemPerformance.csv	伺服器的 CPU、記憶體和儲存組態及效能的詳細資訊。

使用 AWS Command Line Interface 或 API 匯出伺服器資料

1. 執行 start-export-task。對應的 API 操作是 StartExportTask

2. 執行 describe-export-tasks。對應的 API 操作是 DescribeExportTasks。

在 AWS Migration Hub 主控台中分組伺服器

一些探索到的伺服器可能需要共同遷移才能保有其作用。在這種情況下，您可以在邏輯上將探索到的伺服器定義並分組到應用程式。

在分組程序中，您可以搜尋、篩選和新增標籤。

若要將伺服器分組到新的或現有的應用程式

1. 使用 AWS 您的帳戶登入 ， AWS Management Console 並在 https：//https://console.aws.amazon.com/migrationhub/ 開啟 Migration Hub 主控台。
2. 在遷移中樞主控台導覽窗格的探索下，選擇伺服器。
3. 在伺服器清單中，選取您要分組到新的或現有應用程式的每個伺服器。

   為了協助您選擇分組的伺服器，您可以搜尋和篩選您在伺服器清單中指定的任何條件。在搜尋列中按一下，然後選擇清單中的項目、從下一個清單中選擇運算子，然後輸入您的條件。
4. 選用：對於每個選取的伺服器，選擇 Add tag (新增標籤)、輸入 Key (鍵) 的值，然後選擇輸入 Value (值) 的值。
5. 選擇 Group as application (依應用程式組成群組) 建立您的應用程式，或新增到現有的一個。
6. 在 Group as application (依應用程式組成群組) 對話方塊中，選擇 Group as a new application (分組為新的應用程式) 或 Add to an existing application (新增到現有的應用程式)。

   a. 如果您選擇 Group as a new application (分組為新的應用程式) 中，輸入 Application name (應用程式名稱) 的名稱。您可以選擇輸入 Application description (應用程式描述) 的描述。

   b. 如果您選擇 Add to an existing application (新增到現有的應用程式)，請選擇要新增至清單的應用程式名稱。
7. 選擇 Save (儲存)。

使用 Application Discovery Service API 查詢探索的組態項目

組態項目是由 代理程式或 匯入在您的資料中心內發現的 IT 資產。當您使用 AWS Application Discovery Service （應用程式探索服務） 時，您可以使用 API 來指定篩選條件，並查詢伺服器、應用程式、程序和連線資產的特定組態項目。如需 API 的相關資訊，請參閱 Application Discovery Service API 參考。

以下各節中的資料表列出兩個 Application Discovery Service 動作的可用輸入篩選條件和輸出排序選項：

- `DescribeConfigurations`
- `ListConfigurations`

篩選和排序選項是依套用的資產類型 (伺服器、應用程式、程序或連線) 來組織的。

> **Important**
>
> `DescribeConfigurations`、 `ListConfigurations`和 傳回的結果`StartExportTask`可能不包含最近的更新。如需詳細資訊，請參閱the section called “最終一致性”。

使用 **`DescribeConfigurations`**動作

`DescribeConfigurations` 動作會擷取組態 ID 清單的屬性。所有提供的 ID 必須是相同的資產類型 (伺服器、應用程式、程序或連線)。輸出欄位取決於選取的資產類型。例如，伺服器組態項目的輸出包含伺服器相關的屬性清單，例如，主機名稱、作業系統和網路卡數量。如需命令語法的詳細資訊，請參閱 DescribeConfigurations。

`DescribeConfigurations` 動作不支援篩選。

`DescribeConfigurations` 的輸出欄位

下列表格依資產類型組織，其會列出 `DescribeConfigurations` 動作支援的輸出欄位。標示為強制性的欄位一律存在於輸出中。

伺服器資產

欄位	強制性
server.agentId	
server.applications	
server.applications.hasMore Values	
server.configurationId	x
server.cpuType	
server.hostName	
server.hypervisor	
server.networkInterfaceInfo	
server.networkInterfaceInfo .hasMoreValues	
server.osName	
server.osVersion	
server.tags	
server.tags.hasMoreValues	
server.timeOfCreation	x
server.type	
server.performance.avgCpuUs agePct	
server.performance.avgDiskR eadIOPS	

欄位	強制性
server.performance.avgDiskReadsPerSecondInKB	
server.performance.avgDiskWriteIOPS	
server.performance.avgDiskWritesPerSecondInKB	
server.performance.avgFreeRAMInKB	
server.performance.avgNetworkReadsPerSecondInKB	
server.performance.avgNetworkWritesPerSecondInKB	
server.performance.maxCpuUsagePct	
server.performance.maxDiskReadIOPS	
server.performance.maxDiskReadsPerSecondInKB	
server.performance.maxDiskWriteIOPS	
server.performance.maxDiskWritesPerSecondInKB	
server.performance.maxNetworkReadsPerSecondInKB	
server.performance.maxNetworkWritesPerSecondInKB	

欄位	強制性
server.performance.minFreeRAMInKB	
server.performance.numCores	
server.performance.numCpus	
server.performance.numDisks	
server.performance.numNetworkCards	
server.performance.totalRAMInKB	

程序資產

欄位	強制性
process.commandLine	
process.configurationId	x
process.name	
process.path	
process.timeOfCreation	x

應用程式資產

欄位	強制性
application.configurationId	x
application.description	

欄位	強制性
application.lastModifiedTime	x
application.name	x
application.serverCount	x
application.timeOfCreation	x

使用 ListConfigurations動作

ListConfigurations 動作會根據您在篩選條件中指定的準則擷取組態項目清單。如需命令語法的詳細資訊，請參閱 ListConfigurations。

ListConfigurations 的輸出欄位

下列表格依資產類型組織，其會列出 ListConfigurations 動作支援的輸出欄位。標示為強制性的欄位一律存在於輸出中。

伺服器資產

欄位	強制性
server.configurationId	x
server.agentId	
server.hostName	
server.osName	
server.osVersion	
server.timeOfCreation	x
server.type	

程序資產

欄位	強制性
process.commandLine	
process.configurationId	x
process.name	
process.path	
process.timeOfCreation	x
server.agentId	
server.configurationId	x

應用程式資產

欄位	強制性
application.configurationId	x
application.description	
application.name	x
application.serverCount	x
application.timeOfCreation	x
application.lastModifiedTime	x

連線資產

欄位	強制性
connection.destinationIp	x

欄位	強制性
connection.destinationPort	x
connection.ipVersion	x
connection.latestTimestamp	x
connection.occurrence	x
connection.sourceIp	x
connection.transportProtocol	
destinationProcess.configurationId	
destinationProcess.name	
destinationServer.configurationId	
destinationServer.hostName	
sourceProcess.configurationId	
sourceProcess.name	
sourceServer.configurationId	
sourceServer.hostName	

ListConfigurations 支援的篩選條件：

下列表格依資產類型組織，其會列出 ListConfigurations 動作支援的篩選條件。篩選條件和值位於由其中一個支援的邏輯條件所定義的索引鍵/值關係中。您可以排序所指定之篩選條件的輸出。

伺服器資產

篩選條件	支援的條件	支援的值	支援的排序
server.configurationId	• EQUALS • NOT_EQUALS • EQ • NE	• 任何有效的伺服器組態 ID	無
server.hostName	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字串	• ASC • DESC
server.osName	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字串	• ASC • DESC
server.osVersion	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字串	• ASC • DESC
server.agentId	• EQUALS • NOT_EQUALS • EQ • NE	• 字串	無

篩選條件	支援的條件	支援的值	支援的排序
server.connectorId	• EQUALS • NOT_EQUALS • EQ • NE	• 字串	無
server.type	• EQUALS • NOT_EQUALS • EQ • NE	具有下列其中一個值的字串： • EC2 • OTHER • VMWARE_VM • VMWARE_HOST • VMWARE_VM_TEMPLATE	無
server.vmWareInfo.morefId	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字串	無
server.vmWareInfo.vcenterId	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字串	無

篩選條件	支援的條件	支援的值	支援的排序
server.vmWareInfo.hostId	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字串	無
server.networkInterfaceInfo.portGroupId	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字串	無
server.networkInterfaceInfo.portGroupName	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字串	無
server.networkInterfaceInfo.virtualSwitchName	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字串	無

篩選條件	支援的條件	支援的值	支援的排序
server.networkInterfaceInfo.ipAddress	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字串	無
server.networkInterfaceInfo.macAddress	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字串	無
server.performance.avgCpuUsagePct	• GE • LE • GT • LT	• 百分比	無
server.performance.totalDiskFreeSizeInKB	• GE • LE • GT • LT	• Double	無
server.performance.avgFreeRAMInKB	• GE • LE • GT • LT	• Double	無

篩選條件	支援的條件	支援的值	支援的排序
server.tag.value	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字串	無
server.tag.key	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字串	無
server.application.name	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字串	無
server.application.description	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字串	無

篩選條件	支援的條件	支援的值	支援的排序
server.application.configurationId	• EQUALS • NOT_EQUALS • EQ • NE	• 任何有效的應用程式組態 ID	無
server.process.configurationId	• EQUALS • NOT_EQUALS • EQ • NE	• ProcessId	無
server.process.name	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字串	無
server.process.commandLine	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字串	無

應用程式資產

篩選條件	支援的條件	支援的值	支援的排序
application.configurationId	• EQUALS • NOT_EQUALS • EQ	• ApplicationId	無

篩選條件	支援的條件	支援的值	支援的排序
	• NE		
application.name	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字串	• ASC • DESC
application.description	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字串	• ASC • DESC
application.serverCount	不支援篩選。	不支援篩選。	• ASC • DESC
application.timeOfCreation	不支援篩選。	不支援篩選。	• ASC • DESC
application.lastModifiedTime	不支援篩選。	不支援篩選。	• ASC • DESC

篩選條件	支援的條件	支援的值	支援的排序
server.configurationId	• EQUALS • NOT_EQUALS • EQ • NE	• ServerId	無

程序資產

篩選條件	支援的條件	支援的值	支援的排序
process.configurationId	• EQUALS • NOT_EQUALS • EQ • NE	• ProcessId	
process.name	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字串	• ASC • DESC
process.commandLine	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字串	• ASC • DESC
server.configurationId	• EQUALS • NOT_EQUALS • EQ	• ServerId	

篩選條件	支援的條件	支援的值	支援的排序
	• NE		
server.hostName	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字串	• ASC • DESC
server.osName	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字串	• ASC • DESC
server.os Version	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字串	• ASC • DESC
server.agentId	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字串	

連線資產

篩選條件	支援的條件	支援的值	支援的排序
connection.sourceIp	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• IP	• ASC • DESC
connection.destinationIp	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• IP	• ASC • DESC
connection.destinationPort	• EQUALS • NOT_EQUALS • EQ • NE	• Integer	• ASC • DESC
sourceServer.configurationId	• EQUALS • NOT_EQUALS • EQ • NE	• ServerId	
sourceServer.hostName	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字串	• ASC • DESC

篩選條件	支援的條件	支援的值	支援的排序
destinationServer.osName	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字串	• ASC • DESC
destinationServer.osVersion	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字串	• ASC • DESC
destinationServer.agentId	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字串	
sourceProcess.configurationId	• EQUALS • NOT_EQUALS • EQ • NE	• ProcessId	

篩選條件	支援的條件	支援的值	支援的排序
sourceProcess.name	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字串	• ASC • DESC
sourceProcess.commandLine	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字串	• ASC • DESC
destinationProcess.configurationId	• EQUALS • NOT_EQUALS • EQ • NE	• ProcessId	
destinationProcess.name	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字串	• ASC • DESC

篩選條件	支援的條件	支援的值	支援的排序
`destinationprocess.commandLine`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 字串	• ASC • DESC

AWS Application Discovery Service API 中的最終一致性

下列更新操作最終一致。讀取操作 StartExportTask、 DescribeConfigurations 和 ListConfigurations 可能不會立即顯示更新。

- AssociateConfigurationItemsToApplication
- CreateTags
- DeleteApplications
- DeleteTags
- DescribeBatchDeleteConfigurationTask
- DescribeImportTasks
- DisassociateConfigurationItemsFromApplication
- UpdateApplication

管理最終一致性的建議：

- 當您調用讀取操作 StartExportTask、DescribeConfigurations 或 ListConfigurations （或其對應的 AWS CLI 命令） 時，請使用指數退避演算法，以有足夠的時間讓任何先前的更新操作透過系統傳播。若要這樣做，請重複執行讀取操作，從兩秒的等待時間開始，然後逐漸增加到五分鐘的等待時間。
- 在後續操作之間新增等待時間，即使更新操作傳回 200 - OK 回應。從幾秒鐘的等待時間開始套用指數退避演算法，並逐漸增加到大約五分鐘的等待時間。

AWS Application Discovery Service 使用介面端點 (AWS PrivateLink) 存取

您可以使用 在 VPC 和 之間 AWS PrivateLink 建立私有連線 AWS Application Discovery Service。您可以像在 VPC 中一樣存取 Application Discovery Service，無需使用網際網路閘道、NAT 裝置、VPN 連線或 AWS Direct Connect 連線。VPC 中的執行個體不需要公有 IP 地址即可存取 Application Discovery Service。

您可以建立由 AWS PrivateLink提供支援的介面端點來建立此私有連線。我們會在您為介面端點啟用的每個子網中建立端點網路介面。這些是請求者管理的網路介面，可做為目的地為 Application Discovery Service 之流量的進入點。

如需詳細資訊，請參閱「AWS PrivateLink 指南」中的透過 AWS PrivateLink存取 AWS 服務。

Application Discovery Service 的考量事項

設定 Application Discovery Service 的介面端點之前，請先檢閱 AWS PrivateLink 指南中的使用介面 VPC 端點存取 AWS 服務。

Application Discovery Service 支援兩個介面：一個用於呼叫其所有 API 動作，另一個用於無代理程式收集器和 AWS 應用程式探索代理程式傳送探索資料。

建立介面端點

您可以使用 Amazon VPC 主控台或 AWS Command Line Interface (AWS CLI)，建立介面端點。如需詳細資訊，請參閱《 AWS PrivateLink 指南》中的使用介面 VPC 端點存取 AWS 服務。

For Application Discovery Service

使用下列服務名稱建立 Application Discovery Service 的介面端點：

```
com.amazonaws.region.discovery
```

如果您為介面端點啟用私有 DNS，您可以使用其預設的區域 DNS 名稱向 Application Discovery Service 提出 API 請求。例如：`discovery.us-east-1.amazonaws.com`。

For Agentless Collector and AWS Application Discovery Agent

使用以下服務名稱建立介面端點：

```
com.amazonaws.region.arsenal-discovery
```

如果您為介面端點啟用私有 DNS，您可以使用其預設的區域 DNS 名稱向 Application Discovery Arsenal 提出 API 請求。例如：`arsenal-discovery.us-east-1.amazonaws.com`。

為您的介面端點建立端點政策

端點政策為 IAM 資源，您可將其連接至介面端點。預設端點政策允許透過介面端點完整存取 AWS 服務。若要控制從 VPC 對 AWS 服務的允許存取，請將自訂端點政策連接至介面端點。

端點政策會指定以下資訊：

- 可執行動作 (AWS 帳戶、IAM 使用者和 IAM 角色) 的主體。
- 可執行的動作。

如需詳細資訊，請參閱「AWS PrivateLink 指南」中的使用端點政策控制對服務的存取。

範例：VPC 端點政策

以下是自訂端點政策的範例。將此政策附加至介面端點後，此政策會針對所有資源上的所有主體，授予列出的 動作的存取權限。

Example policy for Application Discovery Service

```
{
   "Statement": [
      {
         "Principal": "*",
         "Effect": "Allow",
         "Action": [
            "discovery:action-1",
            "discovery:action-2",
            "discovery:action-3"
         ],
         "Resource":"*"
      }
   ]
}
```

Example policy for the Agentless Collector and AWS Application Discovery Agent

```
{
   "Statement": [
      {
         "Principal": "*",
         "Effect": "Allow",
         "Action": [
            "arsenal:RegisterOnPremisesAgent"
         ],
         "Resource":"*"
      }
   ]
}
```

使用 Agentless Collector 和 AWS Application Discovery Agent 的 VPC 端點

Agentless Collector 和 AWS Application Discovery Agent 不支援可設定的端點。請改為使用 Amazon VPC 端點的私有 DNS `arsenal-discovery` 功能。

- 設定 AWS Direct Connect 路由表，將私有 AWS IP 地址路由至 VPC。例如，目的地 = 10.0.0.0/8，目標 = 本機。針對此設定，您至少需要將 `arsenal-discovery` Amazon VPC 端點私有 IP 地址路由至 VPC。
- 使用 `arsenal-discovery` Amazon VPC 端點私有 DNS 功能，因為 Agentless Collector 不支援可設定的 Arsenal 端點。
- 在私有子網路中，使用您要路由 AWS Direct Connect 流量的相同 VPC 設定 `arsenal-discovery`Amazon VPC 端點。
- 使用安全群組設定 `arsenal-discovery` Amazon VPC 端點，以啟用 VPC 內的傳入流量 （例如 10.0.0.0/8)。
- 設定 Amazon Route 53 傳入解析程式，以路由 `arsenal-discovery` Amazon VPC 端點私有 DNS 名稱的 DNS 解析，這會解析為 VPC 端點的私有 IP。如果您不這樣做，收集器將使用內部部署解析程式來執行 DNS 解析，並將使用公有 Arsenal 端點，且流量不會通過 VPC。
- 如果您已停用所有公有流量，自動更新功能將會失敗。這是因為 Agentless Collector 透過傳送請求到 Amazon ECR 端點來擷取更新。若要讓自動更新功能正常運作，而無需透過公有網際網路傳送請求，請為 Amazon ECR 服務設定 VPC 端點，並為此端點啟用私有 DNS 功能。

中的安全性 AWS Application Discovery Service

的雲端安全性 AWS 是最高優先順序。身為 AWS 客戶，您可以從資料中心和網路架構中受益，這些架構是為了滿足最安全敏感組織的需求而建置。

安全性是 AWS 和 之間的共同責任。共同責任模型 將此描述為雲端的安全和雲端內的安全：

- 雲端的安全性 – AWS 負責保護在 Cloud AWS 中執行 AWS 服務的基礎設施。 AWS 也為您提供可安全使用的服務。第三方稽核人員定期檢測及驗證安全的效率也是我們 AWS 合規計劃的一部分。
- 雲端安全 – 您的責任取決於您使用 AWS 的服務。您也必須對資料敏感度、組織要求，以及適用法律和法規等其他因素負責。

若要使用 AWS Application Discovery Agent 或 Application Discovery Service Agentless Collector，您必須將存取金鑰提供給 AWS 您的帳戶。然後，此資訊會儲存在您的本機基礎設施上。作為共同責任模型的一部分，您有責任保護對基礎設施的存取。

本文件將協助您了解如何在使用 Application Discovery Service 時套用共同的責任模型。下列主題說明如何設定 Application Discovery Service 以符合您的安全和合規目標。您也將了解如何使用其他 AWS 服務，以協助您監控和保護 Application Discovery Service 資源。

主題

- 的身分和存取管理 AWS Application Discovery Service
- 使用 記錄應用程式探索服務 API 呼叫 AWS CloudTrail

的身分和存取管理 AWS Application Discovery Service

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 Application Discovery Service 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 Application Discovery Service 如何使用 IAM

- AWS 的 受管政策 AWS Application Discovery Service
- AWS Application Discovery Service 身分型政策範例
- 使用 Application Discovery Service 的服務連結角色
- 對 AWS Application Discovery Service Identity and Access 進行故障診斷

目標對象

使用方式 AWS Identity and Access Management (IAM) 會有所不同，取決於您在 Application Discovery Service 中執行的工作。

服務使用者 – 如果您使用 Application Discovery Service 服務來執行您的任務，則您的管理員會為您提供所需的登入資料和許可。當您使用更多 Application Discovery Service 功能來執行工作時，您可能需要額外的許可。了解存取許可的管理方式可協助您向管理員請求正確的許可。如果您無法存取 Application Discovery Service 中的功能，請參閱 對 AWS Application Discovery Service Identity and Access 進行故障診斷。

服務管理員 – 如果您在公司負責 Application Discovery Service 資源，您可能可以完整存取 Application Discovery Service。您的任務是判斷服務使用者應存取哪些 Application Discovery Service 功能和資源。接著，您必須將請求提交給您的 IAM 管理員，來變更您服務使用者的許可。檢閱此頁面上的資訊，了解 IAM 的基本概念。若要進一步了解貴公司如何搭配 Application Discovery Service 使用 IAM，請參閱 AWS Application Discovery Service 如何使用 IAM。

IAM 管理員 – 如果您是 IAM 管理員，建議您了解撰寫政策以管理 Application Discovery Service 存取的詳細資訊。若要檢視您可以在 IAM 中使用的 Application Discovery Service 身分型政策範例，請參閱 AWS Application Discovery Service 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 帳戶根使用者身分、IAM 使用者身分或擔任 IAM 角色來驗證 （ 登入 AWS)。

您可以使用透過身分來源提供的憑證，以聯合身分 AWS 身分身分身分身分登入 。 AWS IAM Identity Center (IAM Identity Center) 使用者、您公司的單一登入身分驗證，以及您的 Google 或 Facebook 登入資料，都是聯合身分的範例。您以聯合身分登入時，您的管理員先前已設定使用 IAM 角色的聯合身分。當您使用聯合 AWS 身分存取 時，您會間接擔任角色。

根據您身分的使用者類型，您可以登入 AWS Management Console 或 AWS 存取入口網站。如需登入的詳細資訊 AWS，請參閱AWS 登入 《 使用者指南》中的如何登入您的 AWS 帳戶 。

如果您以 AWS 程式設計方式存取 ， AWS 會提供軟體開發套件 (SDK) 和命令列界面 (CLI)，以使用您的 憑證以密碼編譯方式簽署您的請求。如果您不使用 AWS 工具，則必須自行簽署請求。如需使用建議的方法自行簽署請求的詳細資訊，請參閱《IAM 使用者指南》中的適用於 API 請求的AWS Signature 第 4 版。

無論您使用何種身分驗證方法，您可能都需要提供額外的安全性資訊。例如， AWS 建議您使用多重要素驗證 (MFA) 來提高帳戶的安全性。如需更多資訊，請參閱《AWS IAM Identity Center 使用者指南》中的多重要素驗證和《IAM 使用者指南》中的 IAM 中的AWS 多重要素驗證。

AWS 帳戶 根使用者

當您建立 時 AWS 帳戶，您會從一個登入身分開始，該身分可以完整存取 帳戶中的所有 AWS 服務 和資源。此身分稱為 AWS 帳戶 Theroot 使用者，可透過使用您用來建立帳戶的電子郵件地址和密碼登入來存取。強烈建議您不要以根使用者處理日常任務。保護您的根使用者憑證，並將其用來執行只能由根使用者執行的任務。如需這些任務的完整清單，了解需以根使用者登入的任務，請參閱《IAM 使用者指南》中的需要根使用者憑證的任務。

IAM 使用者和群組

IAM 使用者是 中具有單一人員或應用程式特定許可 AWS 帳戶 的身分。建議您盡可能依賴臨時憑證，而不是擁有建立長期憑證 (例如密碼和存取金鑰) 的 IAM 使用者。但是如果特定使用案例需要擁有長期憑證的 IAM 使用者，建議您輪換存取金鑰。如需更多資訊，請參閱 IAM 使用者指南中的為需要長期憑證的使用案例定期輪換存取金鑰。

IAM 群組是一種指定 IAM 使用者集合的身分。您無法以群組身分簽署。您可以使用群組來一次為多名使用者指定許可。群組可讓管理大量使用者許可的程序變得更為容易。例如，您可以擁有一個名為 IAMAdmins 的群組，並給予該群組管理 IAM 資源的許可。

使用者與角色不同。使用者只會與單一人員或應用程式建立關聯，但角色的目的是在由任何需要它的人員取得。使用者擁有永久的長期憑證，但角色僅提供臨時憑證。如需更多資訊，請參閱《IAM 使用者指南》中的 IAM 使用者的使用案例。

IAM 角色

IAM 角色是 中具有特定許可 AWS 帳戶 的身分。它類似 IAM 使用者，但不與特定的人員相關聯。若要暫時在 中擔任 IAM 角色 AWS Management Console，您可以從使用者切換至 IAM 角色 （ 主控台 ）。您可以透過呼叫 AWS CLI 或 AWS API 操作或使用自訂 URL 來擔任角色。如需使用角色的方法詳細資訊，請參閱《IAM 使用者指南》中的擔任角色的方法。

使用臨時憑證的 IAM 角色在下列情況中非常有用：

- 聯合身分使用者存取 — 如需向聯合身分指派許可，請建立角色，並為角色定義許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並獲授予由角色定義的許可。如需有關聯合角色的相關資訊，請參閱《IAM 使用者指南》中的為第三方身分提供者 (聯合) 建立角色。如果您使用 IAM Identity Center，則需要設定許可集。為控制身分驗證後可以存取的內容，IAM Identity Center 將許可集與 IAM 中的角色相關聯。如需有關許可集的資訊，請參閱 AWS IAM Identity Center 使用者指南中的許可集。
- 暫時 IAM 使用者許可 – IAM 使用者或角色可以擔任 IAM 角色來暫時針對特定任務採用不同的許可。
- 跨帳戶存取權：您可以使用 IAM 角色，允許不同帳戶中的某人 (信任的主體) 存取您帳戶的資源。角色是授予跨帳戶存取權的主要方式。不過，對於某些 AWS 服務，您可以直接將政策連接到資源（而不是使用角色做為代理）。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。
- 跨服務存取 – 有些 AWS 服務 使用其他 中的功能 AWS 服務。例如，當您在服務中進行呼叫時，該服務通常會在 Amazon EC2 中執行應用程式或將物件儲存在 Amazon Simple Storage Service (Amazon S3) 中。服務可能會使用呼叫主體的許可、使用服務角色或使用服務連結角色來執行此作業。
  - 轉送存取工作階段 (FAS) – 當您使用 IAM 使用者或角色在 中執行動作時 AWS，您會被視為主體。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。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。只有當服務收到需要與其他 AWS 服務 或 資源互動才能完成的請求時，才會提出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。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》。
  - 服務角色 – 服務角色是服務擔任的 IAM 角色，可代表您執行動作。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權給 AWS 服務。
  - 服務連結角色 – 服務連結角色是連結至 的服務角色類型 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。
- 在 Amazon EC2 上執行的應用程式 – 您可以使用 IAM 角色來管理在 EC2 執行個體上執行之應用程式的臨時登入資料，以及提出 AWS CLI 或 AWS API 請求。這是在 EC2 執行個體內儲存存取金鑰的較好方式。若要將 AWS 角色指派給 EC2 執行個體，並將其提供給其所有應用程式，您可以建立連接至執行個體的執行個體描述檔。執行個體設定檔包含該角色，並且可讓 EC2 執行個體上執行的程式取得臨時憑證。如需詳細資訊，請參閱《IAM 使用者指南》中的使用 IAM 角色來授予許可權給 Amazon EC2 執行個體上執行的應用程式。

使用政策管理存取權

您可以透過建立政策並將其連接至身分或資源 AWS 來控制 AWS 中的存取。政策是 中的物件，當與身分或資源建立關聯時， AWS 會定義其許可。當委託人（使用者、根使用者或角色工作階段）提出請求時， 會 AWS 評估這些政策。政策中的許可決定是否允許或拒絕請求。大多數政策會以 JSON 文件 AWS 的形式存放在 中。如需 JSON 政策文件結構和內容的詳細資訊，請參閱 IAM 使用者指南中的JSON 政策概觀。

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。

預設情況下，使用者和角色沒有許可。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。然後，管理員可以將 IAM 政策新增至角色，使用者便能擔任這些角色。

IAM 政策定義該動作的許可，無論您使用何種方法來執行操作。例如，假設您有一個允許 `iam:GetRole` 動作的政策。具有該政策的使用者可以從 AWS Management Console AWS CLI、 或 API AWS 取得角色資訊。

身分型政策

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。

身分型政策可進一步分類成內嵌政策或受管政策。內嵌政策會直接內嵌到單一使用者、群組或角色。受管政策是獨立的政策，您可以連接到 中的多個使用者、群組和角色 AWS 帳戶。受管政策包括 AWS 受管政策和客戶受管政策。如需了解如何在受管政策及內嵌政策之間選擇，請參閱《IAM 使用者指南》中的在受管政策和內嵌政策間選擇。

資源型政策

資源型政策是連接到資源的 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。

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。

存取控制清單 (ACL)

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。

Amazon S3 AWS WAF和 Amazon VPC 是支援 ACLs的服務範例。如需進一步了解 ACL，請參閱 Amazon Simple Storage Service 開發人員指南中的存取控制清單 (ACL) 概觀。

其他政策類型

AWS 支援其他較不常見的政策類型。這些政策類型可設定較常見政策類型授予您的最大許可。

- 許可界限 – 許可範圍是一種進階功能，可供您設定身分型政策能授予 IAM 實體 (IAM 使用者或角色) 的最大許可。您可以為實體設定許可界限。所產生的許可會是實體的身分型政策和其許可界限的交集。會在 `Principal` 欄位中指定使用者或角色的資源型政策則不會受到許可界限限制。所有這類政策中的明確拒絕都會覆寫該允許。如需許可界限的詳細資訊，請參閱 IAM 使用者指南中的 IAM 實體許可界限。
- 服務控制政策 SCPs) – SCPs是 JSON 政策，可指定 in. 中組織或組織單位 (OU) 的最大許可 AWS Organizations。 AWS Organizations 是一種用於分組和集中管理您企業擁有 AWS 帳戶 的多個的服務。若您啟用組織中的所有功能，您可以將服務控制政策 (SCP) 套用到任何或所有帳戶。SCP 會限制成員帳戶中實體的許可，包括每個實體 AWS 帳戶根使用者。如需 Organizations 和 SCP 的詳細資訊，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) - RCP 是 JSON 政策，可用來設定您帳戶中資源的可用許可上限，採取這種方式就不需要更新附加至您所擁有的每個資源的 IAM 政策。RCP 會限制成員帳戶中資源的許可，並可能影響身分的有效許可，包括 AWS 帳戶根使用者，無論它們是否屬於您的組織。如需 Organizations 和 RCPs的詳細資訊，包括支援 RCPs AWS 服務 的 清單，請參閱AWS Organizations 《 使用者指南》中的資源控制政策 RCPs)。
- 工作階段政策 – 工作階段政策是一種進階政策，您可以在透過撰寫程式的方式建立角色或聯合使用者的暫時工作階段時，做為參數傳遞。所產生工作階段的許可會是使用者或角色的身分型政策和工作階段政策的交集。許可也可以來自資源型政策。所有這類政策中的明確拒絕都會覆寫該允許。如需詳細資訊，請參閱 IAM 使用者指南中的工作階段政策。

多種政策類型

將多種政策類型套用到請求時，其結果形成的許可會更為複雜、更加難以理解。若要了解如何 AWS 在涉及多種政策類型時決定是否允許請求，請參閱《IAM 使用者指南》中的政策評估邏輯。

AWS Application Discovery Service 如何使用 IAM

使用 IAM 管理 Application Discovery Service 的存取權之前，您應該了解哪些 IAM 功能可與 Application Discovery Service 搭配使用。若要深入了解 Application Discovery Service 和其他 AWS 服務如何與 IAM 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。

主題

- Application Discovery Service 身分型政策
- Application Discovery Service 資源型政策
- 以 Application Discovery Service 標籤為基礎的授權
- 應用程式探索服務 IAM 角色

Application Discovery Service 身分型政策

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。Application Discovery Service 支援特定動作、資源和條件索引鍵。若要了解您在 JSON 政策中使用的所有元素，請參閱 IAM 使用者指南中的 JSON 政策元素參考。

動作

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。政策動作通常具有與相關聯 AWS API 操作相同的名稱。有一些例外狀況，例如沒有相符的 API 操作的僅限許可動作。也有一些作業需要政策中的多個動作。這些額外的動作稱為相依動作。

政策會使用動作來授予執行相關聯動作的許可。

Application Discovery Service 中的政策動作在動作之前使用下列字首：`discovery:`。政策陳述式必須包含 `Action` 或 `NotAction` 元素。Application Discovery Service 會定義自己的動作集，描述您可以使用此服務執行的任務。

若要在單一陳述式中指定多個動作，請用逗號分隔，如下所示：

```
"Action": [
      "discovery:action1",
      "discovery:action2"
```

您也可以使用萬用字元 (*) 來指定多個動作。例如，若要指定開頭是 Describe 文字的所有動作，請包含以下動作：

```
"Action": "discovery:Describe*"
```

若要查看 Application Discovery Service 動作的清單，請參閱《IAM 使用者指南》中的 定義的動作 AWS Application Discovery Service。

資源

Application Discovery Service 不支援在政策中指定資源 ARNs。若要分開存取，請建立並使用個別的 AWS 帳戶。

條件索引鍵

Application Discovery Service 不提供任何服務特定的條件金鑰，但支援使用一些全域條件金鑰。若要查看所有 AWS 全域條件金鑰，請參閱《IAM 使用者指南》中的AWS 全域條件內容金鑰。

範例

若要檢視 Application Discovery Service 身分型政策的範例，請參閱 AWS Application Discovery Service 身分型政策範例。

Application Discovery Service 資源型政策

Application Discovery Service 不支援以資源為基礎的政策。

以 Application Discovery Service 標籤為基礎的授權

Application Discovery Service 不支援標記資源或根據標籤控制存取。

應用程式探索服務 IAM 角色

IAM 角色是您 AWS 帳戶中具有特定許可的實體。

搭配 Application Discovery Service 使用臨時憑證

Application Discovery Service 不支援使用臨時登入資料。

服務連結角色

服務連結角色可讓 AWS 服務存取其他服務中的資源，以代表您完成 動作。服務連結角色會顯示在您的 IAM 帳戶中，並由該服務所擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

Application Discovery Service 支援服務連結角色。如需建立或管理 Application Discovery Service 服務連結角色的詳細資訊，請參閱 使用 Application Discovery Service 的服務連結角色。

服務角色

此功能可讓服務代表您擔任服務角色。此角色可讓服務存取其他服務中的資源，以代表您完成動作。服務角色會出現在您的 IAM 帳戶中，且由該帳戶所擁有。這表示 IAM 管理員可以變更此角色的許可。不過，這樣可能會破壞此服務的功能。

Application Discovery Service 支援服務角色。

AWS 的 受管政策 AWS Application Discovery Service

若要將許可新增至使用者、群組和角色，使用 AWS 受管政策比自行撰寫政策更容易。建立 IAM 客戶受管政策需要時間和專業知識，而受管政策可為您的團隊提供其所需的許可。若要快速開始使用，您可以使用我們的 AWS 受管政策。這些政策涵蓋常見的使用案例，並可在您的 AWS 帳戶中使用。如需受 AWS 管政策的詳細資訊，請參閱《IAM 使用者指南》中的AWS 受管政策。

AWS 服務會維護和更新 AWS 受管政策。您無法變更 AWS 受管政策中的許可。服務偶爾會在 AWS 受管政策中新增其他許可以支援新功能。此類型的更新會影響已連接政策的所有身分識別 (使用者、群組和角色)。當新功能啟動或新操作可用時，服務很可能會更新 AWS 受管政策。服務不會從 AWS 受管政策中移除許可，因此政策更新不會破壞您現有的許可。

此外， AWS 支援跨多個 服務的任務函數的受管政策。例如，ReadOnlyAccess AWS 受管政策提供所有 AWS 服務和資源的唯讀存取權。當服務啟動新功能時， 會為新操作和資源 AWS 新增唯讀許可。如需任務職能政策的清單和說明，請參閱 IAM 使用者指南中有關任務職能的AWS 受管政策。

AWS 受管政策：AWSApplicationDiscoveryServiceFullAccess

此`AWSApplicationDiscoveryServiceFullAccess`政策會授予 IAM 使用者帳戶對 Application Discovery Service 和 Migration Hub APIs存取權。

連接此政策的 IAM 使用者帳戶可以設定 Application Discovery Service、啟動和停止代理程式、啟動和停止無代理程式探索，以及從 AWS Discovery Service 資料庫查詢資料。如需此政策的範例，請參閱 授予 Application Discovery Service 的完整存取權。

AWS 受管政策：AWSApplicationDiscoveryAgentlessCollectorAccess

AWSApplicationDiscoveryAgentlessCollectorAccess 受管政策會授予 Application Discovery Service Agentless Collector (Agentless Collector) 註冊和與 Application Discovery Service 通訊，以及與其他 AWS 服務通訊的存取權。

此政策必須連接到憑證用於設定 Agentless Collector 的 IAM 使用者。

許可詳細資訊

此政策包含以下許可。

- arsenal – 允許收集器向 Application Discovery Service 應用程式註冊。這對於能夠將收集的資料傳回 是必要的 AWS。
- ecr-public – 允許收集器呼叫 Amazon Elastic Container Registry Public (Amazon ECR Public)，其中會找到收集器的最新更新。
- mgh – 允許收集器呼叫 AWS Migration Hub ，以擷取用於設定收集器之帳戶的主區域。這是知道應將收集的資料傳送到哪個區域的必要條件。
- sts – 允許收集器擷取服務承載符記，以便收集器可以呼叫 Amazon ECR Public 以取得最新的更新。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "arsenal:RegisterOnPremisesAgent"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ecr-public:DescribeImages"
            ],
            "Resource": "arn:aws:ecr-
public::446372222237:repository/6e5498e4-8c31-4f57-9991-13b4b992ff7b"
        },
```

```
        {
            "Effect": "Allow",
            "Action": [
                "ecr-public:GetAuthorizationToken"

            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "mgh:GetHomeRegion"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "sts:GetServiceBearerToken"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS 受管政策：AWSApplicationDiscoveryAgentAccess

`AWSApplicationDiscoveryAgentAccess` 政策授予 Application Discovery Agent 註冊和與 Application Discovery Service 通訊的存取權。

您可以將此政策連接到任何使用者，其登入資料由 Application Discovery Agent 使用。

此政策也會授予使用者 Arsenal 的存取許可。Arsenal 是由 管理和託管的代理程式服務 AWS。Arsenal 會將資料轉送至雲端中的 Application Discovery Service。如需此政策的範例，請參閱 [授予對探索代理程式的存取權]。

AWS 受管政策：AWSAgentlessDiscoveryService

此`AWSAgentlessDiscoveryService`政策會授予在 VMware vCenter Server 中執行的無 AWS 代理程式 Discovery Connector 存取權，以註冊、與 Application Discovery Service 通訊和共用連接器運作狀態指標。

您將此政策連接到其登入資料要為連接器所使用的任何使用者。

AWS 受管政策：ApplicationDiscoveryServiceContinuousExportServiceRolePolicy

如果您的 IAM 帳戶已連接 AWSApplicationDiscoveryServiceFullAccess 政策，則當您在 Amazon Athena 中開啟資料探索時ApplicationDiscoveryServiceContinuousExportServiceRolePolicy， 會自動連接到您的帳戶。

此政策允許 AWS Application Discovery Service 建立 Amazon Data Firehose 串流，以將 AWS Application Discovery Service 客服人員收集的資料轉換和交付至您 AWS 帳戶中的 Amazon S3 儲存貯體。

此外，此政策 AWS Glue Data Catalog 會使用名為 application_discovery_service_database 的新資料庫和資料表結構描述來建立 ，以映射客服人員所收集的資料。如需此政策的範例，請參閱 授予代理程式資料收集的許可。

AWS 受管政策：AWSDiscoveryContinuousExportFirehosePolicy

在 Amazon Athena 中使用資料探勘需要此AWSDiscoveryContinuousExportFirehosePolicy政策。它允許 Amazon Data Firehose 將從 Application Discovery Service 收集的資料寫入 Amazon S3。如需有關使用此政策的資訊，請參閱 建立 AWSApplicationDiscoveryServiceFirehose 角色。如需此政策的範例，請參閱 授予資料探勘的許可。

建立 AWSApplicationDiscoveryServiceFirehose 角色

管理員會將受管政策連接至您的 IAM 使用者帳戶。使用AWSDiscoveryContinuousExportFirehosePolicy政策時，管理員必須先建立名為 AWSApplicationDiscoveryServiceFirehose 的角色，並將 Firehose 做為信任的實體，然後將AWSDiscoveryContinuousExportFirehosePolicy政策連接至角色，如下列程序所示。

建立 AWSApplicationDiscoveryServiceFirehose IAM 角色

1. 在 IAM 主控台中，選擇導覽窗格中的角色。
2. 選擇建立角色。
3. 選擇 Kinesis (Kinesis)。
4. 選擇 Kinesis Firehose (Kinesis Firehose) 做為您的使用案例。
5. 選擇下一步：許可。
6. 在 Filter Policies (篩選條件政策) 下搜尋 AWSDiscoveryContinuousExportFirehosePolicy。

7. 選取 AWSDiscoveryContinuousExportFirehosePolicy 旁邊的方塊，然後選擇 Next: Review (下一步：檢閱)。
8. 輸入 AWSApplicationDiscoveryServiceFirehose 做為角色名稱，然後選擇 Create role (建立角色)。

AWS 受管政策的應用程式探索服務更新

檢視自此服務開始追蹤這些變更以來，Application Discovery Service AWS 受管政策更新的詳細資訊。如需有關此頁面變更的自動提醒，請訂閱 的文件歷史記錄 AWS Application Discovery Service 頁面的 RSS 摘要。

變更	描述	日期
AWSApplicationDiscoveryAgentlessCollectorAccess – 無代理程式收集器啟動時提供的新政策	Application Discovery Service 新增了新的受管政策`AWSApplicationDiscoveryAgentlessCollectorAccess` ，授予 Agentless Collector 註冊和與 Application Discovery Service 通訊，以及與其他 AWS 服務通訊的存取權。	2022 年 8 月 16 日
Application Discovery Service 已開始追蹤變更	Application Discovery Service 開始追蹤其 AWS 受管政策的變更。	2021 年 3 月 1 日

AWS Application Discovery Service 身分型政策範例

根據預設，IAM 使用者和角色沒有建立或修改 Application Discovery Service 資源的許可。他們也無法使用 AWS Management Console AWS CLI或 AWS API 來執行任務。IAM 管理員必須建立 IAM 政策，授予使用者和角色在指定資源上執行特定 API 作業的所需許可。管理員接著必須將這些政策連接至需要這些許可的 IAM 使用者或群組。

若要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》中的在 JSON 標籤上建立政策。

主題

政策最佳實務

以身分為基礎的政策會判斷是否有人可以在您的帳戶中建立、存取或刪除 Application Discovery Service 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 AWS 受管政策，將許可授予許多常見使用案例。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，以進一步減少許可。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 使用服務動作，您也可以使用條件來授予存取服務動作的權限 AWS 服務，例如 AWS 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 以增加安全性。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》https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_configure-api-require.html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。

授予 Application Discovery Service 的完整存取權

AWSApplicationDiscoveryServiceFullAccess 受管政策會授予 IAM 使用者帳戶對 Application Discovery Service 和 Migration Hub APIs存取權。

已將此政策連接至其帳戶的 IAM 使用者可設定 Application Discovery Service、啟動和停止代理程式、啟動和停止無代理程式探索，以及從 AWS Discovery Service 資料庫查詢資料。如需此政策的詳細資訊，請參閱 AWS 的 受管政策 AWS Application Discovery Service。

Example AWSApplicationDiscoveryServiceFullAccess 政策

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "mgh:*",
                "discovery:*"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "iam:GetRole"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

授予對探索代理程式的存取權

AWSApplicationDiscoveryAgentAccess 受管政策授予 Application Discovery Agent 註冊和與 Application Discovery Service 通訊的存取權。如需此政策的詳細資訊，請參閱 AWS 的 受管政策 AWS Application Discovery Service。

將此政策連接至任何使用者，其登入資料由 Application Discovery Agent 使用。

此政策也會授予使用者 Arsenal 的存取許可。Arsenal 是由 管理和託管的代理程式服務 AWS。Arsenal 會將資料轉送至雲端中的 Application Discovery Service。

Example AWSApplicationDiscoveryAgentAccess 政策

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

授予代理程式資料收集的許可

ApplicationDiscoveryServiceContinuousExportServiceRolePolicy 受管政策允許 AWS Application Discovery Service 建立 Amazon Data Firehose 串流，以將 Application Discovery Service 代理程式收集的資料轉換和交付至您 AWS 帳戶中的 Amazon S3 儲存貯體。

此外，此政策會使用名為 的新資料庫`application_discovery_service_database`和資料表結構描述來建立 AWS Glue Data Catalog，以映射客服人員所收集的資料。

如需有關使用此政策的資訊，請參閱 AWS 的 受管政策 AWS Application Discovery Service。

Example ApplicationDiscoveryServiceContinuousExportServiceRolePolicy

```
{
   "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "glue:CreateDatabase",
                "glue:UpdateDatabase",
                "glue:CreateTable",
                "glue:UpdateTable",
                "firehose:CreateDeliveryStream",
```

```
                "firehose:DescribeDeliveryStream",
                "logs:CreateLogGroup"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "firehose:DeleteDeliveryStream",
                "firehose:PutRecord",
                "firehose:PutRecordBatch",
                "firehose:UpdateDestination"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:firehose:*:*:deliverystream/aws-application-discovery-
service*"
        },
        {
            "Action": [
                "s3:CreateBucket",
                "s3:ListBucket",
                "s3:PutBucketLogging",
                "s3:PutEncryptionConfiguration"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::aws-application-discovery-service*"
        },
        {
            "Action": [
                "s3:GetObject"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::aws-application-discovery-service*/*"
        },
        {
            "Action": [
                "logs:CreateLogStream",
                "logs:PutRetentionPolicy"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:logs:*:*:log-group:/aws/application-discovery-service/
firehose*"
        },
        {
```

```
            "Action": [
                "iam:PassRole"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:iam::*:role/AWSApplicationDiscoveryServiceFirehose",
            "Condition": {
                "StringLike": {
                    "iam:PassedToService": "firehose.amazonaws.com"
                }
            }
        },
        {
            "Action": [
                "iam:PassRole"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:iam::*:role/service-role/
AWSApplicationDiscoveryServiceFirehose",
            "Condition": {
                "StringLike": {
                    "iam:PassedToService": "firehose.amazonaws.com"
                }
            }
        }
    ]
}
```

授予資料探勘的許可

在 Amazon Athena 中使用資料探勘需要 AWSDiscoveryContinuousExportFirehosePolicy 政策。它允許 Amazon Data Firehose 將從 Application Discovery Service 收集的資料寫入 Amazon S3。如需有關使用此政策的資訊，請參閱 建立 AWSApplicationDiscoveryServiceFirehose 角色。

Example AWSDiscoveryContinuousExportFirehosePolicy

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

```
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:AbortMultipartUpload",
                "s3:GetBucketLocation",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:ListBucketMultipartUploads",
                "s3:PutObject"
            ],
            "Resource": [
                "arn:aws:s3:::aws-application-discovery-service-*",
                "arn:aws:s3:::aws-application-discovery-service-*/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "logs:PutLogEvents"
            ],
            "Resource": [
                "arn:aws:logs:*:*:log-group:/aws/application-discovery-service/
firehose:log-stream:*"
            ]
        }
    ]
}
```

授予使用 Migration Hub 主控台網路圖表的許可

若要在建立允許或拒絕存取 Application Discovery Service 或 Migration Hub 的身分型政策時授予 AWS Migration Hub 主控台網路圖表的存取權，您可能需要將 `discovery:GetNetworkConnectionGraph`動作新增至政策。

您必須在新政策中使用 `discovery:GetNetworkConnectionGraph`動作，或更新舊政策，如果政策符合下列條件：

- 此政策允許或拒絕對 Application Discovery Service 或 Migration Hub 的存取。
- 政策會使用一個更特定的探索動作，例如 `discovery:`*`action-name`* 而非 來授予存取許可`discovery:*`。

下列範例示範如何在 IAM 政策中使用 `discovery:GetNetworkConnectionGraph`動作。

Example

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

如需有關 Migration Hub 網路圖表的資訊，請參閱在 Migration Hub 中檢視網路連線。

使用 Application Discovery Service 的服務連結角色

AWS Application Discovery Service 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 Application Discovery Service 的唯一 IAM 角色類型。服務連結角色由 Application Discovery Service 預先定義，並包含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輕鬆地設定 Application Discovery Service，因為您不需要手動新增必要的許可。Application Discovery Service 會定義其服務連結角色的許可，除非另有定義，否則只有 Application Discovery Service 可以擔任其角色。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 Application Discovery Service 資源，因為您不會意外移除存取資源的許可。

主題

- Application Discovery Service 的服務連結角色許可
- 為 Application Discovery Service 建立服務連結角色
- 刪除 Application Discovery Service 的服務連結角色

如需關於支援服務連結角色的其他服務的資訊，請參閱可搭配 IAM 運作的AWS 服務，並尋找 Service-Linked Role (服務連結角色) 欄顯示為 Yes (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。

Application Discovery Service 的服務連結角色許可

Application Discovery Service 使用名為 AWSServiceRoleForApplicationDiscoveryServiceContinuousExport 的服務連結角色 – 啟用存取使用或管理 AWS 的服務和資源 AWS Application Discovery Service。

AWSServiceRoleForApplicationDiscoveryServiceContinuousExport 服務連結角色信任下列服務擔任該角色：

- `continuousexport.discovery.amazonaws.com`

角色許可政策允許 Application Discovery Service 完成下列動作：

glue

- `CreateDatabase`
- `UpdateDatabase`
- `CreateTable`
- `UpdateTable`

firehose

- `CreateDeliveryStream`
- `DeleteDeliveryStream`
- `DescribeDeliveryStream`
- `PutRecord`
- `PutRecordBatch`
- `UpdateDestination`

s3

- `CreateBucket`
- `ListBucket`
- `GetObject`

日誌

CreateLogGroup

CreateLogStream

PutRetentionPolicy

iam

PassRole

此為顯示以上動作可套用於哪些資源的完整政策：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "glue:CreateDatabase",
                "glue:UpdateDatabase",
                "glue:CreateTable",
                "glue:UpdateTable",
                "firehose:CreateDeliveryStream",
                "firehose:DescribeDeliveryStream",
                "logs:CreateLogGroup"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "firehose:DeleteDeliveryStream",
                "firehose:PutRecord",
                "firehose:PutRecordBatch",
                "firehose:UpdateDestination"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:firehose:*:*:deliverystream/aws-application-discovery-
service*"
        },
        {
            "Action": [
                "s3:CreateBucket",
```

```
                "s3:ListBucket",
                "s3:PutBucketLogging",
                "s3:PutEncryptionConfiguration"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::aws-application-discovery-service*"
        },
        {
            "Action": [
                "s3:GetObject"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::aws-application-discovery-service*/*"
        },
        {
            "Action": [
                "logs:CreateLogStream",
                "logs:PutRetentionPolicy"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:logs:*:*:log-group:/aws/application-discovery-service/
firehose*"
        },
        {
            "Action": [
                "iam:PassRole"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:iam::*:role/AWSApplicationDiscoveryServiceFirehose",
            "Condition": {
                "StringLike": {
                    "iam:PassedToService": "firehose.amazonaws.com"
                }
            }
        },
        {
            "Action": [
                "iam:PassRole"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:iam::*:role/service-role/
AWSApplicationDiscoveryServiceFirehose",
            "Condition": {
                "StringLike": {
```

```
                    "iam:PassedToService": "firehose.amazonaws.com"
                }
            }
        }
    ]
}
```

您必須設定許可，IAM 實體 (如使用者、群組或角色) 才可建立、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 Application Discovery Service 建立服務連結角色

您不需要手動建立一個服務連結角色。當您使用 CLI 呼叫 StartContinuousExport API 時，在選擇「開始資料收集」或按一下標記為「在 Athena 中探索資料」或 b) 的滑桿後，當 a) 隱含開啟持續匯出時，會自動建立 AWSServiceRoleForApplicationDiscoveryServiceContinuousExport StartContinuousExport AWS 服務連結角色，確認從資料收集器頁面呈現的對話方塊中的選項。

> **Important**
>
> 此服務連結角色可以顯示在您的帳戶，如果您於其他服務中完成一項動作時，可以使用支援此角色的功能。若要進一步了解，請參閱我的 IAM 帳戶中出現的新角色。

從 Migration Hub 主控台建立服務連結角色

您可以使用 Migration Hub 主控台來建立 AWSServiceRoleForApplicationDiscoveryServiceContinuousExport 服務連結角色。

建立該服務連結角色 (主控台)

1. 在導覽窗格中，選擇 Data Collectors (資料收集器)。
2. 選擇 Agents (代理程式) 索引標籤。
3. 將 Athena 滑桿中的資料探索切換到開啟位置。
4. 在上一步驟產生的對話方塊中，按一下核取方塊以同意相關成本並選擇 Continue (繼續) 或 Enable (啟用)。

從 建立服務連結角色 AWS CLI

您可以從 使用 Application Discovery Service 命令 AWS Command Line Interface 來建立 AWSServiceRoleForApplicationDiscoveryServiceContinuousExport 服務連結角色。

當您從 啟動連續匯出時，會自動建立此服務連結角色 AWS CLI (AWS CLI 必須先在環境中安裝)。

從 開始連續匯出，以建立服務連結角色 (CLI) AWS CLI

1. AWS CLI 為您的作業系統 (Linux、macOS 或 Windows) 安裝 。如需說明，請參閱 AWS Command Line Interface 使用者指南。
2. 開啟命令提示字元 (Windows) 或終端機 (Linux 或 macOS)。
   a. 輸入 `aws configure` 然後按 Enter 鍵。
   b. 輸入您的 AWS 存取金鑰 ID 和 AWS 私密存取金鑰。
   c. 輸入預設區域名稱的 `us-west-2`。
   d. 輸入預設輸出格式的 `text`。
3. 鍵入以下命令：

```
aws discovery start-continuous-export
```

您也可以使用 IAM 主控台，透過 Discovery Service - Continuous Export 使用案例建立服務連結角色。在 IAM CLI 或 IAM API 中，建立一個使用 `continuousexport.discovery.amazonaws.com` 服務名稱的服務連結角色。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。

刪除 Application Discovery Service 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。然而，務必清除您的服務連結角色，之後才能以手動方式將其刪除。

清除 服務連結角色

在您使用 IAM 刪除服務連結角色之前，您必須先刪除該角色所使用的任何資源。

> **Note**
>
> 如果 Application Discovery Service 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。

從 Migration Hub 主控台刪除 AWSServiceRoleForApplicationDiscoveryServiceContinuousExport 服務連結角色所使用的 Application Discovery Service 資源

1. 在導覽窗格中，選擇 Data Collectors (資料收集器)。
2. 選擇 Agents (代理程式) 索引標籤。
3. 將 Athena 滑桿中的資料探索切換到關閉位置。

從 刪除 AWSServiceRoleForApplicationDiscoveryServiceContinuousExport 服務連結角色所使用的 Application Discovery Service 資源 AWS CLI

1. AWS CLI 為您的作業系統 (Linux、macOS 或 Windows) 安裝 。如需說明，請參閱 AWS Command Line Interface 使用者指南。
2. 開啟命令提示字元 (Windows) 或終端機 (Linux 或 macOS)。
   a. 輸入 `aws configure` 然後按 Enter 鍵。
   b. 輸入您的 AWS 存取金鑰 ID 和 AWS 私密存取金鑰。
   c. 輸入預設區域名稱的 `us-west-2`。
   d. 輸入預設輸出格式的 `text`。
3. 鍵入以下命令：

```
aws discovery stop-continuous-export --export-id <export ID>
```

   - 如果您不知道想停止之持續匯出的匯出 ID，請輸入下列命令，以查看持續匯出的 ID：

```
aws discovery describe-continuous-exports
```

4. 輸入下列命令，確認其傳回狀態為「INACTIVE」，以確保持續匯出已停止：

```
aws discovery describe-continuous-export
```

手動刪除服務連結角色

您可以使用 IAM 主控台、IAM CLI 或 IAM API 來刪除 AWSServiceRoleForApplicationDiscoveryServiceContinuousExport 服務連結角色。如果您不再需要使用需要此服務連結角色的 Discovery Service - Continuous Export 功能，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。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。

> **Note**
>
> 您必須先清除您的服務連結角色才能將其刪除。請參閱清除 服務連結角色。

對 AWS Application Discovery Service Identity and Access 進行故障診斷

使用下列資訊來協助您診斷和修正使用 Application Discovery Service 和 IAM 時可能遇到的常見問題。

主題

- 我未獲得執行 iam：PassRole 的授權

我未獲得執行 iam：PassRole 的授權

如果您收到錯誤，表示您無權執行`iam:PassRole`動作，則必須更新您的政策，以允許您將角色傳遞給 Application Discovery Service。

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 Application Discovery Service 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 沒有將角色傳遞至該服務的許可。

```
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。

使用 記錄應用程式探索服務 API 呼叫 AWS CloudTrail

AWS Application Discovery Service 已與 整合 AWS CloudTrail，此服務提供使用者、角色或 Application Discovery Service 中 AWS 服務所採取動作的記錄。您可以使用 CloudTrail 記錄、持續監控和保留帳戶活動，以進行疑難排解和稽核。CloudTrail 提供 AWS 帳戶活動的事件歷史記錄，包括透過 AWS Management Console、 AWS SDKs和命令列工具採取的動作。

CloudTrail 會將 Application Discovery Service 的所有 API 呼叫擷取為事件。擷取的呼叫包括從 Application Discovery Service 主控台進行的呼叫，以及對 Application Discovery Service API 操作的程式碼呼叫。

如果您建立追蹤，則可以啟用 CloudTrail 事件持續交付至 Amazon S3 儲存貯體，包括 Application Discovery Service 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 收集的資訊，您可以判斷對 Application Discovery Service 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」。

CloudTrail 中的應用程式探索服務資訊

當您建立 AWS 帳戶時，會在您的帳戶上啟用 CloudTrail。當活動在 Application Discovery Service 中發生時，該活動會記錄於 CloudTrail 事件，以及事件歷史記錄中的其他服務 AWS 事件。您可以在 AWS 帳戶中檢視、搜尋和下載最近的事件。如需詳細資訊，請參閱《使用 CloudTrail 事件歷史記錄檢視事件》https://docs.aws.amazon.com/awscloudtrail/latest/userguide/view-cloudtrail-events.html。

若要持續記錄您 AWS 帳戶中的事件，包括 Application Discovery Service 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。根據預設，當您在主控台中建立追蹤時，追蹤會套用至所有 AWS 區域。追蹤會記錄 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 CloudTrail 日誌中收集的事件資料並對其採取行動。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
- 從多個區域接收 CloudTrail 日誌檔案，以及從多個帳戶接收 CloudTrail 日誌檔案

CloudTrail 會記錄所有 Application Discovery Service 動作，並記錄在 Application Discovery Service API 參考中。例如，對 `CreateTags`、`DescribeTags` 以及 `GetDiscoverySummary` 動作發出的呼叫會在 CloudTrail 日誌檔案中產生項目。

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：

- 請求是使用根或 AWS Identity and Access Management (IAM) 使用者登入資料提出。
- 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 Application Discovery Service 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。

以下範例顯示的是展示 `DescribeTags` 動作的 CloudTrail 日誌項目。

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAJBHMC4H6EKEXAMPLE:sample-user",
        "arn": "arn:aws:sts::444455556666:assumed-role/ReadOnly/sample-user",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDAJQABLZS4A3QDU576Q",
                "arn": "arn:aws:iam::444455556666:role/ReadOnly",
                "accountId": "444455556666",
                "userName": "sampleAdmin"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2020-05-05T15:19:03Z"
```

```
            }
        }
    },
    "eventTime": "2020-05-05T17:02:40Z",
    "eventSource": "discovery.amazonaws.com",
    "eventName": "DescribeTags",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "20.22.33.44",
    "userAgent": "Coral/Netty4",
    "requestParameters": {
        "maxResults": 0,
        "filters": [
            {
                "values": [
                    "d-server-0315rfdjreyqsq"
                ],
                "name": "configurationId"
            }
        ]
    },
    "responseElements": null,
    "requestID": "mgh-console-eb1cf315-e2b4-4696-93e5-b3a3b9346b4b",
    "eventID": "7b32b778-91c9-4c75-9cb0-6c852791b2eb",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

AWS Application Discovery Service ARN 格式

Amazon Resource Name (ARN) 是可唯一識別 AWS 資源的字串。 當您想要明確指定所有資源時，AWS 需要 ARN AWS。 會 AWS Application Discovery Service 定義下列 ARNs。

- 探索代理程式： `arn:aws:discovery:region:account:agent/discovery-agent/agentId`
- 無代理程式收集器： `arn:aws:discovery:region:account:agent/agentless-collector/agentId`
- 遷移評估器收集器： `arn:aws:discovery:region:account:agent/migration-evaluator-collector/agentId`
- Discovery Connector： `arn:aws:discovery:region:account:agent/discovery-connector/agentId`

AWS Application Discovery Service 配額

Service Quotas AWS Application Discovery Service 主控台提供配額的相關資訊。您可以使用 Service Quotas 主控台來檢視預設的服務配額，或請求增加可調整配額的配額。

目前，唯一可以增加的配額是每個帳戶的匯入伺服器。

Application Discovery Service 具有下列預設配額：

- 每個帳戶 1，000 個應用程式。

  如果您達到此配額，並想要匯入新的應用程式，您可以使用 `DeleteApplications` API 動作刪除現有的應用程式。如需詳細資訊，請參閱 Application Discovery Service API 參考中的 DeleteApplications。
- 每個匯入檔案的檔案大小上限為 10 MB。
- 每個帳戶 25，000 個匯入的伺服器記錄。
- 每天刪除 25，000 個匯入記錄。
- 每個帳戶 10，000 個匯入的伺服器 （您可以請求提高此配額）。
- 1，000 個作用中代理程式，這些代理程式正在收集資料並將其傳送至 Application Discovery Service。
- 10，000 個非作用中代理程式，這些代理程式回應迅速，但不會收集資料。
- 每個應用程式 400 個伺服器。
- 每個伺服器 30 個標籤。

故障診斷 AWS Application Discovery Service

在本節中，您可以找到有關如何修正 AWS Application Discovery Service常見問題的相關資訊。

主題

依資料探勘停止資料收集

若要停止資料探勘，您可以在探索 > 資料收集器 > 代理程式索引標籤下的 Migration Hub 主控台中關閉切換開關，或叫用 `StopContinuousExport` API。停止資料收集最多可能需要 30 分鐘，在此階段，主控台上的切換開關和 `DescribeContinuousExport` API 調用將顯示資料探索狀態為「停止進行中」。

> **Note**
>
> 若重新整理主控台頁面後，該切換並沒有關閉且擲回錯誤訊息，或是 `DescribeContinuousExport` API 傳回「Stop_Failed」狀態，則您可以透過將開關切換為關閉，或呼叫 `StopContinuousExport` API 以再次嘗試。如果「資料探勘」仍顯示錯誤且無法成功停止，請聯絡 AWS 支援。

或者，您可以手動停止資料集合，如以下步驟所述。

選項 1：停止代理程式資料集合

如果您已經使用 ADS 代理程式完成探索，且不再需要收集 ADS 資料庫儲存庫裡的其他資料：

1. 從 Migration Hub 主控台選擇探索 > 資料收集器 > 代理程式索引標籤。
2. 選取所有現有執行中的代理程式，然後選擇 Stop Data Collection (停止資料集合)。

   這可確保代理程式在 ADS 資料儲存庫和您的 S3 儲存貯體中並沒有收集新資料。您現有的資料仍然可存取。

選項 2：刪除資料探勘的 Amazon Kinesis Data Streams

如果您想要繼續在 ADS 資料儲存庫中由客服人員收集資料，但不想使用資料探勘在 Amazon S3 儲存貯體中收集資料，您可以手動刪除資料探勘建立的 Amazon Data Firehose 串流：

1. 從 AWS 主控台登入 Amazon Kinesis，然後從導覽窗格中選擇 Data Firehose。
2. 刪除資料探索功能建立的下列串流：

   - `aws-application-discovery-service-id_mapping_agent`
   - `aws-application-discovery-service-inbound_connection_agent`
   - `aws-application-discovery-service-network_interface_agent`
   - `aws-application-discovery-service-os_info_agent`
   - `aws-application-discovery-service-outbound_connection_agent`
   - `aws-application-discovery-service-processes_agent`
   - `aws-application-discovery-service-sys_performance_agent`

移除資料探勘所收集的資料

移除資料探勘所收集的資料

1. 移除存放在 Amazon S3 中的探索代理程式資料。

   AWS Application Discovery Service (ADS) 收集的資料會存放在名為 的 S3 儲存貯體中`aws-application-discover-discovery-service-`*`uniqueid`*。

   > **Note**
   >
   > 啟用 Amazon Athena 中的資料探勘時，刪除 Amazon S3 儲存貯體或其任何物件會導致錯誤。 Amazon Athena 它會繼續將新的探索代理程式資料傳送至 S3。刪除的資料也無法在 Athena 中存取。

2. 移除 AWS Glue Data Catalog。

   開啟 Amazon Athena 中的資料探勘時，它會在您的帳戶中建立 Amazon S3 儲存貯體，以定期存放 ADS 代理程式收集的資料。此外，它也會建立 AWS Glue Data Catalog ，讓您從 Amazon Athena 查詢存放在 Amazon S3 儲存貯體中的資料。 Amazon Athena 當您在 Amazon Athena 中

關閉資料探勘時，Amazon S3 儲存貯體中不會儲存任何新資料，但先前收集的資料會保留。如果您不再需要此資料，並想要在開啟 Amazon Athena 中的資料探勘之前，將您的帳戶返回 狀態。

a. 從 AWS 主控台造訪 Amazon S3，並手動刪除名為 "aws-application-discover-discovery-service-uniqueid" 的儲存貯體

b. 您可以刪除 application-discovery-service-database 資料庫和下列所有資料表，手動移除資料探 AWS 勘 Glue Data Catalog：

- `os_info_agent`
- `network_interface_agent`
- `sys_performance_agent`
- `processes_agent`
- `inbound_connection_agent`
- `outbound_connection_agent`
- `id_mapping_agent`

從 移除您的資料 AWS Application Discovery Service

若要從 Application Discovery Service 中移除所有資料，請聯絡 AWS Support 並請求刪除完整資料。

修正 Amazon Athena 中資料探勘的常見問題

在本節中，您可以找到如何在 Amazon Athena 中修正資料探勘常見問題的相關資訊。

主題

Amazon Athena 中的資料探索無法啟動，因為無法建立服務連結角色和所需 AWS 資源

當您在 Amazon Athena 中開啟資料探勘時，它會在您的帳戶中建立服務連結角色 `AWSServiceRoleForApplicationDiscoveryServiceContinuousExport`，以允許它建立必要的 AWS 資源，以便在 Amazon Athena 中存取代理程式收集的資料，包括 Amazon S3 儲存貯

體、Amazon Kinesis 串流和 AWS Glue Data Catalog。如果您的帳戶沒有在 Amazon Athena 中建立此角色的正確資料探勘許可，將無法初始化。請參閱AWS 的 受管政策 AWS Application Discovery Service。

Amazon Athena 中不會顯示新的客服人員資料

如果新資料未流入 Athena，自客服人員啟動以來已超過 30 分鐘，且資料探勘狀態為作用中，請檢查下列解決方案：

- AWS 探索代理程式

  確認您代理程式的 Collection (收集) 狀態標示為 Started (已開始) 且 Health (運作狀態) 狀態標示為 Running (執行中)。

- Kinesis 角色

  請確認您的帳戶中擁有 `AWSApplicationDiscoveryServiceFirehose` 角色。

- Firehose 狀態

  確定下列 Firehose 交付串流正常運作：

  - `aws-application-discovery-service/os_info_agent`
  - `aws-application-discovery-service-network_interface_agent`
  - `aws-application-discovery-service-sys_performance_agent`
  - `aws-application-discovery-service-processes_agent`
  - `aws-application-discovery-service-inbound_connection_agent`
  - `aws-application-discovery-service-outbound_connection_agent`
  - `aws-application-discovery-service-id_mapping_agent`

- AWS Glue Data Catalog

  確定`application-discovery-service-database`資料庫位於其中 AWS Glue。請確定以下資料表存在 AWS Glue中：

  - `os_info_agent`
  - `network_interface_agent`
  - `sys_performance_agent`

- `processes_agent`
- `inbound_connection_agent`
- `outbound_connection_agent`
- `id_mapping_agent`

- Amazon S3 儲存貯體

  請確定您的帳戶`aws-application-discovery-service-`*`uniqueid`*中有名為 的 Amazon S3 儲存貯體。如果儲存貯體中的物件已移動或刪除，則無法在 Athena 中正常顯示。

- 您的現場部署伺服器

  請確認您的伺服器正在執行中，以便您的代理程式可以收集並傳送資料至 AWS Application Discovery Service。

您沒有足夠的許可來存取 Amazon S3、Amazon Data Firehose 或 AWS Glue

如果您在 Amazon Athena 中使用 AWS Organizations和初始化資料探勘失敗，可能是因為您沒有存取 Amazon S3、Amazon Data Firehose、Athena 或 的許可 AWS Glue。

您需要具有管理員許可的 IAM 使用者，才能授予您對這些服務的存取權。管理員可以使用其帳戶來授予此存取權限。請參閱 AWS 的 受管政策 AWS Application Discovery Service。

為了確保 Amazon Athena 中的資料探勘正常運作，請勿修改或刪除 Amazon Athena 中資料探勘建立 AWS 的資源，包括 Amazon S3 儲存貯體、Amazon Data Firehose Streams 和 AWS Glue Data Catalog。如果您不小心刪除或修改了這些資源，請停止並開始資料探勘，以讓它自動重新建立這些資源。如果您刪除資料探勘建立的 Amazon S3 儲存貯體，您可能會遺失在儲存貯體中收集的資料。

對失敗的匯入記錄進行故障診斷

Migration Hub 匯入可讓您直接將內部部署環境的詳細資訊匯入 Migration Hub，而無需使用 Discovery Connector 或 Discovery Agent。這可讓您選擇直接從匯入的資料執行遷移評估和規劃。您也可以將裝置群組為應用程式並追蹤其遷移狀態。

當您匯入資料時可能會發生錯誤。這些錯誤通常會因下列其中一個原因發生：

- 已達到匯入相關配額 – 有與匯入任務相關聯的配額。如果您提出的匯入任務請求會超過配額，則請求將會失敗並傳回錯誤。如需詳細資訊，請參閱AWS Application Discovery Service 配額。
- 匯入檔案中插入了額外的逗號 (,) – .CSV 檔案中的逗號用於區分一個欄位與下一個欄位。在欄位中出現逗號是不被支援的，因為這將會分割欄位。這可能會導致一連串的格式錯誤。請確定只有在欄位之間使用逗號，而且不會用於匯入檔案中。
- 欄位具有超出其支援範圍的值 – 有些欄位，例如 `CPU.NumberOfCores` 必須具有其支援的值範圍。如果數值超出或低於此支援範圍，將無法匯入其記錄。

如果您的匯入請求發生任何錯誤，您可以下載匯入任務的失敗記錄，接著解決失敗項目 CSV 檔案中的錯誤，然後再次執行匯入以解決此問題。

Console

下載失敗記錄存檔

1. 登入 AWS Management Console，並在 開啟 Migration Hub 主控台https://console.aws.amazon.com/migrationhub。
2. 在左側導覽中的 Discover (探索) 下，選擇 Tools (工具)。
3. 從 Discovery (探索) 中選擇 view imports (檢視匯入)。
4. 從 Imports (匯入) 儀表板選擇與匯入請求相關且包含一些數字的 Failed records (失敗記錄) 選項按鈕。
5. 在儀表板的表格上方選擇 Download failed records (下載失敗記錄)。這將開啟您瀏覽器的下載對話方塊，以下載存檔檔案。

AWS CLI

下載失敗記錄存檔

1. 請開啟終端機視窗並輸入下列命令，*`ImportName`* `is the name of the import task with the failed entries that you want to correct.`：

```
aws discovery describe-import-tasks - -name ImportName
```

2. 從輸出複製 `errorsAndFailedEntriesZip` 傳回值的所有內容，不包括前後的引號。
3. 開啟 Web 瀏覽器，並將此內容貼到 URL 文字方塊，然後按下 ENTER。這會下載 .zip 壓縮格式的失敗記錄存檔。

現在您已下載失敗記錄存檔，接下來可以解壓縮其中的兩個檔案並修正錯誤。請注意，如果您的錯誤與基於服務的限制有關，您將必須請求增加上限或刪除足夠的相關資源，讓您的帳戶低於限制。存檔有以下檔案：

- errors-file.csv – 此檔案是您的錯誤日誌，它會追蹤每個失敗項目之每個失敗記錄的行、欄名稱`ExternalId`、 和描述性錯誤訊息。
- failed-entries-file.csv – 此檔案僅包含原始匯入檔案中失敗的項目。

若要修正您遇到的非基於限制的錯誤，請使用 `errors-file.csv` 修正 `failed-entries-file.csv` 檔案中的問題，然後匯入該檔案。如需匯入檔案的詳細資訊，請參閱匯入 資料。

的文件歷史記錄 AWS Application Discovery Service

最新使用者指南文件更新日期：2023 年 5 月 16 日

下表說明 2019 年 1 月 18 日之後 Application Discovery Service 使用者指南的重要變更。如需有關文件更新的通知，您可以訂閱 RSS 摘要。

變更	描述	日期
從 Discovery Connector 轉換至 Agentless Collector	我們建議目前使用 Discovery Connector 的客戶轉換至新的無代理程式收集器。自 2025 AWS Application Discovery Service 年 11 月 17 日起，將停止接受來自 Discovery Connectors 的新資料。如需詳細資訊，請參閱 Discovery Connector。	2024 年 11 月 12 日
發行 Agentless Collector Network Data Collection 模組	網路資料收集模組可讓您探索現場部署資料中心伺服器之間的相依性。如需詳細資訊，請參閱使用 Agentless Collector Network Data Collection 模組。	2024 年 11 月 8 日
支援無代理程式集合以進行相依性映射	如需詳細資訊，請參閱使用 VMware vCenter Agentless Collector 資料收集模組。	2024 年 10 月 24 日
以 Amazon Linux 2023 為基礎的發行版 Agentless Collector 第 2 版	如需詳細資訊，請參閱無代理程式收集器的先決條件。	2024 年 9 月 26 日
更新的 Agentless Collector 先決條件	如需詳細資訊，請參閱無代理程式收集器的先決條件。	2024 年 9 月 9 日

API 中的最終一致性	如需詳細資訊，請參閱 AWS Application Discovery Service API 中的最終一致性。	2024 年 6 月 20 日
無代理程式收集器更新	我們已將 sts.amazonaws.com 新增至需要傳出存取的網域清單。如需詳細資訊，請參閱設定防火牆以傳出存取 AWS 網域。	2024 年 6 月 20 日
若要分開存取，請建立並使用個別的 AWS 帳戶。	如需詳細資訊，請參閱 AWS Application Discovery Service 的動作、資源和條件金鑰。	2024 年 4 月 5 日
介紹 Agentless Collector 資料庫和分析資料收集模組	資料庫和分析資料收集模組是 Application Discovery Service Agentless Collector (Agentless Collector) 的新模組。您可以使用此資料收集模組來連線至您的環境，並從內部部署資料庫和分析伺服器收集中繼資料和效能指標。如需詳細資訊，請參閱資料庫和分析資料收集模組。	2023 年 5 月 16 日
Application Discovery Service Agentless Collector 簡介	Application Discovery Service Agentless Collector AWS Application Discovery Service (Agentless Collector) 是新的內部部署應用程式，可透過無代理程式方法來收集內部部署環境的相關資訊，協助您有效地規劃遷移至 AWS 雲端。如需詳細資訊，請參閱 Agentless Collector。	2022 年 8 月 16 日

IAM 更新	AWS Identity and Access Management (IAM) `discovery:GetNetworkConnectionGraph` 動作現在可用於在建立身分型政策時授予 AWS Migration Hub 主控台網路圖表的存取權。如需詳細資訊，請參閱授予使用網路圖表的許可。	2022 年 5 月 24 日
主區域簡介	Migration Hub 主區域提供整個產品組合的探索和遷移規劃資訊的單一儲存庫，以及遷移至多個 AWS 區域的單一檢視。	2019 年 11 月 20 日
Migration Hub 匯入功能簡介	Migration Hub 匯入可讓您將內部部署伺服器和應用程式的相關資訊匯入 Migration Hub，包括伺服器規格和使用率資料。您也可以使用此資料來追蹤應用程式遷移的狀態。如需詳細資訊，請參閱 Migration Hub Import。	2019 年 1 月 18 日

下表說明 2019 年 1 月 18 日之前 Application Discovery Service 使用者指南的文件版本：

變更	描述	日期
新功能	更新文件以支援 Amazon Athena 中的資料探索，並新增故障診斷章節。	2018 年 8 月 09 日
主要修訂版	重寫使用量和輸出詳細資訊，重建整個文件。	2018 年 5 月 25 日
探索代理程式 2.0	發行全新與改進的 Application Discovery 代理程式。	2017 年 10 月 19 日

變更	描述	日期
主控台	AWS Management Console 已新增 。	2016 年 12 月 19 日
無代理程式探索	此版本說明如何設定和配置無代理程式探索。	2016 年 7 月 28 日
適用於 Microsoft Windows Server 的新詳細資訊和命令問題修正	此更新會新增 Microsoft Windows Server 的詳細資訊。也記載各種命令問題的修正。	2016 年 5 月 20 日
初次出版	這是 Application Discovery Service 使用者指南的第一個版本。	2016 年 5 月 12 日

AWS 詞彙表

如需最新的 AWS 術語，請參閱 AWS 詞彙表 參考中的AWS 詞彙表。

Discovery Connector

> **Important**
>
> 我們建議目前使用 Discovery Connector 的客戶轉換至新的無代理程式收集器。自 2025 年 11 月 17 日起， AWS Application Discovery Service 將停止接受來自 Discovery Connectors 的新資料。

本節說明如何從 AWS Agentless Discovery Connector (Discovery Connector) 轉換到 Application Discovery Service Agentless Collector (Agentless Collector)。

我們建議目前使用 Discovery Connector 的客戶轉換至新的無代理程式收集器。

若要了解如何開始使用 Agentless Collector，請參閱 Application Discovery Service 無代理程式收集器。

部署 Agentless Collector 之後，您可以刪除 Discovery Connector 虛擬機器。先前收集的所有資料將繼續在 （遷移中樞） 中使用 AWS Migration Hub 。

使用 Discovery Connector 收集資料

> **Important**
>
> 我們建議目前使用 Discovery Connector 的客戶轉換至新的無代理程式收集器。自 2025 年 11 月 17 日起， AWS Application Discovery Service 將停止接受來自 Discovery Connectors 的新資料。如需詳細資訊，請參閱Discovery Connector。

Discovery Connector 會收集 VMware vCenter Server 主機和 VMs 的相關資訊。不過，必須安裝 VMware vCenter Server 工具，才能擷取此資料。若要確保您正在使用 AWS 的帳戶具有此任務所需的許可，請參閱 AWS 的 受管政策 AWS Application Discovery Service。

接下來，您可以找到 Discovery Connector 所收集的資訊的清查。

Discovery Connector 收集資料的資料表圖例：

- 收集的資料是以千位元組 (KB) 為單位 (除非另有指明)。

- Migration Hub 主控台中的同等資料會以 MB (MB) 為單位報告。
- 以星號 (*) 表示的資料欄位僅適用於從連接器的 API 匯出函數產生的 .csv 檔案。
- 輪詢期間大約為 60 分鐘間隔。
- 以雙星號 (**) 表示的資料欄位目前傳回 null 值。

資料欄位	描述
applicationConfigurationId*	VM 分組所在遷移應用程式的 ID
avgCpuUsagePct	輪詢期間的 CPU 使用量平均百分比
avgDiskBytesReadPerSecond	輪詢期間從磁碟讀取的平均位元組數目
avgDiskBytesWrittenPerSecond	輪詢期間寫入磁碟的平均位元組數目
avgDiskReadOpsPerSecond**	每秒讀取 I/O 操作的平均次數為 null
avgDiskWriteOpsPerSecond**	每秒寫入 I/O 操作的平均次數
avgFreeRAM	平均免費 RAM，以 MB 表示
avgNetworkBytesReadPerSecond	每秒平均讀取位元組輸送量
avgNetworkBytesWrittenPerSecond	每秒平均寫入位元組輸送量
configId	應用程式探索服務指派 ID 給探索的 VM
configType	探索到的資源類型
connectorId	探索連接器虛擬設備的 ID
cpuType	VM 的 vCPU，主機的實際模型
datacenterId	vCenter 的 ID
hostId*	VM 主機的 ID
hostName	執行虛擬化軟體的主機名稱
hypervisor	Hypervisor 的類型

資料欄位	描述
id	伺服器的 ID
lastModifiedTimeStamp*	資料匯出之前資料收集的最新日期和時間
macAddress	VM 的 MAC 地址
manufacturer	虛擬化軟體的製造商
maxCpuUsagePct	CPU 使用量百分比上限 (輪詢期間)
maxDiskBytesReadPerSecond	從磁碟讀取的位元組數目上限 (輪詢期間)
maxDiskBytesWrittenPerSecond	寫入磁碟的位元組數目上限 (輪詢期間)
maxDiskReadOpsPerSecond**	每秒讀取 I/O 操作的次數上限
maxDiskWriteOpsPerSecond**	每秒寫入 I/O 操作的次數上限
maxNetworkBytesReadPerSecond	每秒讀取的位元組輸送量上限
maxNetworkBytesWrittenPerSecond	每秒寫入的位元組輸送量上限
memoryReservation*	避免超量承諾 VM 記憶體的限制
moRefId	唯一 vCenter 受管物件參考 ID
name*	VM 或網路的名稱 (使用者指定)
numCores	CPU 中的獨立處理單元數目
numCpus	VM 上的中央處理單元數目
numDisks**	VM 上的磁碟數目
numNetworkCards**	VM 上的網路卡數目
osName	VM 上的作業系統名稱
osVersion	VM 上的作業系統版本

資料欄位	描述
portGroupId*	VLAN 的成員連接埠群組 ID
portGroupName*	VLAN 的成員連接埠群組名稱
powerState*	電源狀態
serverId	應用程式探索服務指派 ID 給探索的 VM
smBiosId*	系統管理 BIOS 的 ID/版本
state*	探索連接器虛擬設備的狀態
toolsStatus	VMware 工具的操作狀態 (如需完整清單，請參閱在主控台中 AWS Migration Hub 排序資料收集器)。
totalDiskSize	磁碟總容量，以 MB 表示
totalRAM	VM 上的 RAM 總數量，以 MB 表示
type	主機類型
vCenterId	VM 的唯一 ID 號碼
vCenterName*	vCenter 主機的名稱
virtualSwitchName*	虛擬交換器的名稱
vmFolderPath	VM 檔案的目錄路徑
vmName	虛擬機器的名稱

收集 Discovery Connector 資料

在 VMware 環境中部署和設定 Discovery Connector 之後，如果停止，您可以重新啟動資料收集。您可以透過主控台或透過 進行 API 呼叫，來啟動或停止資料收集 AWS CLI。下列程序說明這兩種方法。

Using the Migration Hub Console

下列程序說明如何在 Migration Hub 主控台的資料收集器頁面上啟動或停止 Discovery Connector 資料收集程序。

開始或停止資料收集

1. 在導覽窗格中，選擇 Data Collectors (資料收集器)。
2. 選擇 Connectors (連接器) 索引標籤。
3. 選取您要啟動或停止之連接器的核取方塊。
4. 選擇 Start data collection (開始資料收集) 或 Stop data collection (停止資料收集)。

> **Note**
>
> 如果在開始使用連接器收集資料後看不到清查資訊，請確認您已向您的 vCenter 伺服器註冊連接器。

Using the AWS CLI

若要從 啟動 Discovery Connector 資料收集程序 AWS CLI， AWS CLI 必須先在您的環境中安裝 ，然後您必須將 CLI 設定為使用您選取的 Migration Hub 主區域。

安裝 AWS CLI 並開始資料收集

1. AWS CLI 為您的作業系統 (Linux、macOS 或 Windows) 安裝 。如需說明，請參閱 AWS Command Line Interface 使用者指南。
2. 開啟命令提示字元 (Windows) 或終端機 (Linux 或 macOS)。
   a. 輸入 `aws configure` 然後按 Enter 鍵。
   b. 輸入您的 AWS 存取金鑰 ID 和 AWS 私密存取金鑰。
   c. 輸入預設區域名稱的主區域。例如：`us-west-2`。
   d. 輸入預設輸出格式的 `text`。
3. 若要尋找您要開始或停止資料收集之連接器的 ID，請輸入下列命令以查看連接器的 ID：

```
aws discovery describe-agents --filters
 condition=EQUALS,name=hostName,values=connector
```

4. 若要由連接器開始資料收集，請輸入下列命令：

```
aws discovery start-data-collection-by-agent-ids --agent-ids <connector ID>
```

> **Note**
>
> 如果在開始使用連接器收集資料後看不到清查資訊，請確認您已向您的 vCenter 伺服器註冊連接器。

若要停止連接器的資料收集，請輸入下列命令：

```
aws discovery stop-data-collection-by-agent-ids --agent-ids <connector ID>
```

Discovery Connector 故障診斷

> **Important**
>
> 我們建議目前使用 Discovery Connector 的客戶轉換至新的無代理程式收集器。自 2025 年 11 月 17 日起， AWS Application Discovery Service 將停止接受來自 Discovery Connectors 的新資料。如需詳細資訊，請參閱Discovery Connector。

本節包含的主題可協助您疑難排解 Application Discovery Service Discovery Connector 的已知問題。

修正設定 AWS 期間無法連線的 Discovery Connector

在主控台中設定 AWS Agentless Discovery Connector 時，您可能會收到下列錯誤訊息：

> **無法連線 AWS**
>
> AWS 無法連線 （連線重設）。請確認網路和代理設定。

此錯誤是因為 Discovery Connector 嘗試建立 HTTPS 連線失敗，而連線器需要在設定程序期間與之通訊的 AWS 網域。如果無法建立連線，則 Discovery Connector 組態會失敗。

修正 的連線 AWS

1. 請洽詢您的 IT 管理員，了解您的公司防火牆是否封鎖連接埠 443 上需要傳出存取的任何 AWS 網域的輸出流量。

   下列 AWS 網域需要傳出存取權：

   - awsconnector.*Migration Hub home Region*.amazonaws.com
   - sns.*Migration Hub home Region*.amazonaws.com
   - arsenal-discovery.*Migration Hub home Region*.amazonaws.com
   - iam.amazonaws.com
   - aws.amazon.com
   - ec2.amazonaws.com

   如果您的防火牆封鎖輸出流量，請將其解除封鎖。更新防火牆後，請重新設定連接器。

2. 如果更新防火牆無法解決連線問題，請檢查連接器虛擬機器是否具有與所列網域的傳出網路連線。如果虛擬機器具有傳出連線，請在連接埠 443 上執行 telnet 來測試所列網域的連線，如下列範例所示。

   ```
   telnet ec2.amazonaws.com 443
   ```

3. 如果已啟用來自虛擬機器的傳出連線，您必須聯絡 AWS Support 進行進一步疑難排解。

修正運作狀態不佳的連接器

您可以在 Migration Hub 主控台的資料收集器頁面中找到每個 Discovery Connector 的運作狀態資訊。您可以透過尋找任何 Health (健康) 狀態為 Unhealthy (不良) 的連接器來識別有問題的連接器。下列程序概述如何存取連接器主控台以識別狀態問題。

存取連接器主控台

1. 在 Web 瀏覽器中開啟 Migration Hub 主控台，然後從左側導覽中選擇 Data Collectors。
2. 從 Connectors 索引標籤中，記下運作狀態為運作狀態不良的每個連接器的 IP 地址。
3. 在任何可連線至連接器虛擬機器的電腦上開啟瀏覽器，然後輸入連接器主控台的 URL，`https://`*`ip_address_of_connector`*其中 `ip_address_of_connector`是運作狀態不佳連接器的 IP 地址。

4. 輸入設定連接器時所設定的連接器管理主控台密碼。

存取連接器主控台之後，您可以採取動作來解決不良狀態。在這裡，您可以選擇檢視 vCenter 連線的資訊，您會看到一個對話方塊，其中包含診斷訊息。 vCenter 只有 1.0.3.12 版或更新版本的連接器才能使用 View Info (檢視資訊) 連結。

修正狀態問題後，連接器將重新建立與 vCenter 伺服器的連線，而連接器的狀態將變更為 HEALTHY (良好) 狀態。如果問題仍然存在，請聯絡 AWS Support。

連接器狀況不良最常見的原因是 IP 位址問題和登入資料問題。下列章節可協助您解決這些問題，並將連接器回復為良好狀態。

主題

IP 地址問題

如果連接器安裝期間提供的 vCenter 端點格式錯誤、無效，或 vCenter 伺服器目前關閉且無法連線，則連接器可能會進入不良狀態。在此情況下，當您選擇檢視 vCenter vCenter 連線的資訊時，您會看到一個對話方塊，其中包含「確認 vCenter 伺服器的操作狀態，或選擇編輯設定來更新 vCenter 端點」訊息。

下列程序可協助您解決 IP 位址問題。

1. 從連接器主控台 (`https://`*`ip_address_of_connector`*) 中，選擇 Edit Settings (編輯設定)。
2. 從左側導覽中，選擇 Step 5: Discovery Connector Set Up (步驟 5：探索連接器設定)。
3. 從 Configure vCenter credentials (設定 vCenter 登入資料) 中，記下 vCenter Host (vCenter 主機) IP 位址。
4. 使用個別的命令列工具，例如 `ping`或 `traceroute`，驗證相關聯的 vCenter 伺服器是否作用中，以及可從連接器 VM 存取 IP。

    - 如果 IP 位址不正確且 vCenter 服務處於作用中狀態，請在連接器主控台中更新 IP 位址，然後選擇 Next (下一步)。
    - 如果 IP 位址正確，但 vCenter 伺服器處於非作用中狀態，請啟動伺服器。
    - 如果 IP 位址正確且 vCenter 伺服器處於作用中狀態，請檢查是否因為防火牆問題而封鎖連入網路連線。如果是，請更新您的防火牆設定，以允許來自連接器 VM 的連入連線。

登入資料問題

如果連接器安裝期間提供的 vCenter 使用者登入資料無效，或沒有 vCenter 讀取和檢視帳戶權限，則連接器可能會進入不良狀態。在這種情況下，當您選擇檢視 vCenter 連線的資訊時，您會看到一個對話方塊，其中包含「選擇編輯設定以使用讀取和檢視權限來更新您帳戶的 vCenter 使用者名稱和密碼」訊息。 vCenter

下列程序可協助您解決登入資料問題。作為先決條件，請確定您已建立具有 vCenter 伺服器上讀取和檢視帳戶權限的 vCenter 使用者。

1. 從連接器主控台 (`https://ip_address_of_connector`) 中，選擇 Edit Settings (編輯設定)。
2. 從左側導覽中，選擇 Step 5: Discovery Connector Set Up (步驟 5：探索連接器設定)。
3. 從 Configure vCenter credentials (設定 vCenter 登入資料) 中，為具有讀取和檢視權限的 vCenter 使用者提供登入資料，以更新 vCenter Password (vCenter 使用者名稱) 和 vCenter Password (vCenter 密碼)。
4. 選擇 Next (下一步) 以完成設定。

獨立 ESX 主機支援

Discovery Connector 不支援獨立的 ESX 主機。ESX 主機必須屬於 vCenter Server 執行個體的一部分。

取得連接器問題的其他支援

如果您遇到問題且需要協助，請聯絡 AWS Support。我們會與您聯絡，並可能會要求您傳送連接器日誌。若要取得日誌，請依下列步驟執行：

- 重新登入 AWS Agentless Discovery Connector 主控台，然後選擇下載日誌套件。
- 日誌服務包下載完成後，依照 AWS Support 指示進行傳送。

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。