



使用者指南

AWS Application Discovery Service



AWS Application Discovery Service: 使用者指南

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Table of Contents

什麼是 AWS Application Discovery Service ?	1
VMware Discovery	2
資料庫探索	2
比較無代理程式收集器和探索代理程式	2
前提	3
設定	5
註冊 Amazon Web Services	5
建立 IAM 使用者	5
建立 IAM 管理使用者	6
建立 IAM 非管理使用者	6
登入移轉中心並選擇主地區域	7
探索代理	8
必要條件	9
在 Linux 上安裝	10
舊版 Linux 平台的需求	14
在 Linux 上管理探查代理程式處理程序	14
解除安裝代理程式	16
排解 Linux 探查代理程式	16
在 Windows 上安裝	17
Package 簽署和自動升級	21
在 Windows 中管理探索代理程式處理程序	21
視窗的疑難排解	23
收集的資料	24
開始或停止資料收集	26
無代理程式收集器	28
入門	28
先決條件	29
步驟 1：建立 IAM 使用者	31
步驟 2：下載收集器	33
步驟 3：部署收集器	33
步驟 4：存取收集器主控台	34
步驟 5：設定收集器	35
步驟 6：設定資料收集模組	41
步驟 7：檢視收集的資料	53

收集的資料	54
VMware 模組所收集的資料	55
數據庫和分析模塊收集的數據	58
使用主控台	59
收集儀表板	59
編輯收集器設定	61
編輯 vCenter 認證	62
更新	63
故障診斷	63
修正無代理程式收集器在安裝期間無法到達 AWS	64
修正連線至 Proxy 主機時的自我簽署憑證問題	65
尋找不健康的收藏家	66
修正 IP 位址問題	67
修正 vCenter 認證問題	67
修正資料轉送問題	68
修正連線問題	68
獨立式 ESX 主機支援	70
聯絡 AWS 支援	70
匯入	71
支援的匯入檔案欄位	71
設定您的匯入許可	75
將您的匯入檔案上傳到 Amazon S3	78
匯入資料	80
追蹤 Migration Hub 匯入要求	81
檢視、匯出與探索資料	84
檢視收集	84
匹配邏輯	85
匯出收集資料	86
Athena 中的資料探索	88
在 Amazon Athena 中啟用資料探索	88
在 Amazon Athena 使用資料探索	90
主控台逐步解說	100
主要儀表板	100
主要儀表板	100
資料收集	100
啟動和停止資料收集器	101

檢視和排序資料收集器	101
檢視、匯出與探索資料	105
檢視和排序伺服器	105
標記伺服器	106
匯出伺服器資料	107
Athena 中的資料探索	108
應用程式	108
使用 API 查詢發現的項目	110
使用 DescribeConfigurations 動作	110
使用 ListConfigurations 動作	114
安全性	129
身分和存取權管理	129
物件	130
使用身分來驗證	130
使用政策管理存取權	133
如何與 IAM AWS Application Discovery Service 搭配使用	135
AWS 受管理政策	137
身分型政策範例	141
了解並使用服務連結角色	148
IAM 故障診斷	155
AWS Application Discovery Service 中的記錄和監控	156
使用記錄 Application Discovery Service API 呼叫AWS CloudTrail	156
配額	159
疑難排解	160
透過資料探索停止資料收集	160
移除資料探索所收集的資料	161
修正 Amazon Athena 資料探索的常見問題	162
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的 AWS 資源 ...	162
新的代理程式資料不會顯示在 Amazon Athena	163
您沒有足夠的權限可以訪問 Amazon S3，Amazon 數據 Firehose 件，或 AWS Glue	164
排解匯入失敗記錄	164
文件歷史記錄	167
AWS 詞彙表	170
附錄	171
.....	171
附錄：探索連接器	171

探索連接器所收集的資料	172
連接器資料收集	175
疑難排解探查連接器	176
.....	clxxx

什麼是 AWS Application Discovery Service ?

AWS Application Discovery Service 可透過收集關於您內部部署伺服器 and 資料庫的使用情況和組態資料，協助您規劃遷移到AWS雲端。Application Discovery Service 與AWS Migration Hub和AWS Database Migration Service車隊顧問整合。Migration Hub 可將您的移轉狀態資訊彙總至單一主控台，簡化您的移轉追蹤作業。您可以從主區域的 Migration Hub 主控台檢視探索到的伺服器、將它們分組到應用程式中，然後追蹤每個應用程式的移轉狀態。您可以使用 DMS 叢集顧問來評估資料庫工作負載的移轉選項。

所有發現的數據都存儲在您的AWS Migration Hub家庭區域中。因此，在執行任何探查和移轉活動之前，您必須先在 Migration Hub 主控台或 CLI 命令中設定主區域。您的資料可以匯出到微軟 Excel 或分AWS析工具，如亞馬遜雅典娜和亞馬遜分析工具QuickSight。

使用應用程式探索服務 API，您可以匯出探查到之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

在開始探索程序之AWS Migration Hub前，您必須先設定您的主地區域，因為您的資料會儲存在您的本地區域。如需有關使用本地區域的詳細資訊，請參閱本[地區域](#)。

Application Discovery Service 提供兩種執行探索和收集內部部署伺服器相關資料的方式：

- 透過 VMware vCenter 部署應用程式探索服務無代理程式收集器 (無代理程式收集器) (OVA 檔案)，即可執行無代理程式探索。設定無代理程式收集器後，它會識別與 vCenter 相關聯的虛擬機器 (VM) 和主機。無代理程式收集器會收集下列靜態組態資料：伺服器主機名稱、IP 位址、MAC 位址、磁碟資源配置、資料庫引擎版本和資料庫結構描述。此外，它還會收集每個虛擬機器和資料庫的使用率資料，提供 CPU、RAM 和磁碟 I/O 等指標的平均和尖峰使用率。
- 透過在每部 VM 和實體伺服器上部署AWS應用程式探索代理程式，即可執行代理程式型探索。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。

Application Discovery Service 與合作AWS夥伴網路 (APN) 合作夥伴的應用程式探索解決方案 這些第三方解決方案可協助您將內部部署環境的詳細資料直接匯入 Migration Hub，而無需使用任何無代理程

式收集器或探索代理程式。協力廠商應用程式探索工具可以查詢 ApAWS plication Discovery Service，而且可以使用公用 API 寫入應用程式探索服務資料庫。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

如果您有在 VMware vCenter 環境中執行的虛擬機器 (VM)，則可以使用無代理程式收集器來收集系統資訊，而不必在每個虛擬機器上安裝代理程式。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。

無代理程式收集器會擷取 vCenter 中執行之每個虛擬機器的系統效能資訊和資源使用率，而不論使用中的作業系統為何。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，如果您需要此詳細資料層級，並想要仔細檢視部分現有 VM 以協助規劃移轉，您可以視需要安裝探索代理程式。

此外，對於 VMware 上託管的虛擬機器，您可以同時使用無代理程式收集器和探索代理程式同時執行探查。如需有關每個探索工具會收集的確切資料類型詳細資訊，請參閱[無代理程式收集器所收集的資料](#)和[探索代理程式收集的資料](#)。

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，則可以使用無代理程式收集器來探索並清查這些伺服器。然後，您可以收集每個資料庫伺服器的效能測量結果，而不需要在環境中的每部電腦上安裝無代理程式收集器。

無代理程式收集器資料庫和分析資料收集模組會擷取中繼資料和效能指標，提供您資料基礎架構的深入分析。資料庫和分析資料收集模組會使用微軟 Active Directory 中的 LDAP 來收集您網路中的作業系統、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的 CPU、記憶體和磁碟容量的實際使用率指標。如需有關收集測量結果的詳細資訊，請參閱[數據庫和分析模塊收集的數據](#)

無代理程式收集器從您的環境完成資料收集之後，您可以使用 AWS DMS 主控台進行進一步分析和規劃移轉。例如，若要在中選擇最佳移轉目標 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[資料庫與分析資料收集模組](#)。

比較無代理程式收集器和探索代理程式

下表提供「Application Discovery Service」資料收集工具的快速比較。

	無代理程式收集器	探索代理
Supported server types		
VMware 虛擬機器	是	是
實體伺服器	否	是
Deployment		
每個伺服器	否	是
每個 vCenter	是	否
Collected data		
靜態伺服器組態資料	Yes	Yes
資料庫組態資料	Yes	No
VM 使用率指標	Yes	No
資料庫使用指標	Yes	No
時間序列效能資訊	No	Yes (Export only)
網路傳入/傳出連線	No	Yes (Export only)
執行中的程序	No	Yes (Export only)
支援的作業系統	Any OS running in VMware vCenter V5.5+	如需支援的 Linux 和視窗作業系統清單，請參閱 探查代理程式的必要 。
支援資料庫	Oracle, SQL Server, MySQL, and PostgreSQL	無

前提

若要使用應用程式探索服務，會假設下列情況：

- 您已經註冊了AWS。如需詳細資訊，請參閱[設定 ApApplication Discovery Service](#)。
- 您已選取 Migration Hub 本位目錄區域。如需詳細資訊，請參閱[關於家用區域的文件](#)。

以下是可以預期的情況：

- Migration Hub 本位目錄區域是應用程式探索服務儲存您的探索和規劃資料的唯一區域。
- 探索代理程式、連接器和匯入只能在您選取的 Migration Hub 本位目錄區域中使用。
- 如需可在其中使用應用程式探索服務的AWS區域清單，請參閱[Amazon Web Services 一般參考](#)。

設定 ApApplication Discovery Service

初次使用 AWS Application Discovery Service 之前，請先完成以下作業：

[註冊 Amazon Web Services](#)

[建立 IAM 使用者](#)

[登入到 Migravice 中心主控台，然後選擇一個主要地區域](#)

註冊 Amazon Web Services

如果您還沒有 AWS 帳戶，請完成下列步驟建立新帳戶。

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。

部分註冊程序需接收來電，並在電話鍵盤輸入驗證碼。

註冊 AWS 帳戶時，會建立 AWS 帳戶根使用者。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，[將管理存取權指派給管理使用者](#)，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

當您建立AWS帳戶時，您會取得單一的登入身分，可以完整存取帳戶中所有AWS Service 和資源。這個身分稱為 AWS 帳戶的根使用者。使用您AWS Management Console用來建立帳戶的電子郵件地址和密碼，以登入AWS並存取。

強烈建議您不要以根使用者處理日常作業，即使是管理作業。請改為遵循安全最佳實務[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作業。

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兩種類型的 IAM 使用者。

主題

- [建立 IAM 管理使用者](#)
- [建立 IAM 非管理使用者](#)

建立 IAM 管理使用者

依預設，管理員帳戶會繼承存取 Application Discovery Service 所需的所有原則。

建立管理員使用者

- 在您的 AWS 帳戶中建立管理員使用者。如需說明，請參閱 [IAM 使用者指南中的建立第一個 IAM 使用者和管理員群組](#)。

建立 IAM 非管理使用者

建立非管理 IAM 使用者時，請遵循安全性最佳實務 [授與最低權限](#)，授與使用者最低權限。

使用 IAM 受管政策定義非管理 IAM 使用者存取 Application Discovery Service 的層級。如需有關 Application Discovery Service 受管原則的資訊，請參閱 [AWS 受管理的政策 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，建立非管理員 IAM 使用者。

遵循 IAM 使用者指南中的指示：

- 執行關於選取存取類型的步驟時，請選取 [程式設計存取]。請注意，雖然不建議使用，但如果您打算使用相同的 IAM 使用者登入資料存取主控台，請僅選取AWS管理AWS主控台存取權。
- 在有關 [設定權限] 頁面的步驟中，選擇 [直接將現有策略附加至使用者] 的選項。然後從政策清單中選取應用程式探索服務的受管 IAM 政策。如需有關 Application Discovery Service 受管原則的資訊，請參閱 [AWS 受管理的政策 AWS Application Discovery Service](#)
- 執行有關檢視使用者存取金鑰 (存取金鑰 ID 和秘密存取金鑰) 的步驟時，請遵循關於將使用者新存取金鑰 ID 和秘密存取金鑰儲存在安全可靠的地方的重要注意事項中的指引。

登入到 Migravice 中心主控台，然後選擇一個主要地區域

您必須在您使用的AWS帳戶中選擇一個AWS Migration Hub主區域AWS Application Discovery Service。

選擇主頁地區

1. 使用您的AWS帳戶，在 <https://console.aws.amazon.com/migrationhub/> 登入AWS Management Console並開啟 Migration Hub 紐主控台。
2. 在 [Migration Hub] 主控台瀏覽窗格中，選擇 [設定]，然後選擇主 [區域]。

您的 Migration Hub 資料會儲存在您的主要區域中，以便進行探索、規劃和移轉追蹤。如需詳細資訊，請參閱 [Migration Hub 本地區域](#)。

AWS 應用程式探索代

AWS 應用程式探索代理程式 (探索代理程式) 是您安裝在內部部署伺服器 and VM 上進行探索和移轉的軟體。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它們。

Note

部署探查代理程式之前，您必須選擇 [Migration Hub 本位目錄區域](#)。您必須在所在區域註冊您的代理程式。

探索代理程式會在您的本機環境中執行，且需要 root 權限。當您啟動探索代理程式時，它會安全地連線至您的本地區域，並向應用程式探索服務註冊。

- 例如，如果 eu-central-1 是您的本地區域，則會向應 `arsenal-discovery.eu-central-1.amazonaws.com` 用程式探索服務註冊。
- 或者，根據需要將您的居住區域替換為除了 us-west-2 之外的所有其他區域。
- 如果 us-west-2 是您的本地區域，它會向應 `arsenal.us-west-2.amazonaws.com` 用程式探索服務註冊。

運作方式

註冊之後，代理程式會開始收集其所在主機或虛擬機器的資料。代理程式會每隔 15 分鐘偵測 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 並規劃移轉。

探索代理程式會使用傳輸層安全性 (TLS) 加密，將資料安全地傳輸至應用程式探索服務。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。

i Tip

在下載並開始安裝探索代理程式之前，請務必先閱讀中的所有必要先決條件 [探查代理程式的必要](#)

主題

- [探查代理程式的必要](#)
- [在 Linux 上安裝探查代理程式](#)
- [在 Windows 上安裝](#)
- [探索代理程式收集的資料](#)
- [啟動或停止探索代理程式資料收集](#)

探查代理程式的必要

以下是您必須先執行的必要條件和工作，才能順利安裝應用程式探索代理 AWS 程式 (探索代理程式)。

- 您必須先設定 [AWS Migration Hub 主區域](#)，然後才能開始安裝探索代理程式。
- 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 微型架構)。
- 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 的 12.04，14.04，16.04，18.04，20.04

紅帽企業版 5.11, 6.10, 7.3, 7.7, 8.1

CentOS 5.11、6.9、7.3

速度 11 SP4, 12 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，如果您的居住區域是 `eu-central-1`，則會使用 `https://arsenal-discovery.eu-central-1.amazonaws.com:443`

- 您必須存取您居住區域中的 Amazon S3，才能自動升級才能運作。
- 在主控台中建立 AWS Identity and Access Management (IAM) 使用者，並附加現有的 `AWSApplicationDiscoveryAgentAccess` IAM 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 受管理的政策 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

探查代理程式具有 32 位元代理程式執行檔，可在 32 位元和 64 位元作業系統上運作。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。

在 Linux 上安裝探查代理程式

在 Linux 上完成下列程序。在開始此程序之前，請確定已設定 [Migration Hub 本地區域](#)。

Note

如果您使用的不是目前的 Linux 版本，請參閱 [舊版 Linux 平台的需求](#)。

在您的資料中心安裝 AWS 應用程式探索代理程式

1. 登入 Linux 型伺服器或 VM，並建立包含代理程式元件的新目錄。

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-us-west-2.amazonaws.com/aws-discovery-agent.us-west-2/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. 開啟主控台並移至 [Discovery Tools \(探索工具\)](#) 頁面。
- ii. 在 Discovery Agent (探索代理程式) 方塊中，選擇 Download agent (下載代理程式)，然後在產生的清單方塊中選擇 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.us-west-2.amazonaws.com/aws-discovery-agent.us-west-2/linux/latest/aws-discovery-agent.tar.gz.sig
```

```
curl -o ./discovery.gpg https://s3.us-west-2.amazonaws.com/aws-discovery-agent.us-west-2/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. 如果要安裝代理程式，請選擇下列其中一種安裝方法。

若要...	執行此作業...
安裝探查代理	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，請使 <i>your-home-region</i> 用您的存取金鑰 ID 和 <i>aws-secret-access-key</i> 秘密存取金

若要...	執行此作業...
	<p>鑰來取代您所在地區的名稱。 <i>aws-access-key-id</i></p> <pre data-bbox="862 331 1507 491">sudo bash install -r <i>your-home-region</i> -k <i>aws-access-key-id</i> -s <i>aws-secret-access-key</i></pre> <p>根據預設，代理程式會在更新可用時自動下載並套用更新。</p> <p>我們建議您使用此預設組態。</p> <p>不過，如果您不想讓代理程式自動下載並套用更新，請在執行代理程式安裝命令時加入 <code>-u false</code> 參數。</p>

若要...	執行此作業...
<p>(選擇性) 安裝探查代理程式並設定非透明 Proxy</p>	<p>如果要設定非透明 Proxy，請將下列參數新增至代理程式安裝命令：</p> <ul style="list-style-type: none"> • -e 代理伺服器密碼。 • -f 代理端口號。 • -g 代理方案。 • -i 代理用戶名。 <p>以下是使用非透明 Proxy 參數的代理程式安裝命令範例。</p> <pre>sudo bash install -r <i>your-home-region</i> -k <i>aws-access-key-id</i> -s <i>aws-secret-access-key</i> -d <i>myproxy.mycompany.com</i> -e <i>mypassword</i> -f <i>proxy-port-number</i> -g https -i <i>myusername</i></pre> <p>如果您的 Proxy 不需要驗證，請省略 -e 和 -i 參數。</p> <p>如果您的代理伺服器使用 HTTPhttps，則安裝命令範例會使 http 用指定 -g 參數值。</p>

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，如果您的居住區域是 eu-central-1，則會使用 `https://arsenal-discovery.eu-central-1.amazonaws.com:443`

主題

- [舊版 Linux 平台的需求](#)
- [在 Linux 上管理探查代理程式處理程序](#)
- [解除安裝探查代理程式](#)
- [排解 Linux 探查代理程式](#)

舊版 Linux 平台的需求

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。這些平台可能會受到阻止代理程式更新指令 out-of-date 碼下載安裝套件的密碼套件的影响。

Curl

應用程式探索代理程式 curl 需要與 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

較舊的 Linux 系統可能有 out-of-date 憑證授權單位 (CA) 套件，這對於保護網際網路通訊的安全至關重要。

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 Linux 上管理探查代理程式處理程序

您可以使用 `systemd`、或 `System V init` 工具在系統層級管理探查代理程式 Upstart 式的行為。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	<code>sudo systemctl status aws-discovery-daemon.service</code>

任務	Command
啟動代理程式	<code>sudo systemctl start aws-discovery-daemon.service</code>
停止代理程式	<code>sudo systemctl stop aws-discovery-daemon.service</code>
重新啟動代理程式	<code>sudo systemctl restart aws-discovery-daemon.service</code>

Upstart

應用程式探索代理程式的管理命令

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

System V init

應用程式探索代理程式的管理命令

任務	Command
驗證代理程式是否執行中	<code>sudo /etc/init.d/aws-discovery-daemon status</code>
啟動代理程式	<code>sudo /etc/init.d/aws-discovery-daemon start</code>

任務	Command
停止代理程式	<code>sudo /etc/init.d/aws-discovery-daemon stop</code>
重新啟動代理程式	<code>sudo /etc/init.d/aws-discovery-daemon restart</code>

解除安裝探查代理程式

本節說明如何在 Linux 上解除安裝探查代理程式。

如果您使用 yum 套件管理員，請解除安裝代理程式

- 如果使用 yum，請使用下列命令來解除安裝代理程式。

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

若要解除安裝代理程式 (如果您使用 apt-get 套件管理員)

- 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
```

若要解除安裝代理程式 (如果您使用 zypper 套件管理員)

- 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
```

排解 Linux 探查代理程式

如果您在 Linux 上安裝或使用探查代理程式時遇到問題，請參閱下列有關記錄和組態的指導。當協助疑難排解代理程式的潛在問題或其與應用程式探索服務的連線時，Sup AWS port 服務經常會要求這些檔案。

- 日誌檔

探查代理程式的記錄檔位於下列目錄中。

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

記錄檔的名稱是用來指出它們是由主要協助程式、自動升級程式還是安裝程式所產生。

- 組態檔案

探查代理程式 2.0.1617.0 版或更新版本的組態檔位於下列目錄中。

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

2.0.1617.0 之前版本之探查代理程式的組態檔位於下列目錄中。

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

- 如需有關如何移除舊版探查代理程式的指示，請參閱[探查代理程式的必要](#)。

在 Windows 上安裝

完成下列程序在 Windows 上安裝代理程式。在開始此程序之前，請確定已設定 [Migration Hub 本地區域](#)。

在您的資料中心安裝 AWS 應用程式探索代理程式

1. 下載 [Windows 代理程式安裝程式](#)，但請勿按兩下以在 Windows 中執行安裝程式。

Important

請勿按兩下以在 Windows 中執行安裝程式，因為安裝程式將無法安裝。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 代理程式安裝程式未在主機上偵測到任何版本的 Visual C++ x86 執行階段，它會在安裝代理程式軟體之前，自動安裝 Visual C++ x86 2015-2019 執行階段。

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. 如果要安裝代理程式，請選擇下列其中一種安裝方法。

若要...	執行此作業...
安裝探查代理	<p>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。在範例中，請<code>your-home-region</code> 以您所在地區的名稱、<code>aws-access-key-id</code> 存取金鑰 ID 和<code>aws-secret-access-key</code> 私密存取金鑰取代。</p> <p>或者，您可以指定 <code>INSTALLLOCATION</code> 參數的資料夾路徑<code>C:\install-location</code>，以設定代理程式安裝位置。例如 <code>INSTALLLOCATION=" C:\install-location "</code>。產生的資料夾階層將是 [安裝位置路徑]\AWS 探索。依預設，安裝位置為資料夾 Program Files。</p> <p>或者，您可以使用 <code>LOGANDCONFIGLOCATION</code> 來覆寫代理程式記錄檔資料夾和組態檔的預設目錄 (ProgramData)。產生的資料夾階層為 [<code>LOGANDCONFIGLOCATION path</code>]\AWS Discovery。</p> <pre data-bbox="862 1203 1507 1444">.\AWSDiscoveryAgentInstaller.exe REGION=" your-home-region " KEY_ID="aws-access-key-id " KEY_SECRET=" aws-secret-access-key " /quiet</pre> <p>根據預設，代理程式會在更新可用時自動下載並套用更新。</p> <p>我們建議您使用此預設組態。</p> <p>不過，如果您不想讓代理程式自動下載並套用更新，請在執行代理程式 <code>install</code> 命令時包含下列參數：<code>AUTO_UPDATE=false</code></p>

若要...	執行此作業...
	<div style="border: 1px solid #f08080; border-radius: 10px; padding: 10px; background-color: #fff9f9;"> <p> Warning</p> <p>停用自動升級可防止安裝最新的安全性修補程式。</p> </div>
<p>(選擇性) 安裝探查代理程式並設定非透明 Proxy</p>	<p>若要設定非透明 Proxy，請將下列公用內容新增至代理程式安裝命令：</p> <ul style="list-style-type: none"> • 代理主機 — 代理主機的名稱 • 代理計劃 — 代理方案 • 代理連接埠 — 代理伺服器連接埠號碼 • 代理使用者 — 代理伺服器使用者名稱 • 代理密碼 — 代理伺服器使用者密碼 <p>以下是使用非透明 Proxy 屬性的代理程式安裝命令範例。</p> <div style="border: 1px solid #ccc; border-radius: 10px; padding: 10px; background-color: #fff9f9;"> <pre>.\AWSDiscoveryAgentInstall.exe REGION=" <i>your-home-region</i> " KEY_ID="<i>aws-access-key-id</i> " KEY_SECRET="<i>aws-secret-access-key</i> " PROXY_HOST="<i>myproxy.mycompany.com</i> " PROXY_SCHEME="https" PROXY_PORT="<i>proxy-port-number</i> " PROXY_USER="<i>myusername</i> " PROXY_PASSWORD="<i>mypassword</i> " /quiet</pre> </div> <p>如果您的 Proxy 不需要驗證，請省略 PROXY_USER 和 PROXY_PASSWORD 屬性。安裝命令使用的示例 https。如果您的代理伺服器使用 HTTP，請指定 http PROXY_SCHEME 值。</p>

4. 如果來自網路的輸出連線受到限制，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，如果您的居住地區是eu-central-1，您可以使用以下內容：<https://arsenal-discovery.eu-central-1.amazonaws.com:443>

Package 簽署和自動升級

對於 Windows 2008 及更新版本，Amazon 以加密方式使用 SHA256 憑證簽署 Application Discovery Service 代理程式安裝套件。對於 SHA2 簽署的自動更新，請確定主機已安裝修補程式以支援 SHA2 簽章驗證。微軟最新的支持[修補程序](#)有助於支持 SHA2 身份驗證視窗服務器 2008 SP2。

Note

對於 SHA256 支持視窗 2003 的修補程序不再公開從 Microsoft。如果您的 Windows 2003 主機尚未安裝這些修正程式，則需要手動升級。

手動執行升級

1. 下載 [Windows 代理程式更新程式](#)。
2. 以管理員身份打開命令提示符。
3. 導覽至儲存更新程式的位置。
4. 執行下列命令。

```
AWSDiscoveryAgentUpdater.exe /Q
```

在 Windows 中管理探索代理程式處理程序

您可以透過 Windows 伺服器管理員服務主控台，在系統層級管理探查代理程式的行為。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	已開始
	AWS 探索更新程式	

任務	服務名稱	服務狀態/動作
啟動代理程式	AWS 探索代理	選擇 Start (啟動)。
	AWS 探索更新程式	
停止代理程式	AWS 探索代理	選擇 Stop (停止)。
	AWS 探索更新程式	
重新啟動代理程式	AWS 探索代理	選擇 Restart (重新啟動)。
	AWS 探索更新程式	

若要解除安裝 Windows 上的探索代理程式

1. 在視窗中開啟控制台。
2. 選擇程式集。
3. 選擇程式和功能。
4. 選取AWS 探查代理程式。
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 上解除安裝探查代理程式

1. 右鍵單擊開始。
2. 選擇命令提示符。

3. 使用下列命令在 Windows 上解除安裝探查代理程式。

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

疑難排解 Windows 中的探索代理

如果您在 Windows 上安裝或使用應用程式探索代理 AWS 程式時遇到問題，請參閱下列有關記錄和組態的指導。AWS Support 在協助疑難排解代理程式的潛在問題或其與 Application Discovery Service 的連線時，通常會要求這些檔案。

- 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
```

記錄檔會命名，以指出是由主要服務、自動升級還是安裝程式所產生。

- 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
```

- 如需有關如何移除舊版探查代理程式的指示，請參閱[探查代理程式的必要](#)。

探索代理程式收集的資料

AWS 應用程式探索代理程式 (探索代理程式) 是您在內部部署伺服器和 VM 上安裝的軟體。探索代理程式會收集系統組態、計算序列使用率或效能資料、處理程序資料，以及傳輸控制通訊協定 (TCP) 網路連線。本節說明所收集的資料。

探查代理程式收集資料的表格圖例：

- 「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 主控台對等的資料會以 MB 為單位報告。
- 輪詢期間以大約 15 秒為間隔，並傳送至 AWS 每 15 分鐘一次。
- 以星號 (*) 表示的資料欄位僅適用於從代理程式的 API 匯出功能產生的 .csv 檔案中。

資料欄位	描述
agentAssignedProcess 身份證 *	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
agentProvidedTime 郵票 *	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
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

資料欄位	描述
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
totalCpuUsage百分比	輪詢期間主機上的 CPU 使用量百分比
totalDiskBytesReadPerSecond (千比特)	所有磁碟的每秒讀取總千位元組
totalDiskBytesWrittenPerSecond (千比特)	所有磁碟上每秒寫入的總千位元組
totalDiskFree大小 (GB)	可用磁碟空間，以 GB 表示
totalDiskReadOpsPerSecond	每秒讀取 I/O 操作的總數
totalDiskSize (GB)	磁碟總容量，以 GB 表示

資料欄位	描述
totalDiskWriteOpsPerSecond	每秒寫入 I/O 操作的總數
totalNetworkBytesReadPerSecond (千比特)	每秒讀取位元組總輸送量
totalNetworkBytesWrittenPerSecond (千比特)	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
totalNumLogical處理器 *	實體核心總數乘以每個核心上可執行的執行緒數目
totalNumNetwork卡片	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

啟動或停止探索代理程式資料收集

部署並設定探查代理程式之後，如果資料收集停止，您可以重新啟動它。您可以透過主控台開始或停止資料收集，或透過 AWS CLI。下列程序會描述這兩種方法。

Using the Migration Hub console

下列程序顯示如何在 Migration Hub 主控台的 [資料收集器] 頁面上啟動或停止探索代理程式資料收集程序。

若要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 Agents (代理程式) 索引標籤。
3. 選取要啟動或停止之代理程式的核取方塊。

i Tip

如果您已安裝多個代理程式，但只想在特定主機上開始或停止資料收集，則代理程式列表中的「主機名稱」欄會識別安裝代理程式所在的主機。

4. 選擇 Start data collection (開始資料收集) 或 Stop data collection (停止資料收集)。

Using the AWS CLI

若要從啟動或停止探索代理程式資料收集程序 AWS CLI，您必須先在環境 AWS CLI 中安裝，然後必須將 CLI 設定為使用您選取的 [Migration Hub 本位目錄區域](#)。

若要安裝 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 適合您的作業系統類型 (視窗或 Mac/Linux)。如需指示，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 秘密存取金鑰。
 - c. 輸入您的所在區域作為預設區域名稱，例如 `us-west-2`。(在此範例中，我們假設 `us-west-2` 是您的所在區域。)
 - d. 輸入預設輸出格式的 `text`。
3. 若要尋找您要停止或開始資料收集的代理程式識別碼，請輸入下列命令：

```
aws discovery describe-agents
```

4. 若要透過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>
```

若要停止代理程式收集資料，請輸入下列命令：

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

Application Discovery Service 無代理收集器

Application Discovery Service 無代理程式收集器 (無代理程式收集器) 是一種內部部署應用程式，可透過無代理程式方法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、CPU 數目、RAM 數量)、資料庫中繼資料和使用率量度。您可以使用開放式虛擬化封存 (OVA) 檔案，在 VMware vCenter Server 環境中將無代理程式收集器安裝為虛擬機器 (VM)。

無代理收集器具有模塊化體系結構，允許使用多個無代理程序收集方法。無代理程式收集器目前支援從 VMware VM 以及從資料庫和分析伺服器收集資料的模組。未來的模組將支援網路連線收集、從其他虛擬化平台收集，以及作業系統層級收集。

無代理程式收集器支援 AWS Application Discovery Service (應用程式探索服務) 的資料收集，藉AWS 雲端由收集內部部署伺服器和資料庫的使用情況和組態資料，協助您規劃移轉至。

Application Discovery Service 與整合AWS Migration Hub，可將您的移轉狀態資訊彙總至單一主控台，以簡化您的移轉追蹤作業。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，然後從主區域的 Migration Hub 主控台追蹤每個應用程式的遷移狀態。

無代理程式收集器資料庫和分析資料收集模組與 AWS Database Migration Service () AWS DMS 整合。此整合可協助您規劃移轉至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，並建立要移轉至的伺服器清單AWS 雲端。該數據收集模塊收集數據庫元數據和 CPU，內存和磁盤容量的實際使用率指標。收集這些測量結果後，您可以使用AWS DMS主控台為來源資料庫產生目標建議。

主題

- [開始使用無代理程式收集器](#)
- [無代理程式收集器所收集的資料](#)
- [使用無代理程式收集器主控台](#)
- [手動更新無代理程式收集器](#)
- [排解無代理程式收集器](#)

開始使用無代理程式收集器

本節說明如何開始使用應用程式探索服務無代理程式收集器 (無代理程式收集器)。

主題

- [無代理程式收集器的先決條件](#)
- [步驟 1：為無代理程式收集器建立 IAM 使用者](#)
- [步驟 2：下載無代理程式收集器](#)
- [步驟 3：部署無代理程式收集器](#)
- [步驟 4：存取無代理程式收集器主控台](#)
- [步驟 5：設定無代理程式收集器](#)
- [步驟 6：設定無代理程式收集器資料收集模組](#)
- [步驟 7：檢視收集的資料](#)

無代理程式收集器的先決條件

以下是使用應用程式探索服務無代理程式收集器 (無代理程式收集器) 的先決條件：

- 一個或多個AWS帳戶。
- 設置了AWS Migration Hub主區域的AWS帳戶，請參閱[登入到 Migravice 中心主控台](#)，然後選擇一個[主要地區域](#)。您的 Migration Hub 資料會儲存在您的主要區域中，以便進行探索、規劃和移轉追蹤。
- 設定為使用AWS受管政策的AWS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 使用者還必須使用兩個客戶受管 IAM 政策DMSCollectorPolicy和FleetAdvisorS3Policy。如需詳細資訊，請參閱[步驟 1：為無代理程式收集器建立 IAM 使用者](#)。IAM 使用者必須在已設定 Migration Hub 本地區域的AWS帳戶中建立。
- VMware vCenter 伺服器版本 5.5、版本 6、6.7 或 7.0 版。

Note

無代理程式收集器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 伺服器安裝程式，請確定您可以提供 vCenter 認證，其中包含針對系統群組設定的讀取和檢視權限。
- 無代理程式收集器需要透過 TCP 連接埠 443 對多個網域進行輸出存取。AWS如需這些網域的清單，請參閱[設定防火牆以存取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 本地區域的 AWS 區域 Amazon S3 儲存貯體中建立一個 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。

設定防火牆以存取AWS網域

如果來自網路的輸出連線受到限制，您必須更新防火牆設定，以允許對無代理程式收集器所需的網域進行輸出存取。哪些AWS網域需要輸出存取，取決於您的 Migration Hub 本地區域是美國西部 (奧勒岡) 區域、US-西 2 或其他區域。

如果您的AWS帳戶首頁區域是 us-west-2，則下列網域需要輸出存取：

- `arsenal-discovery.us-west-2.amazonaws.com`— 收集器使用此網域驗證是否已使用必要的 IAM 使用者登入資料進行設定。收集器還使用它來發送和存儲收集的數據，因為主區域是 US-西-2。
- `migrationhub-config.us-west-2.amazonaws.com`— 收集器會根據提供的 IAM 使用者登入資料，使用此網域判斷收集器將資料傳送至哪個主區域。
- `api.ecr-public.us-east-1.amazonaws.com`— 收集器使用此網域來探索可用的更新。
- `public.ecr.aws`— 收集器會使用此網域來下載更新。
- `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到您的 Amazon S3 儲存貯體。

如果您的AWS帳戶主頁區域不是，則下列網域需要輸出存取**us-west-2**：

- `arsenal-discovery.us-west-2.amazonaws.com`— 收集器使用此網域驗證是否已使用必要的 IAM 使用者登入資料進行設定。
- `arsenal-discovery.your-migrationhub-home-region.amazonaws.com`— 收集器使用此網域來傳送和儲存收集的資料。
- `migrationhub-config.us-west-2.amazonaws.com`— 收集器會根據提供的 IAM 使用者登入資料，使用此網域判斷收集器應將資料傳送至哪個主區域。
- `api.ecr-public.us-east-1.amazonaws.com`— 收集器使用此網域來探索可用的更新。
- `public.ecr.aws`— 收集器會使用此網域來下載更新。
- `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到您的 Amazon S3 儲存貯體。

設定無代理程式收集器時，您可能會收到錯誤訊息，例如安裝失敗 — 請檢查您的認證，然後再試一次或AWS無法連線到。請確認網路設定。這些錯誤可能是由於無代理程式收集器嘗試建立 HTTPS 連線到其中一個需要輸出存取的AWS網域失敗所致。

如果無法建立連線，AWS無代理程式收集器就無法從您的內部部署環境收集資料。若要取得有關如何修正連線的資訊AWS，請參閱[修正無代理程式收集器在安裝期間無法到達 AWS](#)。

步驟 1：為無代理程式收集器建立 IAM 使用者

若要使用無代理程式收集器，您必須在中[登入到 Migravice 中心主控台](#)，然後選擇一個主要地區域使用的AWS帳戶中建立 AWS Identity and Access Management (IAM) 使用者。然後，將此 IAM 使用者設定為使用下列AWS受管政策[AWSApplicationDiscoveryAgentlessCollectorAccess](#)。您可以在建立 IAM 使用者時附加此 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。這些政策提供存取您的 Amazon S3 儲存貯體和 AWS DMS 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 程式碼建立原**DMSCollectorPolicy**則。

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

- 使用下列 JSON 程式碼建立原**FleetAdvisorS3Policy**則。

```
{
  "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，請以您在先決條件步驟中建立的 Amazon S3 儲存貯體名稱取 *bucket_name* 代。

建議您建立非管理 IAM 使用者，以搭配無代理程式收集器使用。建立非管理 IAM 使用者時，請遵循安全性最佳實務 [授與最低權限](#)，授與使用者最低權限。

建立非管理員 IAM 使用者以搭配無代理程式收集器使用

1. 在中AWS Management Console，使用您用來設定主區域的AWS帳戶導覽至 IAM 主控台 [登入到 Migravice 中心主控台](#)，然後選擇一個主要地區域。
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](#)，透過主控台建立使用者的指示，建立非管理員 IAM 使用者。

遵循 IAM 使用者指南中的指示進行操作：

- 執行關於選取存取類型的步驟時，請選取 [程式設計存取]。請注意，雖然不建議使用，但如果您打算使用相同的 IAM 使用者登入資料存取主控台，請僅選取AWS管理AWS主控台存取權。
- 在有關 [設定權限] 頁面的步驟中，選擇 [直接將現有策略附加至使用者] 的選項。然後從策略清單中選取AWSApplicationDiscoveryAgentlessCollectorAccessAWS受管理的策略。

接下來，選取DMSCollectorPolicy和FleetAdvisorS3Policy客戶受管 IAM 政策。

- 執行有關檢視使用者存取金鑰 (存取金鑰 ID 和秘密存取金鑰) 的步驟時，請遵循關於將使用者新存取金鑰 ID 和秘密存取金鑰儲存在安全可靠的地方的重要注意事項中的指引。您將需要這些訪問密鑰 [步驟 5：設定無代理程式收集器](#)。

這是旋轉存取金鑰的AWS安全性最佳做法。如需 [輪換金鑰的詳細資訊](#)，請參閱 [《IAM 使用者指南》](#) 中針對需要長期登入資料的使用案例定期輪換存取金鑰。

步驟 2：下載無代理程式收集器

若要設定 Application Discovery Service 無代理程式收集器 (無代理程式收集器)，您必須下載並部署無代理程式收集器開放虛擬化封存 (OVA) 檔案。無代理程式收集器是您在內部部署 VMware 環境中安裝的虛擬應用裝置。此步驟說明如何下載收集器 OVA 檔案，下一個步驟說明如何部署它。

下載收集器 OVA 檔案並驗證其總和檢查碼

1. 以 VMware 管理員身分登入 vCenter，然後切換至要下載無代理程式收集器 OVA 檔案的目錄。
2. 從下列網址下載 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上一個步驟中下載的 ApplicationDiscoveryServiceAgentlessCollector 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
```

步驟 3：部署無代理程式收集器

Application Discovery Service 無代理程式收集器 (無代理程式收集器) 是您在內部部署 VMware 環境中安裝的虛擬應用裝置。本節說明如何在 VMware 環境中部署您在上一個步驟中下載的開放虛擬化封存 (OVA) 檔案。

無代理程式收集器虛擬機器規格

- 操作系統 — Amazon Linux 2
- 記憶體 — 16 GB
- 中央處理器 — 4 核心

下列程序會逐步引導您在 VMware 環境中部署無代理程式收集器 OVA 檔案。

部署無代理程式收集器

1. 以 VMware 管理員身分登入 vCenter。
2. 使用下列其中一種方式安裝 OVA 檔案：
 - 使用 UI：選擇 [檔案]，選擇 [部署 OVF 範本]，選取您在上一節中下載的收集器 OVA 檔案，然後完成精靈。
 - 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 開放虛擬化格式工具 (ovftool)。若要下載 ovftool，請從 [OVF 工具](#) 文件頁面中選取一個版本。

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

- 名稱是您要用於無代理程式收集器虛擬機器的名稱。
 - 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 檔案的名稱。
 - 使用者名稱/密碼是您的 vCenter 認證。
 - 虛擬中心網址是您 vCenter 的網址。
 - vi 路徑是指向您的 VMware ESXi 主機的路徑。
3. 在 vCenter 中找出已部署的無代理程式收集器。以滑鼠右鍵按一下虛擬機器，然後選擇電源、開啟電源。
 4. 幾分鐘後，收集器的 IP 位址就會顯示在 vCenter 中。您可以使用此 IP 位址連線到收集器。

步驟 4：存取無代理程式收集器主控台

下列程序說明如何存取 Application Discovery Service 無代理程式收集器 (無代理程式收集器) 主控台。

存取無代理程式收集器主控台

1. 開啟網頁瀏覽器，然後在網址列中輸入下列 URL：**https://<ip_address>**，其 <ip_address> 中是收集器的 IP 位址 [步驟 3：部署無代理程式收集器](#)。
2. 第一次存取無代理程式收集器時，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無代理程式收集器主控台，接下來就可以了。[步驟 5：設定無代理程式收集器](#) 否則，接下來你會看到[無代理程式收集器儀表板](#)。

步驟 5：設定無代理程式收集器

Application Discovery Service 無代理程式收集器 (無代理程式收集器) 是以 Amazon Linux 2 為基礎的虛擬機器 (VM)。下節說明如何在無代理程式收集器主控台的 [設定無代理程式收集器] 頁面上設定收集器虛擬機器。

在 [設定無代理程式收集器] 頁面上設定收集器虛擬機器

1. 在收集器名稱中，輸入收集器名稱以識別它。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存取金鑰和密鑰，以指定為用於接收收集器探索到的資料的目的地帳戶。如需 IAM 使用者需求的相關資訊，請參閱[步驟 1：為無代理程式收集器建立 IAM 使用者](#)。
 - a. 對於AWS存取金鑰，請輸入您指定為目標AWS帳戶之帳戶 IAM 使用者的存取金鑰。
 - b. 對於AWS密鑰，請輸入您指定為目標AWS帳戶的帳戶 IAM 使用者的密鑰。
 - c. (選擇性) 如果您的網路需要使用 Proxy 來存取AWS，請輸入 Proxy 主機、Proxy 連接埠，並選擇性地輸入與現有 Proxy 伺服器進行驗證所需的認證。
3. 在無代理程式收集器密碼下，設定用來驗證無代理程式收集器存取權的密碼。
 - 密碼區分大小寫
 - 密碼長度必須介於 8 到 64 個字元之間
 - 密碼必須包含以下四種類別中的至少一個字元：
 - 小寫字母 (a-z)
 - 大寫字母 (A-Z)
 - 數字 (0-9)
 - 非字母數字字元 (@ \$! #%*? &)
 - 密碼不能包含下列字元以外的特殊字元：@ \$! #%*? &
 - a. 對於無代理程式收集器密碼，請輸入用來驗證收集器存取權的密碼。
 - b. 對於重新輸入無代理程式收集器密碼，以進行驗證，請再次輸入密碼。
4. 在「其他設定」下，閱讀「授權合約」。如果您同意接受，請選取核取方塊。

- 若要啟用無代理程式收集器的自動更新，請在「其他設定」下，選取「自動更新無代理程式收集器」。如果您未選取此核取方塊，則需要手動更新無代理程式收集器，如中所述。[手動更新無代理程式收集器](#)
- 選擇 [儲存組態]。

下列主題說明選用的收集器組態工作。

選擇性組態工作

- [\(選擇性\) 為無代理程式收集器虛擬機器設定靜態 IP 位址](#)
- [\(選擇性\) 將無代理程式收集器虛擬機器重設回使用 DHCP](#)
- [\(選擇性\) 設定 Kerberos 驗證通訊協定](#)

(選擇性) 為無代理程式收集器虛擬機器設定靜態 IP 位址

下列步驟說明如何為 Application Discovery Service 收集器 (無代理程式收集器) 虛擬機器設定靜態 IP 位址。第一次安裝時，收集器虛擬機器會設定為使用動態主機設定通訊協定 (DHCP)。

Note

無代理程式收集器支援 IPv4。它不支持 IPv6。

設定收集器虛擬機器的靜態 IP 位址

- 從 VMware 虛擬 vCenter 收集下列網路資訊：
 - 靜態 IP 位址 — 子網路中未簽署的 IP 位址。例如，一九二六八年八月一三八日。
 - 網路遮罩 — 這可透過檢查裝載收集器虛擬機器之 VMware vCenter 主機的 IP 位址設定來取得。舉例來說，是一個例子。
 - 預設閘道 — 這可透過檢查裝載收集器虛擬機器之 VMware vCenter 主機的 IP 位址設定來取得。例如，一九二一六八年一月一日。
 - 主要 DNS — 這可透過檢查裝載收集器虛擬機器之 VMware vCenter 主機的 IP 位址設定來取得。例如，一九二一六八年一月一日。
 - (選擇性) 次要 DNS
 - (選用) 本機網域名稱 — 這可讓收集器存取不含網域名稱的 vCenter 主機 URL。
- 開啟收集器的 VM 主控台，然後 `ec2-user` 使用密碼 `collector` 登入，如下列範例所示。

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

3. 透過在遠端終端機中輸入以下指令來停用網路介面。

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

4. 使用下列步驟更新介面 eth0 組態。

- a. 使用以下命令在 vi 編輯器中打開 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介面值，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. 使用以下命令在 vi 中打開 resolv.conf 文件。

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

- b. 使用以下命令更新 vi 中的 resolv.conf 文件。

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

下列範例顯示編輯過的 resolv.conf 檔案。

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

6. 輸入以下指令來啟用網路介面。

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

7. 將虛擬機器重新開機，如下列範例所示。

```
sudo reboot
```

8. 使用以下步驟驗證您的網路設定。

- a. 通過輸入以下命令來檢查 IP 地址是否配置正確。

```
ifconfig
ip addr show
```

- b. 輸入下列指令，檢查閘道是否已正確新增。

```
route -n
```

輸出應與下列範例類似。

```
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      0
```

- c. 輸入下列命令，確認您可以 Ping 公開 URL。

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

- d. 確認您可以偵測 vCenter IP 位址或主機名稱，如下列範例所示。

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

(選擇性) 將無代理程式收集器虛擬機器重設回使用 DHCP

下列步驟說明如何將無代理程式收集器虛擬機器重新設定為使用 DHCP。

將收集器虛擬機器設定為使用 DHCP

1. 透過在遠端終端機中輸入以下指令來停用網路介面。

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

2. 使用下列步驟更新網路組態。

- a. 使用以下命令在 vi 編輯器中打開 `ifcfg-eth0` 文件。

```
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. 輸入以下指令來啟用網路介面。

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

5. 將收集器虛擬機器重新開機，如下列範例所示。

```
sudo reboot
```

(選擇性) 設定 Kerberos 驗證通訊協定

如果您的作業系統伺服器支援 Kerberos 驗證通訊協定，則您可以使用此通訊協定來連線到伺服器。若要這麼做，您必須設定 Application Discovery Service 無代理程式收集器虛擬機器。

下列步驟說明如何在應用程式探索服務無代理程式收集器虛擬機器上設定 Kerberos 驗證通訊協定。

在收集器虛擬機器上設定 Kerberos 驗證通訊協定

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

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

2. 開啟 `/etc` 料夾中的 `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. 將收集器虛擬機器重新開機，如下列範例所示。

```
sudo reboot
```

步驟 6：設定無代理程式收集器資料收集模組

在資料收集下的 Application Discovery Service 無代理程式收集器 (無代理程式收集器) 主控台儀表板頁面上，您可以設定資料收集模組，以便從伺服器收集庫存、設定檔和使用率資料。

無代理程式收集器目前支援從 VMware VM 以及資料庫和分析伺服器收集資料。未來的模組將支援從其他虛擬化平台收集，以及作業系統層級的集合。

主題

- [無代理程式收集器資料收集模組](#)
- [資料庫與分析資料收集模組](#)

無代理程式收集器資料收集模組

本節說明 Application Discovery Service 無代理程式收集器 (無代理程式收集器) VMware vCenter 資料收集模組，該模組用於從 VMware VM 收集伺服器詳細目錄、設定檔和使用率資料。

主題

- [如何為 VMware vCenter 設定無代理程式收集器資料收集模組](#)
- [VMware 資料收集詳細資料](#)
- [控制 vCenter 資料收集的範圍](#)

如何為 VMware vCenter 設定無代理程式收集器資料收集模組

本節說明如何設定無代理程式收集器 VMware vCenter 資料收集模組，以便從 VMware 虛擬機器收集伺服器詳細目錄、設定檔和使用率資料。

Note

在開始 vCenter 安裝之前，請確定您可以提供 vCenter 認證，並為系統群組設定「讀取」和「檢視」權限。

若要設定資料收集模組

1. 在無代理程式收集器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 認證下：
 - i. 對於 vCenter 網址/IP，請輸入您的 VMware vCenter 伺服器主機的 IP 位址。
 - ii. 對於 vCenter 使用者名稱，請輸入收集器用來與 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：
 - 若要在成功設定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 資料收集詳細資料頁面，如下一個主題所述。

VMware 資料收集詳細資料

VMware 資料收集詳細資料頁面會顯示您在中設定之 vCenter 的詳細資料[如何為 VMware vCenter 設定無代理程式收集器資料收集模組](#)。

在 [探查到的 vCenter 伺服器] 下，會列出您設定的 vCenter，其中包含有關 vCenter 的下列資訊：

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

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。資料收集開始之後，[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 伺服器詳細目錄的資料，則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。

如果未封鎖您對網際網路的存取，您可以在此頁面上選擇「檢視 Migration Hub」中的伺服器，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 主控台的相關資訊，請參閱[步驟 7：檢視收集的資料](#)。

以下是根據移轉規劃活動建議的資料收集時間長度的準則：

- 總持有成本 (總擁有成本)-2 至 4 週
- 移轉規劃-2 至 6 週

控制 vCenter 資料收集的範圍

vCenter 使用者需要每個 ESX 主機或虛擬機器的唯讀權限，才能使用應用程式探索服務進行清查。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 下的所有主機和虛擬機器，也可以授與權限。case-by-case

Note

我們的安全最佳實務是建議您不是將其他不需要的權限授與 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 用戶端 6.7.0.2 版。其他版本用戶端的程序可能會有所不同，具體取決於您使用的 vSphere Client 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，然後選擇權限。
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元件。
4. 從「角色」功能表選擇「唯讀」。
5. 選擇「傳播至子系」，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 主機或子系虛擬機器的相關資料

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)。
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 OK (確定)。

Note

如果您選擇 [傳播至子系]，您仍然可以 case-by-case 依據從 ESX 主機和虛擬機器移除唯讀權限。此選項不會影響套用到其他 ESX 主機和 VM 的已繼承許可。

資料庫與分析資料收集模組

本節說明如何設定、設定和使用資料和分析資料收集模組和分析資料收集模組。您可以使用此資料收集模組連線至資料環境，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。如需可使用此模組收集的測量結果資訊，請參閱 [無代理程式收集器資料庫和分析資料收集模組所收集的資料](#)。

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 Server 2012 版本及截止至 2019 年版本和 2019 版本
- MySQL 5.6 版本 5.6 版本和最新版本 5.6 版本
- 甲骨文版本 11 克版本 2 和最多 12 分，19c 和 21c
- PostgreSQL 9.6 版和最新版本 9.6 版本和最新版本

建立資AWS DMS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控制台中查看收集的數據，也可以使用它來確定大小適中的AWS目標引擎。如需詳細資訊，請參閱[使用AWS DMS叢集建議程式目標建議功能](#)。

在建立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。當您完成中的先決條件時，就已建立此 Amazon S3 儲存貯體[無代理程式收集器的先決條件](#)。

為您的AWS DMS資料收集器建立 IAM 角色以存取 Amazon S3 S3 S3 的角色。

1. 登入 AWS Management Console，並開啟位於 <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 [選取信任的實體] 頁面上，針對 [信任的實體類型] 選擇 [AWS服務] 對於其他AWS服務的使用案例，請選擇 DMS。
4. 選取 [DMS] 核取方塊，然後選擇 [下一步]。
5. 在 [新增權限] 頁面上，選擇您之前建立的 FleetAdvisorS3 原則。選擇 下一步。
6. 在 [名稱、檢閱和建立] 頁面上，輸入 **FleetAdvisorS3Role** [角色名稱]，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 Edit trust policy (編輯信任政策)。
8. 在 [編輯信任原則] 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 Update policy (更新政策)。

現在，在控制台中創建一個數據收集AWS DMS器。

建立AWS DMS資料收集器

1. 請登入AWS Management Console並開啟AWS DMS主控台，網址為 <https://console.aws.amazon.com/dms/v2/>。
2. 選擇您設定為 Migration Hub 本AWS 區域地區域的項目。如需詳細資訊，請參閱[登入移轉中心並選擇主地區域](#)。
3. 在導覽窗格中，選擇探索下的資料收集器。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」區段中的「名稱」中，輸入資料收集器的名稱。
6. 在「連線」區段中，選擇「瀏覽 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FleetAdvisorS3Role之前建立的角色。
8. 選擇建立資料收集器。

設定資料轉送

建立必要的AWS資源之後，請設定從資料庫和 Analytics 資料AWS DMS收集模組轉送至您的收集器的資料。

設定資料轉送

1. 開啟無代理程式收集器主控台。如需詳細資訊，請參閱[步驟 4：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 [資料轉寄] 區段中的 [設定資料轉寄]。
4. 對於 AWS 區域IAM 存取金鑰 ID 和 IAM 秘密存取金鑰，您的無代理程式收集器會使用您之前設定的值。如需詳細資訊，請參閱[登入移轉中心並選擇主地區域](#) 及 [步驟 1：建立 IAM 使用者](#)。

5. 對於 [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。

設定資料轉寄之後，請檢查 [儀表板] 頁面上的 [資料轉寄] 區段。請確定您的資料庫和分析資料收集模組顯



示
連線以存取 DMS 和 S3 存取。

已

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會使用微軟 Active Directory 中的 LDAP 來收集您網路中的作業系統、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。

若要將 LDAP 伺服器新增至您的資料庫和分析資料收集模組

1. 開啟無代理程式收集器主控台。如需詳細資訊，請參閱[步驟 4：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. 在主機名稱中，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. 在使用者名稱中，輸入您用來連線 LDAP 伺服器的使用者名稱。
7. 針對密碼，輸入您用來連線 LDAP 伺服器的密碼。
8. (選擇性) 選擇驗證連線，確定您已正確新增 LDAP 伺服器認證。或者，您可以稍後從 LDAP 伺服器頁面上的清單驗證 LDAP 伺服器連線認證。
9. 選擇 [新增 LDAP 伺服器]。
10. 在 LDAP 伺服器頁面上，從清單中選取您的 LDAP 伺服器，然後選擇探索作業系統伺服器。

⚠ Important

針對作業系統探查，資料收集模組需要認證，網域伺服器才能使用 LDAP 通訊協定執行要求。

數據庫和分析數據收集模塊連接到您的 LDAP 服務器，並發現您的操作系統服務器。資料收集模組完成作業系統伺服器探索之後，您可以選擇 [檢視作業系統伺服器] 來查看探查到的作業系統伺服器清單。

或者，您可以手動新增作業伺服器，或從逗號分隔值 (CSV) 文件格式的伺服器清單。此外，您也可以使用 VMware vCenter 無代理程式收集器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[資料收集模組](#)。

若要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 [OS 伺服器]。
2. 選擇 [新增 OS 伺服器]。新增作業系統伺服器頁面隨即開啟
3. 提供作業系統伺服器認證。
 - a. 對於作業系統類型，請選擇伺服器的作業系統。
 - b. 在主機名稱/IP 中，輸入作業系統伺服器的主機名稱或 IP 位址。
 - c. 針對連接埠，輸入用於遠端查詢的連接埠號碼。
 - d. 針對 [驗證類型]，請選擇作業系統伺服器使用的驗證類型。
 - e. 在使用者名稱中，輸入您用來連線到作業系統伺服器的使用者名稱。
 - f. 針對密碼，輸入您用於連線作業系統伺服器的密碼。
 - g. 選擇 [驗證] 以確定您已正確新增作業系統伺服器認證。
4. (選擇性) 從 CSV 檔案新增多個作業系統伺服器。
 - a. 選擇「從 CSV 大量匯入 OS 伺服器」。
 - b. 選擇「下載範本」以儲存包含您可自訂範本的 CSV 檔案。
 - c. 根據範本，將作業系統伺服器的連線認證輸入到檔案中。以下範例示範如何在 CSV 檔案中提供作業伺服器連線憑證。

```
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認證後，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 OS 伺服器]。
6. 新增所有作業系統伺服器的認證後，請選取您的作業系統伺服器並選擇探索資料庫伺服器

探索資料庫伺服器

對於資料庫探索，請使用資料收集模組所需的最低權限為來源資料庫建立使用者。如需詳細資訊，請參閱《[使用指南](#)》中的「[為AWS DMS叢集建立資料庫AWS DMS使用者](#)」。

若要探索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。確定您的資料庫可以存取您在連線設定中指定的連接埠。接下來，打開數據庫服務器上的遠程身份驗證。除此之外，請為您的資料收集模組提供下列權限。

在 Windows 中探索資料庫伺服器

1. 提供授權的認證，以執行 Windows 管理檢測 (WMI) 和 WMI 查詢語言 (WQL) 查詢，並讀取登錄。
2. 將您在作業系統伺服器連線認證中指定的 Windows 使用者新增至下列群組：分散式 COM 使用者、效能記錄檔使用者、效能監視器使用者和事件記錄讀取器。若要這麼做，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，取代 *username* 您在作業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認證中指定的 Windows 使用者授與必要權限。
 - 對於 [Windows 管理及檢測內容]，請選擇 [本機啟動和遠端啟動]。
 - 對於 WMI Control，請為、和 WMI 命名空間選擇執行方法、啟用帳戶 **CIMV2DEFAULTStandartCimv2**、遠端啟用和讀取安全性權限。
 - 對於 WMI 外掛程式，請執行 `winrm configsddl default` 然後選擇讀取並執行。
4. 使用下列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 ICMP 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 Negotiate auth usage
winrm set winrm/config/service '@{AllowUnencrypted="true"}' # Allow unencrypted
connection
```

在 Linux 中探索資料庫伺服器

1. 提供 `sudo` 對 `ss` 和 `netstat` 指令的存取權。

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

```
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，取代 *username* 您在 OS Server 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` 指令的 `/usr/bin/` 路徑。此路徑在您的環境中可能會有所不同。若要確定 `ss` 和 `netstat` 指令的路徑，請執行 `which ss` 和 `which netstat` 指令。

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。

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 [OS 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，然後選擇 [動作] 功能表上的 [驗證連線]。
3. 對於連線狀態為失敗的伺服器，請編輯連線認證。
 - a. 選取單一或多部伺服器，如果它們具有相同的認證，然後選擇「動作」功能表上的「編輯」。
[編輯 OS 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 [驗證類型]，請選擇作業系統伺服器使用的驗證類型。
 - d. 在使用者名稱中，輸入您用來連線到作業系統伺服器的使用者名稱。
 - e. 針對密碼，輸入您用於連線作業系統伺服器的密碼。
 - f. 選擇 [驗證連線]，確定您已正確更新作業系統伺服器認證。接下來，選擇「儲存」。
4. 更新所有作業系統伺服器的認證後，請選取您的作業系統伺服器並選擇探索資料庫伺服器

資料庫和分析資料收集模組會連接到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查之後，您可以選擇檢視資料庫伺服器，查看探查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詳細目錄。此外，您也可以從 CSV 檔案匯入伺服器清單。如果您已將所有資料和分析伺服器和分析伺服器和分析伺服器和分析伺服器和分析伺服器

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認證。
 - a. 對於「資料庫引擎」，請選擇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. 在「主機名稱/IP」中，輸入資料庫或分析伺服器的主機名稱或 IP 位址。
 - c. 在連接埠中，輸入伺服器執行的連接埠。
 - d. 針對「驗證類型」，請選擇資料庫或分析伺服器使用的驗證類型。
 - e. 在 [使用者名稱] 中，輸入您用來連線至伺服器的使用者名稱。
 - f. 針對密碼，輸入您用於連線伺服器的密碼。
 - g. 選擇 [驗證] 以確定您已正確新增資料庫或分析伺服器認證。
4. (選擇性) 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」以儲存包含您可自訂範本的 CSV 檔案。
 - c. 根據範本，將資料庫和分析伺服器的連線認證輸入到檔案中。以下範例示範如何在 CSV 檔案中提供資料或分析伺服器連線憑證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認證後，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認證後，請選取您的作業系統伺服器並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，請將它們新增至詳細目錄。資料庫和分析資料收集模組可以從清查連線到伺服器，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詳細目錄

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. 選取您要為其收集中繼資料和效能度量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詳細目錄後，就可以開始收集中繼資料和效能指標。如需詳細資訊，請參閱 [資料庫與分析資料收集](#)。

步驟 7：檢視收集的資料

您可以檢視應用程式探索服務無代理程式收集器 (無代理程式收集器) 在 Migration Hub 主控台中收集的資料。您可以在 AWS DMS 主控台中檢視為資料庫和分析伺服器收集的指標。

檢視 VMware vCenter 無代理程式收集器資料收集模組探查到的資料

1. 登入AWS Management Console並開啟 Migration Hub 主控台，網址為 <https://console.aws.amazon.com/migrationhub/>。針對此工作，建議您使用與您建立的 IAM 使用者不同的 IAM 使用者帳戶來設定和存取無代理程式收集器。
2. 在 [Migration Hub] 主控台瀏覽窗格的 [探索] 下，選擇 [伺服器]。
3. 若要檢視伺服器的詳細資訊，請從「伺服器資訊」欄中選擇伺服器的主機名稱。伺服器的詳細資訊頁面會顯示伺服器的相關資訊，例如主機名稱、IP 位址、效能測量結果等。

若要檢視資料庫和分析資料收集模組探索到的資料

1. 請登入AWS Management Console並開啟AWS DMS主控台，網址為 <https://console.aws.amazon.com/dms/v2/>。
2. 選擇 [探索] 下的 [庫存「庫存」頁面隨即開啟。
3. 選擇 [分析清查] 以決定資料庫結構描述屬性，例如相似性和複雜性。
4. 選擇綱要頁籤以查看分析結果。

您可以使用AWS DMS主控台來識別重複的結構描述、判斷移轉複雜度，以及匯出詳細目錄資訊以供 future 分析之用。如需詳細資訊，請參閱[AWS DMS叢集顧問中的使用庫存進行分析](#)。

無代理程式收集器所收集的資料

您可以設定 Application Discovery Service 無代理程式收集器 (無代理程式收集器) 資料收集模組，以便從伺服器收集庫存、設定檔和使用率資料。

無代理程式收集器目前支援從 VMware VM 以及資料庫和分析伺服器收集資料。未來的模組將支援從其他虛擬化平台收集，以及作業系統層級的集合。若要取得有關設定資料收集的資訊，請參閱[步驟 6：設定無代理程式收集器資料收集模組](#)。

下列主題說明 Application Discovery Service 收集器 (無代理程式收集器) 資料收集模組所收集的資料。

主題

- [無代理程式收集器 VMware vCenter 資料收集模組所收集的資料](#)
- [無代理程式收集器資料庫和分析資料收集模組所收集的資料](#)

無代理程式收集器 VMware vCenter 資料收集模組所收集的資料

下列資訊說明 Application Discovery Service 收集器 (無代理程式收集器) VMware vCenter 資料收集模組所收集的資料。若要取得有關設定資料收集的資訊，請參閱[如何為 VMware vCenter 設定無代理程式收集器資料收集模組](#)。

無代理程式收集器 VMware vCenter 收集資料的表格圖例：

- 收集的資料是以千位元組 (KB) 為單位 (除非另有指明)。
- Migration Hub 主控台對等的資料以 MB 為單位報告。
- 以星號 (*) 表示的資料欄位只能在從應用程式探索服務 API 匯出功能產生的 .csv 檔案中使用。

無代理程式收集器支援使用 CLI 匯出資料。AWS 若要使用 AWS CLI 匯出收集的資料，請遵循「應用程式探索服務使用者指南」中「匯出收集的資料」頁面中「匯出所有伺服器的系統效能資料」中所述的指示進行。

- 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*	虛擬機器分組所在之移轉應用程式的識別碼。
avgCpuUsage百分比	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 作業的平均數為空值。
avgDiskWriteOpsPerSecond**	每秒寫入 I/O 作業的平均數目。
avgFreeRAM	平均可用記憶體 (以 MB 表示)。
avgNetworkBytesReadPerSecond	每秒讀取的位元組平均輸送量。
avgNetworkBytesWrittenPerSecond	每秒寫入的位元組平均輸送量。
電腦製造商	ESXi 主機報告的廠商。

資料欄位	描述
计算机模型	ESXi 主機報告的電腦型號。
configId	應用程式探索服務指派給探查到的虛擬機器的 ID。
configType	發現的資源類型。
connectorId	虛擬應用裝置的識別碼。
cpuType	虛擬機器的 vCPU，主機的實際模型。
datacenterId	vCenter 的識別碼。
hostId*	虛擬機器主機識別碼。
hostName	執行虛擬化軟體的主機名稱。
hypervisor	管理程序的類型。
id	伺服器的識別碼。
lastModifiedTime郵票*	資料匯出前最近收集資料的日期和時間。
macAddress	虛擬機器的 MAC 位址。
manufacturer	虛擬化軟體的製造商。
maxCpuUsage百分比	輪詢期間 CPU 使用率的最大百分比。
maxDiskBytesReadPerSecond	輪詢期間從磁碟讀取的最大位元組數。
maxDiskBytesWrittenPerSecond	輪詢期間寫入磁碟的最大位元組數。
maxDiskReadOpsPerSecond**	每秒讀取 I/O 作業的最大數目。
maxDiskWriteOpsPerSecond**	每秒寫入 I/O 作業數目上限。
maxNetworkBytesReadPerSecond	每秒讀取的最大位元組輸送量。
maxNetworkBytesWrittenPerSecond	最大。每秒寫入的字節吞吐量。

資料欄位	描述
memoryReservation [*]	限制以避免虛擬機器上的記憶體過度承諾。
moRefId	唯一的 vCenter 受管理物件參考識別碼。
name [*]	虛擬機器或網路的名稱 (使用者指定)。
numCores	指派給虛擬機器的 CPU 核心數目。
numCpus	ESXi 主機上的 CPU 通訊端數目。
numDisks ^{**}	虛擬機器上的磁碟數目。
numNetworkCards ^{**}	虛擬機器上的網路卡數目。
osName	虛擬機器上的作業系統名稱。
osVersion	虛擬機器上的作業系統版本。
portGroupId [*]	VLAN 成員連接埠群組的識別碼。
portGroupName [*]	VLAN 成員連接埠群組的名稱。
powerState [*]	電源狀態。
serverId	Application Discovery Service 指派給探查到的虛擬機器的 ID
smBiosId [*]	系統管理 BIOS 的識別碼/版本。
state [*]	虛擬應用裝置的狀態。
toolsStatus	VMware 工具的運作狀態
totalDiskFree大小	可用磁碟空間 (以 MB 表示)。適用於 vCenter 伺服器 7.0 及更新版本。
totalDiskSize	磁碟總容量 (以 MB 表示)。
totalRAM	虛擬機器上可用的 RAM 總容量，以 MB 為單位。

資料欄位	描述
type	主機的類型。
vCenterId	虛擬機器的唯一識別碼。
vCenterName *	vCenter 主機的名稱。
virtualSwitchName *	虛擬交換器的名稱。
vmFolderPath	虛擬機器檔案的目錄路徑。
vmName	虛擬機器的名稱。

無代理程式收集器資料庫和分析資料收集模組所收集的資料

應用程式探索服務無代理程式收集器 (無代理程式收集器) 資料庫和分析資料收集模組會從您的資料環境收集下列指標。如需設定資料收集的資訊，請參閱[資料庫與分析資料收集模組](#)。

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

- OS 伺服器上的可用記憶體
- 作業系統伺服器上的可用儲存
- 資料庫版本與版本
- 作業系統伺服器上的 CPU 數量
- 綱要數目
- 預存程序的次數 ()
- 表格數目
- 觸發程序的次數
- 觀看次數
- 結構構造

在AWS DMS主控台中啟動結構描述分析之後，您的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

- 架構複雜性
- 綱要的相似性

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

- 資料庫伺服器上的 I/O 輸送量
- 資料庫伺服器上的每秒讀寫次數 (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
- 作業系統伺服器的儲存使用量

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

使用無代理程式收集器主控台

本節說明如何使用應用程式探索服務無代理程式收集器 (無代理程式收集器) 主控台。

主題

- [無代理程式收集器儀表板](#)
- [編輯無代理程式收集器設定](#)
- [編輯 vCenter 認證](#)

無代理程式收集器儀表板

在 Application Discovery Service 無代理程式收集器 (無代理程式收集器) 儀表板頁面上，您可以看到收集器的狀態，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

收集器狀態會提供有關收集器的狀態資訊。收集器名稱、收集器與 AWS 的連線狀態、Migration Hub 本地區域以及版本。

若您有AWS連線問題，您可能需要編輯無代理程式收集器組態設定。

欲編輯收集器組態設定，請選擇「編輯收集器設定」，然後遵循中所述的指示[編輯無代理程式收集器設定](#)。

資料收集

在「資料收集」下，您可以選擇資料收集方法。Application Discovery Service 無代理程式收集器 (無代理程式收集器) 目前支援從 VMware VM 以及資料庫和分析伺服器收集資料。未來的模組將支援從其他虛擬化平台收集，以及作業系統層級的集合。

主題

- [vCenter 睿資料收集](#)
- [資料庫與分析資料收集](#)

vCenter 睿資料收集

若要從 VMware 虛擬機器收集伺服器詳細目錄、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，然後依照中所述的指示進行[步驟 6：設定無代理程式收集器資料收集模組](#)。

設定 vCenter 資料收集後，您可以從儀表板執行下列動作：

- 檢視資料收集狀態
- 開用資料收集
- 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。

資料庫與分析資料收集

您可以在以下兩種模式下運行數據庫和分析數據收集模塊。

元數據和數據庫容量

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、CPU、記憶體和磁碟容量等資訊。您可以使用此收集的資訊來計算AWS DMS主控台目標建議。如果來源資料庫已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的 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精確的目標建議，因為建議是根據實際的資料庫工作負載。在此模式中，資料收集模組會每分鐘收集效能測量結果。

若要開始從資料庫和分析伺服器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「資料庫詳細目錄」清單中，選取要為其收集中繼資料和效能測量結果的資料庫和分析伺服器。
3. 選擇 [執行資料收集]。[資料集合類型] 對話方塊隨即開啟。
4. 選擇如何收集資料以進行分析。

如果您選擇中繼資料、資料庫容量及資源使用率選項，請設定資料收集的期間。您可以在接下來的 7 天內收集資料，或將自訂範圍設定為 1-60 天。

5. 選擇 [執行資料收集]。「資料收集」頁面隨即開啟。
6. 選擇「集合健康情況」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到 Amazon S3 儲存貯體。然後，您可以按照中的說明檢視此收集的資料[步驟 7：檢視收集的資料](#)。

編輯無代理程式收集器設定

您在第一次設定應用程式探索服務無代理程式收集器 (無代理程式收集器) 時設定收集器，如中所述[步驟 5：設定無代理程式收集器](#)。下列程序說明如何編輯無代理程式收集器組態設定。

編輯收集器組態設定

- 選擇「無代理程式收集器」圖標板上的「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：

- 針對收集器名稱，輸入用來識別收集器的名稱。名稱可以包含空格，但不能包含特殊字元。
- 在探索資料的目的地AWS帳戶下，輸入AWS帳戶的AWS存取金鑰和秘密金鑰，以指定為接收收集器探索到的資料的目的地帳戶。如需 IAM 使用者需求的相關資訊，請參閱[步驟 1：為無代理程式收集器建立 IAM 使用者](#)。
 - 對於AWS存取金鑰，請輸入您指定為目標AWS帳戶之帳戶 IAM 使用者的存取金鑰。
 - 對於AWS密鑰，請輸入您指定為目標AWS帳戶的帳戶 IAM 使用者的密鑰。
- 在無代理程式收集器密碼下，變更新用來驗證無代理程式收集器存取權的密碼。
 - 對於無代理程式收集器密碼，請輸入用來驗證無代理程式收集器存取權的密碼。
 - 對於重新輸入無代理程式收集器密碼，以進行驗證，請再次輸入密碼。
- 選擇 [儲存組態]。

接下來，您會看到[無代理程式收集器儀表板](#)。

編輯 vCenter 認證

若要從 VMware 虛擬機器收集伺服器詳細目錄、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 連線的詳細資訊，請參閱[步驟 6：設定無代理程式收集器資料收集模組](#)。

本節說明如何編輯 vCenter 認證。

Note

在編輯 vCenter 認證之前，請確定您可以提供 vCenter 認證，並為系統群組設定了讀取和檢視權限。

若要編輯 vCenter 認證

在[VMware 資料收集詳細資料](#)頁面上，選擇編輯 vCenter 伺服器。

- 在「編輯 vCenter」頁面上，執行下列動作：
 - a. 在 vCenter 認證下：
 - i. 對於 vCenter 網址/IP，請輸入您的 VMware vCenter 伺服器主機的 IP 位址。
 - 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)。

手動更新無代理程式收集器

當您設定 Application Discovery Service 無代理程式收集器 (無代理程式收集器) 時，您可以選擇啟用自動更新，如中所述[步驟 5：設定無代理程式收集器](#)。如果您當時未啟用自動更新，則需要手動更新無代理程式收集器。

下列程序說明如何手動更新無代理程式收集器。

若要手動更新無代理程式收集器

1. 取得最新的無代理程式收集器開放式虛擬封存 (OVA) 檔案。
2. (選擇性) 建議您先刪除先前的無代理程式收集器 OVA 檔案，然後再部署最新檔案。
3. 在中[開始使用無代理程式收集器](#)區段中，遵循步驟[步驟 3：部署無代理程式收集器](#)通過[步驟 6：設定無代理程式收集器資料收集模組](#)。

Amazon Linux 2 上的 Kernel Live Patching

無代理程式收集器虛擬機器使用亞馬遜 Linux 2，如中所述[步驟 3：部署無代理程式收集器](#)。

若要啟用和使用 Amazon Linux 2 的即時修補，請參閱[Amazon Linux 2 上的 Kernel Live Patching](#)中的 Amazon EC2 Linux 執行個體使用者指南。

排解無代理程式收集器

本節包含的主題可協助您疑難排解應用程式探索服務無代理程式收集器 (無代理程式收集器) 的已知問題。

主題

- [修正無代理程式收集器在安裝期間無法到達 AWS](#)
- [修正連線至 Proxy 主機時的自我簽署憑證問題](#)
- [尋找不健康的收藏家](#)
- [修正 IP 位址問題](#)
- [修正 vCenter 認證問題](#)
- [修正資料庫和分析資料收集模組中的資料轉送問題](#)
- [修正資料庫和分析資料收集模組中的連線問題](#)
- [獨立式 ESX 主機支援](#)
- [連絡 Sup AWS port 以解決無代理程式收集器問題](#)

修正無代理程式收集器在安裝期間無法到達 AWS

無代理程式收集器需要透過 TCP 連接埠 443 對多個網域進行輸出存取。AWS 在主控台中設定無代理程式收集器時，您可能會收到下列錯誤訊息。

無法到達 AWS

AWS 無法到達。請確認網路設定。

發生此錯誤的原因是無代理程式收集器嘗試建立 HTTPS 連線至收集器在安裝程序期間需要與之通訊的 AWS 網域失敗。如果無法建立連線，無代理程式收集器組態就會失敗。

若要修正連線 AWS

1. 請洽詢您的 IT 管理員，瞭解貴公司的防火牆是否封鎖連接埠 443 上傳輸至任何需要輸出存取之 AWS 網域的輸出流量。哪些 AWS 網域需要輸出存取，取決於您的本地區域是美國西部 (奧勒岡) 區域、美國西部 -2 或其他區域。

如果您的 AWS 帳戶首頁區域為 us-west-2，則下列網域需要輸出存取：

- 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`

如果您的 AWS 帳戶主頁區域不是，則下列網域需要輸出存取 `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無代理程式收集器需要與之通訊之 AWS 網域的輸出存取，請在收集器組態下的 [資料同步化] 區段中設定 Proxy 主機。

2. 如果更新防火牆無法解決連線問題，請使用下列步驟來確保收集器虛擬機器具有與上一步驟所列網域的輸出網路連線。
 - a. 從 VMware vCenter 取得無代理程式收集器的 IP 位址。
 - b. 開啟收集器的 VM 主控台，並 `ec2-user` 使用密碼 `collector` 登入，如下列範例所示。

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

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

```
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](#) 設定靜態 DNS 伺服器。
4. 如果錯誤仍然存在，如需進一步的支援，請參閱 [連絡 Sup AWS port 以解決無代理程式收集器問題](#)。

修正連線至 Proxy 主機時的自我簽署憑證問題

如果與選擇性提供的 Proxy 通訊是透過 HTTPS，而代理伺服器具有自我簽署憑證，您可能需要提供憑證。

1. 從 VMware vCenter 取得無代理程式收集器的 IP 位址。
2. 開啟收集器的 VM 主控台，並 `ec2-user` 使用密碼 `collector` 登入，如下列範例所示。

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

3. 將與安全 Proxy 相關聯的憑證主體 (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，重新啟動無代理程式收集器：

```
sudo shutdown -r now
```

尋找不健康的收藏家

您可以在 AWS Migration Hub (Migration Hub) 主控台的 [資料收集器] 頁面上找到每個收集器的狀態資訊。您可以尋找任何「狀態」為「需要注意」的收集器，以識別有問題的收集器。

下列程序說明如何存取無代理程式收集器主控台以識別健全狀況問題。

存取無代理程式收集器主控台

1. 使用您的 AWS 帳戶登入 AWS Management Console 並開啟 Migration Hub 主控台，網址為 <https://console.aws.amazon.com/migrationhub/>。
2. 在 [Migration Hub] 主控台瀏覽窗格的 [探索] 下，選擇 [資料收集器]
3. 從無代理程式收集器索引標籤中，記下狀態為「需要注意」之每個連接器的 IP 位址。
4. 若要開啟無代理程式收集器主控台，請開啟 Web 瀏覽器。然後在網址列中輸入下列 URL：**https://<ip_address>**，其中 ip_address 是狀態不良的收集器的 IP 位址。
5. 選擇 [登入]，然後輸入 [無代理程式收集器] 密碼，此密碼是在中設定收集器時設定的。[步驟 5：設定無代理程式收集器](#)
6. 在無代理程式收集器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. 請依照中[編輯 vCenter 認證](#)的指示更正 URL 和認證。

修正健全狀況問題後，收集器將重新建立與 vCenter Server 的連線，且收集器的狀態將變更為 [收集] 狀態。如果問題仍然存在，請參閱[連絡 Sup AWS port 以解決無代理程式收集器問題](#)。

不健全的收集器最常見的原因是 IP 位址和認證問題。[修正 IP 位址問題](#)並[修正 vCenter 認證問題](#)可協助您解決這些問題，並將收集器恢復為正常狀態。

修正 IP 位址問題

如果收集器設定期間提供的 vCenter 端點格式錯誤、無效，或者 vCenter Server 目前已關閉且無法連線，則收集器可能會進入狀況不良狀態。在此情況下，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 位址問題

1. 從 VMware vCenter 取得無代理程式收集器的 IP 位址。
2. 開啟網頁瀏覽器以開啟無代理程式收集器主控台，然後在網址列中輸入下列 URL：**https://<ip_address>**，其中 ip_address 是收集器的來源 IP 位址。[步驟 3：部署無代理程式收集器](#)
3. 選擇 [登入]，然後輸入 [無代理程式收集器] 密碼，此密碼是在中設定收集器時設定的。[步驟 5：設定無代理程式收集器](#)
4. 在無代理程式收集器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 資料收集詳細資料頁面的 [探查到的 vCenter 伺服器] 下，記下 vCenter 資料行中的 IP 位址。
6. 使用單獨的命令列工具 (例如 ping 或 traceroute)，驗證關聯的 vCenter 伺服器處於作用中狀態，並且可從收集器虛擬機器存取 IP。
 - 如果 IP 位址不正確且 vCenter 服務處於作用中狀態，請在收集器主控台中更新 IP 位址，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，請更新防火牆設定以允許來自收集器虛擬機器的傳入連線。

修正 vCenter 認證問題

如果設定收集器時提供的 vCenter 使用者認證無效，或者沒有 vCenter 讀取和 View 帳戶權限，則收集器可能會進入狀況不良狀態。

如果您遇到與 vCenter 認證相關的問題，請檢查以確保您已為系統群組設定 vCenter 讀取和檢視權限。

如需編輯 vCenter 認證的相關資訊，請參閱[編輯 vCenter 認證](#)。

修正資料庫和分析資料收集模組中的資料轉送問題

無代理程式收集器中資料庫和分析資料收集模組的首頁會顯示 DMS 存取和 S3 存取的連線狀態。如果您看到「無法存取 DMS」和「S3 的存取權」，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 DMS CollectorPolicy 和 FleetAdvisorS3 政策政策新增至您的 IAM 使用者。如需詳細資訊，請參閱[步驟 1：為無代理程式收集器建立 IAM 使用者](#)。

如果您的資料收集模組無法連線到 AWS，請提供下列網域的輸出存取權。

- `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

無代理程式收集器中的資料庫和分析資料收集模組會連線到 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到您的作業系統伺服器，以探索資料庫和分析伺服器。資料收集模組會從這些資料庫伺服器收集容量和效能測量結果。如果您的資料收集模組無法連線到這些伺服器，請確認您可以連線到伺服器。

在下列範例中，將#取代值取代為您的值。

- 若要確認您是否可以連線到 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。

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

- 若要確認您是否可以連線到 Linux 作業系統伺服器，請使用下列指令。

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

在 Windows 中以系統管理員身分執行上一個範例。

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

在 Linux 中執行上一個範例。

- 若要確認您是否可以連線到 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 中以系統管理員身分執行上一個範例。

```
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 中執行上一個範例。

- 若要確認您是否可以連線到 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
```

- 要驗證您是否可以連接到 MySQL 數據庫，請使用以下命令。

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

- 若要確認您是否可以連線到 Oracle 資料庫，請使用下列命令。

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

- 若要確認您是否可以連線到 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
```

如果您無法連線到資料庫和分析伺服器，請確定您提供必要的權限。如需詳細資訊，請參閱 [探索資料庫伺服器](#)。

獨立式 ESX 主機支援

無代理程式收集器不支援獨立 ESX 主機。ESX 主機必須屬於 vCenter Server 執行個體的一部分。

連絡 Sup AWS port 以解決無代理程式收集器問題

如果您遇到應用程式探索服務無代理程式收集器 (無代理程式收集器) 的問題，並且需要協助，請連絡 Sup [AWS port](#) 部門，系統可能會要求您傳送收集器記錄檔。

取得無代理程式收集器記錄

1. 從 VMware vCenter 取得無代理程式收集器的 IP 位址。
2. 開啟收集器的 VM 主控台，並 **ec2-user** 使用密碼 **collector** 登入，如下列範例所示。

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

3. 使用下列命令導覽至記錄檔資料夾。

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

4. 使用下列命令壓縮記錄檔。

```
sudo cp /local/agentlesscollector/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. 從無代理程式收集器虛擬機器複製記錄檔。

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

6. 將 tar.gz 檔案交給 AWS 企業 Support。

Migration Hub 匯入

AWS Migration Hub(Migration Hub) 匯入可讓您將現場部署環境的詳細資訊直接匯入 Migration Hub，而無需使用 Application Discovery Service 無代理程式收集器 (無代理程式收集器) 或AWS應用程式探索代理程式 (探索代理程式)，因此您可以執行遷移評估和直接規劃匯入的資料。您也可以將裝置群組為應用程式並追蹤其遷移狀態。

啟動匯入請求

- 下載特殊格式化的逗號分隔值 (CSV) 匯入範本。
- 填入您現有的內部部署伺服器資料。
- 使用 Migration Hub 主控台將其上傳至 Migration Hub，AWS CLI或其中一個AWS開發套件

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 已提供連結以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](#)。

支援的匯入檔案欄位

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。

以下表格中匯入欄位名稱旁的星號表示其為必要欄位。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。

Note

如果您使用的是 VMware。MoRefId 或者 VMWARECenterId，為識別記錄，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 "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
VMwareMoRefId*	受管物件參考 ID。必須以 VMware.VCenterId。	
VMware.VCenterId*	虛擬機器唯一識別符。必須以 VMwareMoRefId。	
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 CPU 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

匯入欄位名稱	描述	範例
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
RAM.UsedSizeIn平均百分比	伺服器上已用記憶體的平均數量，以 MB 為單位。	64 128
RAM.UsedSizeIn兆。最大	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。最大	當探索工具收集資料時的最大 CPU 使用率。	55.34 24
DiskReadsPerSecondIn平均	磁碟平均每秒讀取的數目，以 KB 為單位。	1159 84506
DiskWritesPerSecondIn平均	磁碟平均每秒寫入的數目，以 KB 為單位。	199 6197

匯入欄位名稱	描述	範例
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
DiskReadsOpsPerSecond。最大	磁碟每秒讀取操作的最大數目。	1083 176
DiskWritesOpsPerSecond。最大	磁碟寫入操作的每秒最大次數。	535 71
NetworkReadsPerSecondIn平均	網路讀取操作的每秒平均數量，以 KB 為單位。	45 28
NetworkWritesPerSecondIn平均	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

匯入欄位名稱	描述	範例
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"
Tags (標籤)	以逗號分隔的標籤清單，格式為「名稱:值」。 <div style="border: 1px solid #f08080; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p>⚠ Important</p> <p>請不要將敏感資訊 (例如個人資料) 儲存在標籤中。</p> </div>	"zone:1, critical:yes" "zone:3, critical:no, zone:1"

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[探索到的伺服器 and 應用程式的比對](#)。

Note

Migration Hub 匯入不支援匯入範本所定義之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。

設定您的匯入許可

在您可以匯入您的資料之前，請確定您的 IAM 使用者具有必要的 Amazon S3 許可，可以上傳 (s3:PutObject) 你的導入文件到 Amazon S3，並讀取對象 (s3:GetObject)。您也必須建立程式設計方式的存取 (適用於AWS CLI) 或主控台存取，透過建立一個 IAM 政策，並將其連接至在您的 IAM 使用者，以執行匯入的 IAM 使用者AWS帳戶。

Console Permissions

使用下列步驟編輯將在您的下列步驟進行匯入請求的 IAM 使用者的許可政策。AWS 使用主控台的帳戶。

編輯使用者連接的受管政策

1. 登入 AWS Management Console，並開啟位於 <https://console.aws.amazon.com/iam/> 的 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 Review policy (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 Create policy (建立政策)。
6. 返回授予許可IAM 主控台頁面的使用者，讓您的匯入請求在您的AWS帳戶。
 7. 重新整理政策表，並搜尋您剛建立的政策名稱。
 8. 選擇 Next: (下一步 :) Review (檢閱)。
 9. 選擇 Add permissions (新增許可)。

現在您已將政策新增至 IAM 使用者，您已準備好啟動匯入程序。

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AWS CLI。

建立並連接受管政策

1. 使用`aws iam create-policy` AWS CLI命令以建立具備以下許可的 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/*"]
    }
  ]
}

```

```
]
}
```

如需使用這個命令的詳細資訊，請參閱[create-policy](#)中的AWS CLI命令參考。

2. 使用`aws iam create-policy` AWS CLI命令以建立具備以下許可的其他 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，將您在前兩個步驟建立的政策連接至 IAM 使用者，這名使用者將在您的AWS帳戶使用AWS CLI。如需使用這個命令的詳細資訊，請參閱[attach-user-policy](#)中的AWS CLI命令參考。

現在您已將政策新增至 IAM 使用者，您已準備好啟動匯入程序。

請記住，當 IAM 使用者上傳物件至您指定的 Amazon S3 儲存貯體時，他們必須保留物件的預設許可設定，讓使用者可以讀取該物件。

將您的匯入檔案上傳到 Amazon S3

接著，您必須上傳 CSV 格式的匯入檔案至 Amazon S3，以便將其匯入。開始之前，您應該擁有 Amazon S3 儲存貯體，用於存放先前建立和/或選擇的匯入檔案。

Console S3 Upload

上傳您的匯入檔案至 Amazon S3

1. 登入 AWS Management Console，並開啟位於 <https://console.aws.amazon.com/s3/> 的 Amazon S3 主控台。
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 Upload (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 Upload (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. 前往匯入 Migration Hub 主控台中的頁面，如中所述[匯入資料](#)。然後，將物件 URL 貼到 Amazon S3 Object 網址欄位。

AWS CLI S3 Upload

上傳您的匯入檔案至 Amazon S3

1. 開啟終端機視窗，導覽到儲存匯入檔案的目錄。
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，您將需要用到此 URL。

匯入資料

從 Migration Hub 主控台之後填入下載匯入範本，並讓它與您現有的現場部署伺服器的資料，您就可以開始將資料放入 Migration Hub。下列指示說明兩種方式可以執行此步驟：透過使用主控台，或透過進行 API 呼叫。AWS CLI。

Console Import

啟動資料匯入工具[Migration Hub] 主控台的頁面。

開始匯入資料

1. 在導覽窗格中的 Discover (探索) 下，選擇 Tools (工具)。
2. 如果您還沒有填寫匯入範本，請選擇下載範本匯入範本中的匯入box (方塊) 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：https://s3.us-west-2.amazonaws.com/templates-7cfcf56-bd96-4b1c-b45b-a5b42f282e46/import_template.csv
3. 開啟匯入頁面中的匯入中的匯入box (方塊)
4. UNder匯入名稱，指定匯入的名稱。
5. 填寫Amazon S3 Object 網址欄位。為執行此步驟，您必須將匯入資料檔案上傳至 Amazon S3。如需詳細資訊，請參閱 [將您的匯入檔案上傳到 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。從這個畫面中，您也可以導覽至伺服器頁面下探索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。當您從匯入(匯入歷史) 頁面，方法是選取中列出的匯入名稱名稱欄中，系統會將您導向至伺服器根據所選匯入的資料集套用篩選的頁面。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 AWS CLI 開始資料匯入程序，必須先在您的環境中安裝 AWS CLI。如需詳細資訊，請參閱「[安裝AWSCommand Line Interface](#)」中的AWS Command Line Interface使用者指南。

Note

如果您還沒有填寫匯入範本，可以從 Amazon S3 儲存貯體下載匯入範本：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 Migration Hub 匯入要求

您可以使用主控台，追蹤 Migration Hub 匯入請求的狀態。AWS CLI，或AWS開發套件

Console Tracking

來自匯入 Migration Hub 主控台中的儀表板，您會發現下列元素。

- 名稱— 匯入請求的名稱。
- 匯入識別碼— 匯入請求的唯一 ID。
- 匯入時— 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。
 - 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匯入失敗。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— 未匯入資料檔案中的任何記錄。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量。
- 失敗的記錄— 特定資料檔案中未匯入的記錄數量。

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[排解匯入失敗記錄](#)。

檢視、匯出和探索探索到的資料

Application Discovery Service 無代理程式收集器 (無代理程式收集器) 和AWS探索代理程式 (探索代理程式) 會根據平均和尖峰使用率提供系統效能資料。您可以使用收集到的系統效能資料來執行高階總持有成本 (TCO)。探索代理程式會收集更詳細的資料，包括系統效能資訊的時間序列資料、輸入和輸出網路連線，以及伺服器上執行的處理程序。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，您將找到有關如何檢視和使用無代理程式收集器和探索代理程式從主控台和AWS CLI。

主題

- [使用 Migration Hub 主控台檢視收集的資料](#)
- [匯出收集資料](#)
- [Amazon Athena 中的資料探索](#)

使用 Migration Hub 主控台檢視收集的資料

對於應用程式探索服務無代理程式收集器 (無代理程式收集器) 和AWS探索代理程式 (探索代理程式)，在資料收集程序開始之後，您可以使用主控台來檢視其收集到的伺服器和虛擬機器相關資料。資料會在資料收集開始後約 15 分鐘出現在主控台中。您也可以透過使用進行 API 呼叫匯出收集的資料，以 CSV 格式檢視此資料AWS CLI。下一節[匯出收集資料](#)將說明如何匯出收集的資料。

若要檢視所收集的探索到的伺服器相關資料

1. 從主控台的導覽窗格中，選擇 Servers (伺服器)。探索到的伺服器會出現在伺服器清單中。
2. 如需所收集資料的詳細資訊，請選擇 Server info (伺服器資訊) 欄中的伺服器名稱連結。這麼做會顯示一個畫面，其中描述詳細資訊 (例如系統資訊，效能指標等等)。

若要深入了解如何使用主控台來檢視、排序和標記無代理程式收集器或探索代理程式所探索到的伺服器，請參閱[AWS Application Discovery Service 主控台逐步解說](#)。

無代理程式收集器資料庫和分析資料收集模組會將收集的資料上傳到 Amazon S3 儲存貯體。您可以在 AWS DMS 主控台中檢視此值區中的資料。

檢視有關探查到的資料庫和分析伺服器的收集資

1. 登入AWS Management Console並開啟AWS DMS 主控台，網址為 <https://console.aws.amazon.com/dms/v2/>。
2. 選擇 [探索] 下的 [庫存 [詳細目錄] 頁面隨即開啟，並顯示探查到的資料庫和分析伺服器清單

探索到的伺服器和應用程式的比對

AWS Application Discovery Service(Application Discovery Service) 具有內建的比對邏輯，可識別探索到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。

此比對邏輯可處理來自多個來源的重複伺服器，包括AWS Migration Hub (Migration Hub) 匯入、Application Discovery Service 無代理程式收集器 (無代理程式收集器)、AWS應用程式探索代理程式 (探索代理程式)，以及其他移轉工具。如需 Migration Hub 匯入的相關資訊，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，您只會找到伺服器的一個唯一項目。

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— 這是用來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中的值相同，則「Application Discovery Service」會比對這兩個項目，不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，「應用程式探索服務」才能執行比對。

匯出收集資料

對於 Application Discovery Service 無代理程式收集器 (無代理程式收集器) 和 AWS 應用程式探索代理程式 (探索代理程式)，在資料收集程序開始之後，您可以匯出其收集到的伺服器 and VM 相關資料。您可以透過與主控台互動或透過 API 呼叫來匯出此資料 AWS CLI，具體取決於您用來收集資料的探索工具。

展開您選擇的方法，即可取得兩種方式的說明：

使用匯出針對所有伺服器收集的資料 AWS CLI

您可以使用 () 大量匯出從主機和 VM 上執行的所有無代理程式收集器和探索代理程式收集的資料 AWS Command Line Interface AWS CLI。AWS CLI 必須先在您的環境中安裝，才能匯出資料。

若要安裝 AWS CLI 並匯出收集的資料

1. 如果您尚未這樣做，請安裝適用於您作業系統類型 (Windows 或 Mac/Linux) 的 AWS CLI。如需安裝指示，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 秘密存取金鑰。
 - 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. 輸入下列命令來產生匯出 ID：

```
aws discovery start-export-task
```

4. 使用先前步驟中產生的匯出 ID，輸入以下命令產生 S3 URL 做為參數 "configurationsDownloadUrl" 的值：

```
aws discovery describe-export-tasks --export-ids <export ID>
```

5. 複製上一步驟中產生的 URL 並貼到瀏覽器中，以下載包含所探索伺服器之收集資料的 zip 檔。

使用主控台匯出代理程式收集資料

當您在特定伺服器的詳細資料頁面上時，只能將從主控台匯出代理程式收集的資料僅限於一個代理程式。在詳細資訊頁面上，您可以在畫面底部的 [匯出] 下方找到伺服器的匯出工作。如果資料表為空白，則資料表為空白。您一次最多可以執行五次匯出伺服器資料。

若要匯出所收集的探索到的伺服器相關資料

1. 在導覽窗格中，選擇 Servers (伺服器)。
2. 在 Server info (伺服器資訊) 欄中，選擇您要匯出其資料的伺服器連結。
3. 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)。
4. 對於 Export server details (匯出伺服器詳細資訊)，填入 Start date (開始日期) 和 Time (時間)。

Note

開始時間不能超過目前時間的 72 小時前。

5. 選擇 Export (匯出)，啟動工作。初始狀態為 In-progress (進行中)；若要更新狀態，請按一下 Exports (匯出) 區段標題中的重新整理圖示。
6. 當匯出工作完成時，請選擇 Download (下載) 並儲存 .zip 檔。
7. 解壓縮儲存的檔案。一組 .csv 檔案包含匯出資料。

您可以在 Microsoft Excel 中開啟 .csv 檔案，並檢閱匯出的伺服器資料。

在這些檔案中，您會找到包含匯出工作相關資料及其結果的 JSON 檔案。

Note

如需在主控台中產生和匯出 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體建議的相關資 AWS Migration Hub 訊，請參閱 AWS Migration Hub 使用者指南中的 [Amazon EC2 執行個體建議](#)。

Amazon Athena 中的資料探索

Amazon Athena 的資料探索可讓您在單一位置分析探索代理程式從所有探索到的現場部署伺服器收集的資料。從遷移中樞主控台啟用 Amazon Athena 中的資料探索之後 (或使用 StartContinuousExport API) 並開啟代理程式的資料收集，代理程式收集的資料會定期自動存放在 S3 儲存貯體中。

然後，您可以造訪 Amazon Athena 執行預先定義的查詢，以分析每部伺服器的時間序列系統效能、每部伺服器上執行的處理程序類型，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，並將探索到的伺服器與實際的商務應用程式建立關聯。您還可以將 Athena 數據庫與亞馬遜集成 QuickSight 可視化查詢輸出並執行其他分析

步驟

1. [在 Amazon Athena 中啟用資料探索](#)
2. [在 Amazon Athena 使用資料探索](#)

在 Amazon Athena 中啟用資料探索

Amazon Athena 中的資料探索可透過使用遷移中樞主控台開啟連續匯出，或從 AWS CLI。您必須先開啟資料探索，才能在 Amazon Athena 查看並開始探索到的資料。

當您開啟連續匯出服務連結角

色 `AWSServiceRoleForApplicationDiscoveryServiceContinuousExport` 您的帳戶會自動使用。如需此服務連結角色的詳細資訊，請參閱 [Application Discovery 的服務連結角色許可](#)。

下列指示說明如何 Amazon Athena 用主控台和 AWS CLI。

Enable with the console

當您選擇「開始資料收集」或按一下標示為「Amazon Athena 中的資料探索」的切換按鈕時，會隱含開啟「連續匯出」啟用 Amazon Athena 中的資料探索功能資料收集器 [Migration Hub] 主控台的頁面。

從主控台啟用 Amazon Athena 的資料探索

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功能，請按一下 Amazon Athena 中的資料探索切換。
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「連續匯出」模式執行，可讓您在 Amazon Athena 查看並使用探索到的資料。第一次啟用此功能時，您的資料最多可能需要 30 分鐘才會顯示在 Amazon Athena 中。

Enable with the AWS CLI

Amazon Athena 中的資料探索是透過 API 呼叫明確啟用的連續匯出功能 AWS CLI。若要執行此操作，AWS CLI 必須先安裝在您的環境。

安裝 AWS CLI 並在 Amazon Athena 啟用資料探索

1. 安裝適用於您作業系統的 AWS CLI (Linux、macOS 或 Windows)。請參閱 [AWS Command Line Interface 使用者指南](#) 以取得說明。
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. 請輸入您的 AWS 存取金鑰 ID 和 AWS 秘密存取金鑰。
 - 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. 輸入以下命令：

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

Note

您的代理程式現在以「連續匯出」模式執行，可讓您在 Amazon Athena 查看並使用探索到的資料。第一次啟用此功能時，您的資料最多可能需要 30 分鐘才會顯示在 Amazon Athena 中。

在 Amazon Athena 使用資料探索

在 Amazon Athena 啟用資料探索之後，您可以直接在 Athena 中查詢資料，開始探索並使用代理程式所發現的詳細目前資料。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。

本節中的主題說明如何使用 Athena 中的資料，以評估和規劃將本機環境移轉至 AWS。

主題

- [在 Amazon Athena 中直接探索資料](#)
- [將 Amazon Athena 資料視覺化](#)
- [要在 Athena 使用的預先定義查詢](#)

在 Amazon Athena 中直接探索資料

下列指示會說明如何在 Athena 主控台中直接瀏覽您的代理資料。如果您在 Athena 中沒有任何資料，或者尚未在 Amazon Athena 啟用資料探索，系統會出現對話方塊提示您啟用 Amazon Athena 中的資料探索，如中所述在 [Amazon Athena 中啟用資料探索](#)。

直接在 Athena 探索代理程式探索的資料

1. 開啟 AWS Migration Hub 主控台，然後在導覽窗格中選擇 Servers (伺服器)。
2. 若要開啟 Amazon Athena 主控台，請選擇探索 Amazon Athena 中的資料。
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. 在 Athena 查詢編輯器中撰寫和執行 SQL 查詢，以查詢 Amazon Athena 主控台內的資料。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[要在 Athena 使用的預先定義查詢](#)。

將 Amazon Athena 資料視覺化

若要視覺化您的資料，可以將查詢移植到 Amazon 等視覺化程式 QuickSight 或其他開源可視化工具，例如 Cytoscape，YED 或格爾福。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至 Athena，以便它可以存取您收集的資料做為來源來產生視覺效果。

使用亞馬遜可視化您的 Amazon Athena 數據 QuickSight

1. 登入[亞馬遜 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。所以此新 Athena 資料來源將顯示對話方塊。
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. Select 一個 agents-servers-os 中的資料表選擇您的資料表對話方塊並選擇 Select。
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。

要在 Athena 使用的預先定義查詢

本節包含一組預先定義的查詢，此查詢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. 開啟 AWS Migration Hub 主控台，然後在導覽窗格中選擇 Servers (伺服器)。
2. 若要開啟 Amazon Athena 主控台，請選擇探索 Amazon Athena 中的資料。
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 位址和主機名稱

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。如需建立檢視的資訊，請參閱[建立檢視](#)在 Amazon 使用者指南。

```
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");
```

識別具有或不含代理程式的伺服器

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，追蹤伺服器之間的輸出通訊

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。如需建立檢視的資訊，請參閱 [建立檢視](#) 在 Amazon 使用者指南。

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. 建立 `valid_outbound_ips_helperview`，使用下列列出所有不同輸出目的地 IP 位址的說明器函式。

```
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

```

根據端口號和進程詳細信息跟踪服務器之間的輸入通信

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入流量。如需建立檢視的資訊，請參閱[建立檢視](#)在 Amazon 使用者指南。

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. 下載 IANA 連接埠登錄資料庫 CSV 檔案來源 [服務名稱與傳輸通訊協定連接埠號碼登錄](#) 上國際機構。
2. 將檔案上傳到 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 Athena 創建一個名為的新表 `iana_service_ports_import`。如需說明，請參閱 [建立資料表](#) 在 Amazon 使用者指南。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");
```

AWS Application Discovery Service 主控台逐步解說

AWS Application Discovery Service (Application Discovery Service) 與 AWS Migration Hub (遷移中樞) 和客戶可以在 Migration Hub 中檢視和管理其資料收集器、伺服器 and 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。

本節提供如何管理和監視 Application Discovery Service 無代理程式收集器 (無代理程式收集器) 和 AWS 使用主控台的應用程式探索代理程式 (探索代理程式)。

主題

- [主要儀表板](#)
- [資料收集](#)
- [檢視、匯出及瀏覽伺服器資料](#)

主要儀表板

若要檢視主儀表板，請選擇儀表板來自 AWS Migration Hub (Migration Hub) 主控台瀏覽窗格。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 無代理程式收集器 (無代理程式收集器) 和 AWS 應用程式探索代理程式 (探索代理程式)。

主要儀表板

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。

若要檢視主儀表板，請選擇儀表板從導覽窗格 (位於 Migration Hub 主控台首頁左側)。

資料收集

Application Discovery Service 無代理程式收集器 (無代理程式收集器) 和 AWS 應用程式探索代理程式 (探索代理程式) 是資料收集工具 AWS Application Discovery Service (Application Discovery Service) 用來協助您探索現有的基礎結構。下列主題說明如何下載並部署這些探索資料收集工具。[開始使用無代理程式收集器](#) 和 [AWS 應用程式探索代](#)。

這些資料收集工具會將其資料儲存在應用程式探索服務的儲存庫中，提供有關每部伺服器及其上執行之處理序的詳細資訊。部署這些工具之一時，您可以啟動、停止和檢視收集的資料AWS Migration Hub(Migration Hub) 主控台。

主題

- [啟動和停止資料收集器](#)
- [檢視和排序資料收集器](#)

啟動和停止資料收集器

之後AWS已部署應用程式探索代理程式 (探索代理程式)，您可以在資料收集器頁面AWS Migration Hub(Migration Hub) 主控台。

若要開始或停止資料收集工具

1. 使用您的AWS帳戶，登入AWS Management Console並在以下位置開啟 Migration Hub 主控台：<https://console.aws.amazon.com/migrationhub/>。
2. 在 [Migration Hub] 主控台瀏覽窗格的下方探索，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)。

檢視和排序資料收集器

如果您部署了許多資料收集器，您可以將已部署收集器的顯示清單排序資料收集器主控台的頁面。您可以在搜尋列中套用篩選來排序清單。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。

下表顯示可用於的搜尋條件代理程式，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)	==	從安裝收集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)	== !=	<p>已啟動：資料正在收集並傳送至 Application Discovery Service</p> <p>啟動排程：資料收集排定開始。資料將在下次偵測時傳送至 Application Discovery Service，狀態會變更為啟動。</p> <p>停止 (Stopped) 資料不會收集或傳送至 Application Discovery Service。</p> <p>停止排程：資料收集排定停止。資料將在下次 ping 時停止傳送至 Application Discovery Service，且狀態會變更為停止。</p>

搜尋條件	運算子	值：定義
運作狀態	<p>==</p> <p>!=</p>	<p>狀態良好 資料收集未開啟。此工具運作正常。</p> <p>運作狀態不佳：工具處於錯誤狀態。不會收集或報告資料。</p> <p>不明：一個多小時內沒有建立連接。</p> <p>關閉：由於系統，服務或守護進程關閉，該工具上次通信「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。</p> <p>執行：資料收集已開啟。此工具運作正常。</p>
IP 地址	<p>==</p> <p>!=</p>	<p>從已安裝收集工具之預先填入清單中選擇的任何 IP 地址。</p>

下表顯示可用於的搜尋條件無代理程式收集器，包括運算子、值和值的定義。

搜尋條件	運算子	值：定義
ID	<p>==</p>	<p>從安裝收集工具的預先填入清單中選取的任何無代理程式收集器 ID。</p>
Hostname (主機名稱)	<p>==</p> <p>!=</p>	<p>對於無代理程式收集器，從安裝無代理程式收集器之預先填入的主機清單中選取的任何主機名稱。</p>

搜尋條件	運算子	值：定義
狀態	==	收集資料：資料收集已開啟。 此工具運作正常。
	!=	準備好設定：未開啟資料收集功能。此工具運作正常。
		需要注意：工具處於錯誤狀態且需要注意。
		不明：一個多小時內沒有建立連接。
		關閉：由於系統，服務或守護進程關閉，該工具上次通信「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. 使用您的AWS帳戶，登入AWS Management Console並在以下位置開啟 Migration Hub 主控台：<https://console.aws.amazon.com/migrationhub/>。
2. 在 [Migration Hub] 主控台瀏覽窗格的下方探索，選擇資料收集器。
3. 選擇其中一個無代理程式收集器或者代理程式標籤。
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。

檢視、匯出及瀏覽伺服器資料

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。

主題

- [檢視和排序伺服器](#)
- [標記伺服器](#)
- [匯出伺服器資料](#)
- [Athena 中的資料探索](#)
- [應用程式](#)

檢視和排序伺服器

您可以檢視由資料收集工具探索而得的伺服器相關資訊，您也可以使用篩選條件來排序伺服器。

檢視伺服器

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. 使用您的AWS帳戶，登入AWS Management Console並在以下位置開啟 Migration Hub 主控台：<https://console.aws.amazon.com/migrationhub/>。
2. 在 [Migration Hub] 主控台瀏覽窗格的下方探索，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[匯出伺服器資料](#)。

使用搜尋篩選器排序伺服器

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. 使用您的AWS帳戶，登入AWS Management Console並在以下位置開啟 Migration Hub 主控台：<https://console.aws.amazon.com/migrationhub/>。
2. 在 [Migration Hub] 主控台瀏覽窗格的下方探索，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。

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。您可以在單一作業中標記個別伺服器或多部伺服器。AWS Application Discovery Service(Application Discovery Service) 標籤類似於AWS標籤，但這兩種類型的標籤不能互換使用。

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. 使用您的AWS帳戶，請登入AWS Management Console並在以下位置開啟 Migration Hub 主控台：<https://console.aws.amazon.com/migrationhub/>。
2. 在 [Migration Hub] 主控台瀏覽窗格的下方探索，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，於索引鍵欄位，以及 (選擇性) 中的值數值欄位。

通過選擇添加更多標籤新增標籤並添加更多信息。

6. 選擇 Save (儲存)。

若要從一或多個伺服器移除標籤

1. 使用您的AWS帳戶，請登入AWS Management Console並在以下位置開啟 Migration Hub 主控台：<https://console.aws.amazon.com/migrationhub/>。
2. 在 [Migration Hub] 主控台瀏覽窗格的下方探索，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。選取多部伺服器的核取方塊，以一次從多部伺服器移除標籤。
4. 選擇移除標籤。
5. 選取每個標籤。
6. 選擇 Confirm (確認)。

匯出伺服器資料

若要一次匯出一個伺服器的網路相依性和處理程序資訊，您可以使用伺服器的詳細資訊畫面。您可以在伺服器詳細資訊畫面中，Exports (匯出) 區段的一個表格中找到匯出工作。如果不存在任何匯出工作，表格會是空的。您可以同時匯出最多五個資料集合。

Note

只有在該伺服器上執行的代理程式所收集的資料，才能從主控台匯出伺服器資料。如果您要大量匯出已安裝代理程式的所有伺服器的資料，請參閱[Amazon Athena 中的資料探索](#)。

若要匯出詳細的伺服器資料

1. 使用您的AWS帳戶，請登入AWS Management Console並在以下位置開啟 Migration Hub 主控台：<https://console.aws.amazon.com/migrationhub/>。
2. 在 [Migration Hub] 主控台瀏覽窗格的下方探索，選擇伺服器。
3. 在 Server info (伺服器資訊) 欄中，選擇您要匯出資料之伺服器的 ID。
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)。
5. 對於 Export server details (匯出伺服器詳細資訊)，填入 Start date (開始日期) 和 Time (時間)。

Note

開始時間不能超過目前時間的 72 小時前。

6. 選擇 Export (匯出)，啟動工作。初始狀態為 In-progress (進行中)；若要更新狀態，請按一下 Exports (匯出) 區段標題中的重新整理圖示。
7. 當匯出工作完成時，請選擇 Download (下載) 並儲存 .zip 檔。
8. 解壓縮儲存的檔案。一組 .csv 檔案包含匯出資料，類似如下：
 - <AWS## ID_destinationProcessConnection.csv
 - <AWS## ID_networkInterface.csv
 - <AWS## ID_osInfo.csv
 - <AWS## ID_process.csv
 - <AWS## ID_sourceProcessConnection.csv
 - <AWS## ID_systemPerformance.csv

您可以在 Microsoft Excel 中開啟 .csv 檔案，並檢閱匯出的伺服器資料。

在這些檔案中，您會找到包含匯出工作相關資料及其結果的 JSON 檔案。

Athena 中的資料探索

Amazon Athena 的資料探索可讓您在單一位置分析探索代理程式從所有探索到的現場部署伺服器收集的資料。從遷移中樞主控台啟用 Amazon Athena 中的資料探索之後 (或使用 StartContinuousExport API) 並開啟代理程式的資料收集，代理程式收集的資料會定期自動存放在 S3 儲存貯體中。如需詳細資訊，請參閱 [Amazon Athena 中的資料探索](#)。

應用程式

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. 使用您的AWS帳戶，登入AWS Management Console並在以下位置開啟 Migration Hub 主控台：<https://console.aws.amazon.com/migrationhub/>。
2. 在 [Migration Hub] 主控台瀏覽窗格的下方探索，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，請選擇新增標籤，輸入一個值索引鍵，然後選擇性地輸入值數值。
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)。

使用應用程式探索服務 API 查詢探索到的組態項目

設定項目是由代理程式在您的資料中心探索的 IT 資產。使用 AWS Application Discovery Service (應用程式探索服務) 時，您可以使用 API 來指定篩選器，並查詢伺服器、應用程式、處理序和連線資產的特定組態項目。如需 API 的資訊，請參閱 [Application Discovery Service API 參考](#)。

下列各節中的表格列出兩個「應用 Application Discovery Service」動作的可用輸入篩選器和輸出排序選項：

- 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。

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。如需指令語法的詳細資訊，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.hasMoreValues	

欄位	強制性
<code>server.configurationId</code>	x
<code>server.cpuType</code>	
<code>server.hostName</code>	
<code>server.hypervisor</code>	
<code>server.networkInterfaceInfo</code>	
<code>server.networkInterfaceInfo.hasMoreValues</code>	
<code>server.osName</code>	
<code>server.osVersion</code>	
<code>server.tags</code>	
<code>server.tags.hasMoreValues</code>	
<code>server.timeOfCreation</code>	x
<code>server.type</code>	
<code>server.performance.avgCpuUsagePct</code>	
<code>server.performance.avgDiskReadIOPS</code>	
<code>server.performance.avgDiskReadsPerSecondInKB</code>	
<code>server.performance.avgDiskWriteIOPS</code>	
<code>server.performance.avgDiskWritesPerSecondInKB</code>	

欄位	強制性
<code>server.performance.avgFreeRAMInKB</code>	
<code>server.performance.avgNetworkReadsPerSecondInKB</code>	
<code>server.performance.avgNetworkWritesPerSecondInKB</code>	
<code>server.performance.maxCpuUsagePct</code>	
<code>server.performance.maxDiskReadIOPS</code>	
<code>server.performance.maxDiskReadsPerSecondInKB</code>	
<code>server.performance.maxDiskWriteIOPS</code>	
<code>server.performance.maxDiskWritesPerSecondInKB</code>	
<code>server.performance.maxNetworkReadsPerSecondInKB</code>	
<code>server.performance.maxNetworkWritesPerSecondInKB</code>	
<code>server.performance.minFreeRAMInKB</code>	
<code>server.performance.numCores</code>	
<code>server.performance.numCpus</code>	
<code>server.performance.numDisks</code>	

欄位	強制性
<code>server.performance.numNetworkCards</code>	
<code>server.performance.totalRAMInKB</code>	

程序資產

欄位	強制性
<code>process.commandLine</code>	
<code>process.configurationId</code>	x
<code>process.name</code>	
<code>process.path</code>	
<code>process.timeOfCreation</code>	x

應用程式資產

欄位	強制性
<code>application.configurationId</code>	x
<code>application.description</code>	
<code>application.lastModifiedTime</code>	x
<code>application.name</code>	x
<code>application.serverCount</code>	x
<code>application.timeOfCreation</code>	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。如需指令語法的詳細資訊，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	

欄位	強制性
<code>process.timeOfCreation</code>	X
<code>server.agentId</code>	
<code>server.configurationId</code>	X

應用程式資產

欄位	強制性
<code>application.configurationId</code>	X
<code>application.description</code>	
<code>application.name</code>	X
<code>application.serverCount</code>	X
<code>application.timeOfCreation</code>	X
<code>application.lastModifiedTime</code>	X

連線資產

欄位	強制性
<code>connection.destinationIp</code>	X
<code>connection.destinationPort</code>	X
<code>connection.ipVersion</code>	X
<code>connection.latestTimestamp</code>	X
<code>connection.occurrence</code>	X
<code>connection.sourceIp</code>	X

欄位	強制性
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	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE 	<ul style="list-style-type: none"> 任何有效的伺服器組態 ID 	無
server.hostName	<ul style="list-style-type: none"> EQUALS NOT_EQUALS 	<ul style="list-style-type: none"> 字串 	<ul style="list-style-type: none"> ASC DESC

篩選條件	支援的條件	支援的值	支援的排序
	<ul style="list-style-type: none"> • EQ • NE • CONTAINS • NOT_CONTAINS 		
<code>server.osName</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • 字串 	<ul style="list-style-type: none"> • ASC • DESC
<code>server.osVersion</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • 字串 	<ul style="list-style-type: none"> • ASC • DESC
<code>server.agentId</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE 	<ul style="list-style-type: none"> • 字串 	無
<code>server.connectorId</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE 	<ul style="list-style-type: none"> • 字串 	無

篩選條件	支援的條件	支援的值	支援的排序
server.type	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE 	具有下列其中一個值的字串： <ul style="list-style-type: none"> • EC2 • OTHER • VMWARE_VM • VMWARE_HOST • VMWARE_VM_TEMPLATE 	無
server.vmWareInfo.morefId	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • 字串 	無
server.vmWareInfo.vcenterId	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • 字串 	無
server.vmWareInfo.hostId	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • 字串 	無

篩選條件	支援的條件	支援的值	支援的排序
server.networkInterfaceInfo.portGroupId	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE CONTAINS NOT_CONTAINS 	<ul style="list-style-type: none"> 字串 	無
server.networkInterfaceInfo.portGroupName	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE CONTAINS NOT_CONTAINS 	<ul style="list-style-type: none"> 字串 	無
server.networkInterfaceInfo.virtualSwitchName	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE CONTAINS NOT_CONTAINS 	<ul style="list-style-type: none"> 字串 	無
server.networkInterfaceInfo.ipAddress	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE CONTAINS NOT_CONTAINS 	<ul style="list-style-type: none"> 字串 	無

篩選條件	支援的條件	支援的值	支援的排序
server.networkInterfaceInfo.macAddress	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE CONTAINS NOT_CONTAINS 	<ul style="list-style-type: none"> 字串 	無
server.performance.avgCpuUsagePct	<ul style="list-style-type: none"> GE LE GT LT 	<ul style="list-style-type: none"> 百分比 	無
server.performance.totalDiskFreeSizeInKB	<ul style="list-style-type: none"> GE LE GT LT 	<ul style="list-style-type: none"> Double 	無
server.performance.avgFreeRAMInKB	<ul style="list-style-type: none"> GE LE GT LT 	<ul style="list-style-type: none"> Double 	無
server.tag.value	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE CONTAINS NOT_CONTAINS 	<ul style="list-style-type: none"> 字串 	無

篩選條件	支援的條件	支援的值	支援的排序
<code>server.tag.key</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE CONTAINS NOT_CONTAINS 	<ul style="list-style-type: none"> 字串 	無
<code>server.application.name</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE CONTAINS NOT_CONTAINS 	<ul style="list-style-type: none"> 字串 	無
<code>server.application.description</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE CONTAINS NOT_CONTAINS 	<ul style="list-style-type: none"> 字串 	無
<code>server.application.configurationId</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE 	<ul style="list-style-type: none"> 任何有效的應用程式組態 ID 	無
<code>server.process.configurationId</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE 	<ul style="list-style-type: none"> ProcessId 	無

篩選條件	支援的條件	支援的值	支援的排序
<code>server.process.name</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE CONTAINS NOT_CONTAINS 	<ul style="list-style-type: none"> 字串 	無
<code>server.process.commandLine</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE CONTAINS NOT_CONTAINS 	<ul style="list-style-type: none"> 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
<code>application.configurationId</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE 	<ul style="list-style-type: none"> ApplicationId 	無
<code>application.name</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE CONTAINS NOT_CONTAINS 	<ul style="list-style-type: none"> 字串 	<ul style="list-style-type: none"> ASC DESC

篩選條件	支援的條件	支援的值	支援的排序
<code>application.description</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE CONTAINS NOT_CONTAINS 	<ul style="list-style-type: none"> 字串 	<ul style="list-style-type: none"> ASC DESC
<code>application.serverCount</code>	不支援篩選。	不支援篩選。	<ul style="list-style-type: none"> ASC DESC
<code>application.timeOfCreation</code>	不支援篩選。	不支援篩選。	<ul style="list-style-type: none"> ASC DESC
<code>application.lastModifiedTime</code>	不支援篩選。	不支援篩選。	<ul style="list-style-type: none"> ASC DESC
<code>server.configurationId</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE 	<ul style="list-style-type: none"> ServerId 	無

程序資產

篩選條件	支援的條件	支援的值	支援的排序
<code>process.configurationId</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS 	<ul style="list-style-type: none"> ProcessId 	

篩選條件	支援的條件	支援的值	支援的排序
	<ul style="list-style-type: none"> • EQ • NE 		
<code>process.name</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • 字串 	<ul style="list-style-type: none"> • ASC • DESC
<code>process.commandLine</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • 字串 	<ul style="list-style-type: none"> • ASC • DESC
<code>server.configurationId</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE 	<ul style="list-style-type: none"> • ServerId 	
<code>server.hostName</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • 字串 	<ul style="list-style-type: none"> • ASC • DESC

篩選條件	支援的條件	支援的值	支援的排序
<code>server.osName</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • 字串 	<ul style="list-style-type: none"> • ASC • DESC
<code>server.osVersion</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • 字串 	<ul style="list-style-type: none"> • ASC • DESC
<code>server.agentId</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • 字串 	

連線資產

篩選條件	支援的條件	支援的值	支援的排序
<code>connection.sourceIp</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS 	<ul style="list-style-type: none"> • IP 	<ul style="list-style-type: none"> • ASC • DESC

篩選條件	支援的條件	支援的值	支援的排序
	<ul style="list-style-type: none"> • NOT_CONTAINS 		
connection.destinationIp	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • IP 	<ul style="list-style-type: none"> • ASC • DESC
connection.destinationPort	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE 	<ul style="list-style-type: none"> • 整數 	<ul style="list-style-type: none"> • ASC • DESC
sourceServer.configurationId	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE 	<ul style="list-style-type: none"> • ServerId 	
sourceServer.hostName	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • 字串 	<ul style="list-style-type: none"> • ASC • DESC
destinationServer.osName	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • 字串 	<ul style="list-style-type: none"> • ASC • DESC

篩選條件	支援的條件	支援的值	支援的排序
destinationServer.osVersion	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • 字串 	<ul style="list-style-type: none"> • ASC • DESC
destinationServer.agentId	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • 字串 	
sourceProcess.configurationId	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE 	<ul style="list-style-type: none"> • ProcessId 	
sourceProcess.name	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • 字串 	<ul style="list-style-type: none"> • ASC • DESC

篩選條件	支援的條件	支援的值	支援的排序
sourceProcess.commandLine	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • 字串 	<ul style="list-style-type: none"> • ASC • DESC
destinationProcess.configurationId	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE 	<ul style="list-style-type: none"> • ProcessId 	
destinationProcess.name	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • 字串 	<ul style="list-style-type: none"> • ASC • DESC
destinationprocess.commandLine	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • 字串 	<ul style="list-style-type: none"> • ASC • DESC

AWS Application Discovery Service 中的安全性

雲端安全是 AWS 最重視的一環。身為 AWS 的客戶，您將能從資料中心和網路架構中獲益，這些都是專為最重視安全的組織而設計的。

安全是 AWS 與您共同的責任。[共同的責任模型](#) 將此描述為雲端本身的安全和雲端內部的安全：

- 雲端本身的安全：AWS 負責保護在 AWS Cloud 中執行 AWS 服務的基礎設施。AWS 也提供您可安全使用的服務。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。
- 雲端內部的安全：您的責任取決於所使用的 AWS 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 應用程式探索代理程式或 Application Discovery Service 無代理程式收集器，您必須提供帳戶的 AWS 存取金鑰。然後，此資訊會儲存在您的本機基礎結構中。作為共同責任模式的一部分，您有責任保護對基礎結構的存取。

本文件將協助您瞭解如何在使用應用程式探索服務時套用共同的責任模型。下列主題說明如何設定 Application Discovery Service，以符合您的安全性與合規性目標。您也將學習如何使用其他 AWS 可協助您監視和保護應用程式探索服務資源的服務。

主題

- [的 Identity and Access Management AWS Application Discovery Service](#)
- [AWS Application Discovery Service 中的記錄和監控](#)

的 Identity and Access Management AWS Application Discovery Service

AWS Identity and Access Management (IAM) 可協助系統管理員安全地控制 AWS 資源存取權。AWS 服務 IAM 管理員控制哪些人可以驗證 (登入) 和授權 (具有權限) 以使用應用程式探索服務資源。IAM 是您可以使用的 AWS 服務，無需額外付費。

主題

- [物件](#)
- [使用身分來驗證](#)
- [使用政策管理存取權](#)

- [如何與 IAM AWS Application Discovery Service 搭配使用](#)
- [AWS 受管理的政策 AWS Application Discovery Service](#)
- [AWS Application Discovery Service 以身分為基礎的原則範例](#)
- [使用 Application Discovery 的服務連結角色](#)
- [疑難排解 AWS Application Discovery Service 身分與存取](#)

物件

您使用 AWS Identity and Access Management (IAM) 的方式會有所不同，視您在 Application Discovery Service 中所做的工作而定。

服務使用者 — 如果您使用 Application Discovery Service 務來執行工作，則管理員會為您提供所需的認證和權限。當您使用更多 Application Discovery Service 功能來完成工作時，您可能需要其他權限。瞭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[疑難排解 AWS Application Discovery Service 身分與存取](#)。

服務管理員 — 如果您負責公司的 Application Discovery Service 資源，您可能擁有 Application Discovery Service 的完整存取權。決定您的服務使用者應存取哪些應用程式探索服務功能和資源是您的工作。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。若要深入瞭解貴公司如何搭配應用程式探索服務使用 IAM，請參閱[如何與 IAM AWS Application Discovery Service 搭配使用](#)。

IAM 管理員 — 如果您是 IAM 管理員，您可能想要瞭解如何撰寫政策以管理 Application Discovery Service 存取權的詳細資訊。若要檢視可在 IAM 中使用的應用程式探索服務身分型政策範例，請參閱[AWS Application Discovery Service 以身分為基礎的原則範例](#)

使用身分來驗證

驗證是您 AWS 使用身分認證登入的方式。您必須以 IAM 使用者身分或假設 IAM 角色進行驗證 (登入 AWS)。AWS 帳戶根使用者

您可以使用透過 AWS 身分識別來源提供的認證，以聯合身分識別身分登入。AWS IAM Identity Center (IAM 身分中心) 使用者、貴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識別的範例。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 AWS 用同盟存取時，您會間接擔任角色。

根據您的使用者類型，您可以登入 AWS Management Console 或 AWS 存取入口網站。如需有關登入的詳細資訊 AWS，請參閱《AWS 登入 使用指南》AWS 帳戶中的[如何登入](#)您的。

如果您 AWS 以程式設計方式存取，請 AWS 提供軟體開發套件 (SDK) 和命令列介面 (CLI)，以使用您的認證以加密方式簽署要求。如果您不使用 AWS 工具，則必須自行簽署要求。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[簽署 AWS API 請求](#)。

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) 來增加帳戶的安全性。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[在 AWS 中使用多重要素驗證 \(MFA\)](#)。

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，該身分可完整存取該帳戶中的所有資源 AWS 服務和資源。此身分稱為 AWS 帳戶 root 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作業。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](#)是您內部的身分，具 AWS 帳戶 有單一人員或應用程式的特定許可。建議您盡可能依賴暫時憑證，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。如需詳細資訊，請參閱《IAM 使用者指南》<https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#rotate-credentials>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。您無法以群組身分登入。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過程變得更為容易。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，但角色僅提供暫時憑證。如需進一步了解，請參閱《IAM 使用者指南》中的[建立 IAM 使用者 \(而非角色\) 的時機](#)。

IAM 角色

[IAM 角色](#)是您 AWS 帳戶 內部具有特定許可的身分。它類似 IAM 使用者，但不與特定的人員相關聯。您可以[切換角色，在中暫時擔任 IAM 角色](#)。AWS Management Console 您可以透過呼叫 AWS CLI 或 AWS API 作業或使用自訂 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[使用 IAM 角色](#)。

使用暫時憑證的 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，並取得由角色定義的許可。如需有關聯合角色的詳細資訊，請參閱《IAM 使用者指南》https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_create_for-idp.html中的為第三方身分供應商建立角色。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 (信任的委託人) 存取您帳戶中的資源。角色是授予跨帳戶存取權的主要方式。但是，對於某些策略 AWS 服務，您可以將策略直接附加到資源 (而不是使用角色作為代理)。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 角色與資源類型政策的差異](#)。
- 跨服務訪問 — 有些 AWS 服務 使用其他 AWS 服務功能。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。
- 轉寄存取工作階段 (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。當您使用某些服務時，您可能會執行一個動作，而該動作之後會在不同的服務中啟動另一個動作。FAS 會使用主體呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。只有當服務收到需要與其 AWS 服務 他資源互動才能完成的請求時，才會發出 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給 AWS 服務 服務](#)。
- 服務連結角色 — 服務連結角色是連結至 AWS 服務 服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中，AWS 帳戶 且屬於服務所有。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 執行個體上執行的應用程式以及發出 AWS CLI 或 AWS API 請求的臨時登入資料。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 執行個體並提供給其所有應用程式，請建立連接至執行個體的執行個體設定檔。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暫時憑證。如需詳細資訊，請參閱《IAM 使用者指南》中的[利用 IAM 角色來授予許可給 Amazon EC2 執行個體上執行的應用程式](#)。

如需了解是否要使用 IAM 角色或 IAM 使用者，請參閱《IAM 使用者指南》中的[建立 IAM 角色 \(而非使用者\) 的時機](#)。

使用政策管理存取權

您可以透過 AWS 過建立原則並將其附加至 AWS 身分識別或資源來控制中的存取。原則是一個物件 AWS，當與身分識別或資源相關聯時，會定義其權限。AWS 當主參與者 (使用者、root 使用者或角色工作階段) 提出要求時，評估這些原則。政策中的許可決定是否允許或拒絕請求。大多數原則會 AWS 以 JSON 文件的形式儲存在中。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哪些內容。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。若要授與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。具有該原則的使用者可以從 AWS Management Console AWS CLI、或 AWS API 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。若要了解如何建立身分類型政策，請參閱《IAM 使用者指南》中的[建立 IAM 政策](#)。

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。受管理的策略是獨立策略，您可以將其附加到您的 AWS 帳戶。受管政策包括 AWS 受管政策和客戶管理的策略。如需瞭解如何在受管政策及內嵌政策間選擇，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。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](#)。主參與者可以包括帳戶、使用者、角色、同盟使用者或。AWS 服務

資源型政策是位於該服務中的內嵌政策。您無法在以資源為基礎的政策中使用 IAM 的 AWS 受管政策。

存取控制清單 (ACL)

存取控制清單 (ACL) 可控制哪些委託人 (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 和 Amazon VPC 是支援 ACL 的服務範例。AWS WAF 若要進一步了解 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原則類型。這些政策類型可設定較常見政策類型授與您的最大許可。

- 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。如需許可範圍的更多相關資訊，請參閱《IAM 使用者指南》中的[IAM 實體許可範圍](#)。
- 服務控制策略 (SCP) — SCP 是 JSON 策略，用於指定中組織或組織單位 (OU) 的最大權限。AWS Organizations 是一種用於分組和集中管理您企業擁有的多個 AWS 帳戶的服務。若您啟用組織中的所有功能，您可以將服務控制策略 (SCP) 套用到任何或所有帳戶。SCP 限制成員帳戶中實體的權限，包括每個 AWS 帳戶根使用者帳戶。如需組織和 SCP 的更多相關資訊，請參閱《AWS Organizations 使用者指南》中的[SCP 運作方式](#)。
- 工作階段政策 – 工作階段政策是一種進階政策，您可以在透過編寫程式的方式建立角色或聯合使用者的暫時工作階段時，作為參數傳遞。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。如需更多資訊，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。要了解如何在涉及多個政策類型時 AWS 確定是否允許請求，請參閱《IAM 使用者指南》中的[政策評估邏輯](#)。

如何與 IAM AWS Application Discovery Service 搭配使用

在您使用 IAM 管理應用 Application Discovery Service 的存取權限之前，您應該瞭解哪些 IAM 功能可與應用 Application Discovery Service 搭配使用。若要取得應用程式探索服務和其他 AWS 服務如何與 IAM 搭配運作的高階檢視，請參閱 IAM 使用者指南中的與 IAM [搭配使用的AWS 服務](#)。

主題

- [Application Discovery Service 身分型原則](#)
- [Application Discovery Service 資源型原則](#)
- [根據 Application Discovery Service 號的授權](#)
- [Application Discovery Service IAM 角色](#)

Application Discovery Service 身分型原則

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哪些內容。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。原則動作通常與關聯的 AWS API 作業具有相同的名稱。有一些例外狀況，例如沒有相符的 API 操作的僅限許可動作。也有一些操作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與執行相關聯操作的許可。

應用 Application Discovery Service 中的原則動作會在動作之前使用下列前置詞：discovery:政策陳述式必須包含 Action 或 NotAction 元素。Application Discovery Service 會定義它自己的一組動作，說明您可以使用此服務執行的工作。

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*"
```

若要查看應用程式探索服務動作清單，請參閱 [IAM 使用者指南 AWS Application Discovery Service 中的定義動作](#)。

資源

Application Discovery Service 不支援在策略中指定資源 ARN。

條件金鑰

Application Discovery Service 不提供任何服務特定的條件金鑰，但它確實支援使用某些全域條件金鑰。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 身分型原則的範例，請參閱 [AWS Application Discovery Service 以身分為基礎的原則範例](#)

Application Discovery Service 資源型原則

Application Discovery Service 不支援以資源為基礎的原則。

根據 Application Discovery Service 號的授權

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

Application Discovery Service IAM 角色

[IAM 角色](#)是您 AWS 帳戶中具有特定許可的實體。

將臨時登入資料搭配 Application Discovery Service

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 連結角色的詳細資訊，請參閱[使用 Application Discovery 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 受管理的政策 AWS Application Discovery Service

若要新增使用者、群組和角色的權限，使用 AWS 受管理的原則比自己撰寫原則更容易。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 AWS 受管政策的詳細資訊，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 受管理的策略。您無法變更 AWS 受管理原則中的權限。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 受管理的政策移除權限，因此政策更新不會破壞您現有的權限。

此外，還 AWS 支援跨多個服務之工作職能的受管理原則。例如，ReadOnlyAccess AWS 受管理的策略提供對所有 AWS 服務和資源的唯讀存取權。當服務啟動新功能時，會為新作業和資源新 AWS 增唯讀權限。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 受管理的策略：AWSApplicationDiscoveryServiceFullAccess

此AWSApplicationDiscoveryServiceFullAccess政策授予 IAM 使用者帳戶存取應用 Application Discovery Service 和 Migration Hub API。

附加此政策的 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，以及查詢 Disco AWS very Service 資料庫中的資料。如需此政策的範例，請參閱 [授與 Application Discovery Service 的完整存取](#)。

AWS 受管理的策略：AWSApplicationDiscoveryAgentlessCollectorAccess

AWSApplicationDiscoveryAgentlessCollectorAccess 受管理的原則會授與 Application Discovery Service 無代理程式收集器 (無代理程式收集器) 存取權，以便註冊並與 Application Discovery Service 通訊，以及與其他服務通訊。AWS

此政策必須附加至 IAM 使用者，其登入資料用於設定無代理程式收集器。

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 程式註冊。這對於能夠將收集的數據發送回來是必要的 AWS。
- `ecr-public`— 允許收集器撥打電話給 Amazon 彈性容器註冊表公共 (Amazon ECR 公共)，其中找到了收集器的最新更新。
- `mgh`— 允許收集器呼叫 AWS Migration Hub 以擷取用於配置收集器之帳戶的主區域。這對於知道收集的數據應發送到哪個區域是必要的。
- `sts`— 允許收集器擷取服務承載權杖，以便收集器可以撥打電話給 Amazon ECR Public 以取得最新更新。

```
{
  "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 受管理的策略：AWSApplicationDiscoveryAgentAccess

此AWSApplicationDiscoveryAgentAccess原則會授與應用程式探索代理程式的存取權，以便註冊並與 Application Discovery Service

您可以將此原則附加至應用程式探索代理程式使用其認證的任何使用者。

此政策也會授予使用者 Arsenal 的存取許可。阿森納是由管理和託管的代理服務 AWS。阿仙奴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 [授與探索代理程式存取權](#)。

AWS 受管理的策略：AWSAgentlessDiscoveryService

此AWSAgentlessDiscoveryService原則會授與在 VMware vCenter Server 中執行的 AWS 無代理程式探查連接器存取權，以便向應用程式探索服務註冊、通訊和共用連接器健康情況指標。

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：ApplicationDiscoveryServiceContinuousExportServiceRole策略

如果您的 IAM 帳戶已附加AWSApplicationDiscoveryServiceFullAccess政策，ApplicationDiscoveryServiceContinuousExportServiceRolePolicy則當您在 Amazon Athena 開啟資料探索時，系統會自動將其附加到您的帳戶。

此政策 AWS Application Discovery Service 允許建立 Amazon 資料 Firehose 串流，以將 AWS Application Discovery Service 代理程式收集的資料轉換並交付到您 AWS 帳戶中的 Amazon S3 儲存貯體。

此外，此原則還會建立一個 AWS Glue Data Catalog 名為 application_discovery_service_Database 的新資料庫和資料表結構描述，以對應代理程式所收集的資料。如需此政策的範例，請參閱 [授與代理程式資料收集的權限](#)。

AWS 受管理的策略：AWSDiscoveryContinuousExportFirehosePolicy

必須有AWSDiscoveryContinuousExportFirehosePolicy政策才能在 Amazon Athena 使用資料探索。它可讓 Amazon 資料 Firehose 將從 Application Discovery Service 收集到的資料寫入 Amazon S3。如需有關使用此政策的資訊，請參閱 [建立角 AWSApplicationDiscoveryServiceFirehose 色](#)。如需此政策的範例，請參閱 [授與資料探索的權限](#)。

建立角 AWSApplicationDiscoveryServiceFirehose 色

管理員會將受管政策附加到您的 IAM 使用者帳戶。使用AWSDiscoveryContinuousExportFirehosePolicy原則時，系統管理員必須先建立以 Firehose 命名AWSApplicationDiscoveryServiceFirehose為信任實體的角色，然後將AWSDiscoveryContinuousExportFirehosePolicy原則附加至該角色，如下列程序所示。

若要建立 AWSApplicationDiscoveryServiceFirehoseIAM 角色

1. 在 IAM 主控台中，選擇導覽窗格上的 [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 Next: Permissions (下一步：許可)。
6. 在「篩選策略」下搜尋AWSDiscoveryContinuousExportFirehosePolicy。
7. 選取旁邊的核取方塊 AWSDiscoveryContinuousExportFirehosePolicy，然後選擇 [下一步：檢閱]。

8. 輸入AWSApplicationDiscoveryServiceFirehose作為角色名稱，然後選擇 [建立角色]。

AWS 受管政策的 Application Discovery Service 更新

檢視有關 Application Discovery Service AWS 受管理原則更新的詳細資料，因為此服務開始追蹤這些變更。如需有關此頁面變更的自動提醒，請訂閱 [AWS Application Discovery Service 的文件歷史記錄](#) 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新原則	Application Discovery Service 新增了新的受管理原則AWSApplicationDiscoveryAgentlessCollectorAccess，授與無代理程式收集器存取權，以便註冊並與 Application Discovery Service 通訊，以及與其他 AWS 服務通訊。	2022 年 8 月 16 日
Application Discovery Service 已開始追蹤	Application Discovery Service 開始追蹤其 AWS 受管理原則的變更。	2021 年 3 月 1 日

AWS Application Discovery Service 以身分為基礎的原則範例

依預設，IAM 使用者和角色沒有建立或修改應用程式探索服務資源的權限。他們也無法使用 AWS Management Console AWS CLI、或 AWS API 執行工作。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 操作的所需許可。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](#)
- [授與 Application Discovery Service 的完整存取](#)
- [授與探索代理程式存取權](#)
- [授與代理程式資料收集的權限](#)
- [授與資料探索的權限](#)
- [授與使用 Migration Hub 主控台網路圖表的權限](#)

政策最佳實務

以身分識別為基礎的原則會決定某人是否可以建立、存取或刪除您帳戶中的 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 受管原則並邁向最低權限權限 — 若要開始授與使用者和工作負載的權限，請使用可授與許多常見使用案例權限的 AWS 受管理原則。它們可用在您的 AWS 帳戶。建議您透過定義特定於您使用案例的 AWS 客戶管理政策，進一步降低使用權限。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](#)。
- 套用最低許可許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的權限。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。您也可以使用條件來授與對服務動作的存取權 (如透過特定) 使用這些動作 AWS 服務，例如 AWS CloudFormation。如需更多資訊，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，可協助您編寫安全且實用的政策。如需更多資訊，請參閱 IAM 使用者指南中的 [IAM Access Analyzer 政策驗證](#)。
- 需要多因素身份驗證 (MFA) — 如果您的案例需要 IAM 使用者或根使用者 AWS 帳戶，請開啟 MFA 以獲得額外的安全性。如需在呼叫 API 操作時請求 MFA，請將 MFA 條件新增至您的政策。如需更多資訊，請參閱 [IAM 使用者指南](#) 中的設定 MFA 保護的 API 存取。

有關 IAM 中最佳實務的更多相關資訊，請參閱 IAM 使用者指南中的 [IAM 最佳安全實務](#)。

授與 Application Discovery Service 的完整存取

受 `AWSApplicationDiscoveryServiceFullAccess` 管政策授予 IAM 使用者帳戶存取應用 Application Discovery Service 和 Migration Hub API。

將此政策附加至其帳戶的 IAM 使用者可以設定 Application Discovery Service、啟動和停止代理程式、啟動和停止無代理程式探索，以及查詢 Disco AWS very Service 資料庫中的資料。如需此政策的詳細資訊，請參閱 [AWS 受管理的政策 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": "*"
    }
  ]
}
```

授與探索代理程式存取權

`AWSApplicationDiscoveryAgentAccess` 受管理的原則會授與應用程式探索代理程式存取權，以便註冊並與 Application Discovery Service 如需此政策的詳細資訊，請參閱 [AWS 受管理的政策 AWS Application Discovery Service](#)。

將此原則附加至「應用程式探索代理程式」使用其認證的任何使用者。

此政策也會授予使用者 Arsenal 的存取許可。阿森納是由管理和託管的代理服務 AWS。阿仙奴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": "*"
    }
  ]
}
```

授與代理程式資料收集的權限

ApplicationDiscoveryServiceContinuousExportServiceRole政策受管政策 AWS Application Discovery Service 允許建立 Amazon Data Firehose 串流，以將應用程式探索服務代理程式收集的資料轉換並傳遞到 AWS 帳戶中的 Amazon S3 儲存貯體。

此外，此原則還會建立「AWS Glue 資料目錄」，其中包含名為的新資料庫 `application_discovery_service_database` 和資料表結構描述，以對應代理程式所收集的資料。

如需有關使用此政策的資訊，請參閱 [AWS 受管理的政策 AWS Application Discovery Service](#)。

Example ApplicationDiscoveryServiceContinuousExportServiceRole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"
      }
    }
  }
]
}

```

授與資料探索的權限

必須有 `AWSDiscoveryContinuousExportFirehosePolicy` 政策才能在 Amazon Athena 使用資料探索。它可讓 Amazon 資料 Firehose 將從 Application Discovery Service 收集到的資料寫入 Amazon S3。如需有關使用此政策的資訊，請參閱 [建立角 AWSApplicationDiscoveryServiceFirehose 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:*"
    ]
  }
]
}

```

授與使用 Migration Hub 主控台網路圖表的權限

若要在建立允許或拒絕存取 Application Discovery Service 或 Migration Hub 的身分識別型原則時授與 AWS Migration Hub 主控台網路圖的存取權，您可能需要將 `discovery:GetNetworkConnectionGraph` 動作新增至原則。

您必須在新策略中使用該 `discovery:GetNetworkConnectionGraph` 動作，或更新較舊的策略，如果策略的下列情況均成立：

- 此原則允許或拒絕存取應用程式探索服務或 Migration Hub。
- 原則會使用一個更特定的探索動作 (例如，`discovery:action-name` 而非) 來授與存取權限 `discovery:*`。

下列範例顯示如何在 IAM 政策中使用 `discovery:GetNetworkConnectionGraph` 動作。

Example

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

如需 Migration Hub 網路圖表的相關資訊，請參閱[在 Migration Hub 中檢視網路連線](#)。

使用 Application Discovery 的服務連結角色

AWS Application Discovery Service 使用 AWS Identity and Access Management (IAM) [服務連結的角色](#)。服務連結角色是直接連結至 Application Discovery 的一種特殊 IAM 角色類型。服務連結角色由 Application Discovery 預先定義，並包含該服務呼叫其他所需的所有許可AWS代表您的服務。

服務連結角色可讓設定 Application Discovery 更為簡單，因為您不必手動新增必要的許可。Application Discovery 定義其服務連結角色的許可，除非另有定義，否則只有 ApApplication 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，並且該許可政策不能連接到任何其他 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。如此可保護您的 ApApplication Discovery Service 資源，避免您不小心移除資源的存取許可。

主題

- [Application Discovery 的服務連結角色許可](#)
- [為 Application Discovery 建立服務連結角色](#)
- [刪除 Application Discovery 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 Yes (是)，以檢視該服務的服務連結角色文件。

Application Discovery 的服務連結角色許可

Application Discovery 使用名為的服務連結角色 `AWSServiceRoleForApplicationDiscoveryServiceContinuousExport`— 允許訪問AWS使用或管理的服務和資源AWS Application Discovery Service。

所以此 `AWSServiceRoleForApplicationDiscoveryServiceContinuousExport` 服務連結角色信任下列服務擔任角色：

- `continuousexport.discovery.amazonaws.com`

此角色許可政策允許 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`

logs

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 建立服務連結角色

您不需要手動建立一個服務連結角色。所以此

`AWSServiceRoleForApplicationDiscoveryServiceContinuousExport` 當您隱含開啟連續匯出時，會自動建立服務連結角色：a) 在您選擇「開始資料收集器」之後，確認資料收集器頁面中顯示的對話方塊中的選項，或按一下標示為「Athena 中的資料探索」的滑桿，或 b) 當您呼叫 `StartContinuousExport` API 使用 `AWSCLI`。

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. 切換 Athena 中的資料探索滑桿至「開啟」(On) 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

您可以使用 Application Discovery Service 命令，AWS Command Line Interface若有建立 AWSServiceRoleForApplicationDiscoveryServiceContinuousExport服務連結角色。

當您啟動「連續匯出」時，會自動建立此服務連結角色AWS CLI(該AWS CLI必須先安裝在您的環境中)。

若有建立服務連結角色 (CLI)，請從AWS CLI

1. 安裝適用於您作業系統的 AWS CLI (Linux、macOS 或 Windows)。請參閱[AWS Command Line Interface使用者指南](#)如需說明。
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. 請輸入您的AWS存取金鑰 ID 和AWS秘密存取金鑰。
 - 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. 輸入以下命令：

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

您也可以使用 IAM 主控台透過建立一個服務連結角色探索服務-連續匯出使用案例。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 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。

清除該服務連結角色

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 ApApplication Discovery Service 在您試圖刪除資源時正在使用該角色，刪除動作可能會失敗。若此情況發生，請等待數分鐘後並再次嘗試操作。

若 Application Discovery Service 刪除由

AWSServiceRoleForApplicationDiscoveryServiceContinuousExport 從 Migration Hub 主控台中的服務連結角色

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. 切換 Athena 中的資料探索滑桿至「關閉」位置。

若 Application Discovery Service 刪除由

AWSServiceRoleForApplicationDiscoveryServiceContinuousExport 來自的服務連結角色 AWS CLI

1. 安裝適用於您作業系統的 AWS CLI (Linux、macOS 或 Windows)。請參閱 [AWS Command Line Interface 使用者指南](#) 如需說明。
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. 請輸入您的 AWS 存取金鑰 ID 和 AWS 秘密存取金鑰。
 - 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. 輸入以下命令：

```
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. 輸入下列指令，以確保連續匯出已停止，方法是確認傳回狀態為「非作用中」：

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

手動刪除服務連結角色

您可以刪除 `AWSServiceRoleForApplicationDiscoveryServiceContinuousExport` 使用 IAM 主控台、IAM CLI 或 IAM API。如果您不再需要使用需要此服務連結角色的探索服務-連續匯出功能，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 [清除該服務連結角色](#)。

疑難排解 AWS Application Discovery Service 身分與存取

使用下列資訊可協助您診斷並修正使用 Application Discovery Service 和 IAM 時可能會遇到的常見問題。

主題

- [我沒有授權執行 iam : PassRole](#)

我沒有授權執行 iam : PassRole

如果您收到未獲授權執行 `iam:PassRole` 動作的錯誤訊息，則必須更新您的原則，以允許您將角色傳遞給 Application Discovery Service。

有些 AWS 服務 允許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 使用者 `marymajor` 嘗試使用主控台在應用 Application Discovery Service 中執行動作時，就會發生下列範例錯誤。但是，該動作要求服務具備服務角色授與的許可。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 系統管理員。您的管理員提供您的登入憑證。

AWS Application Discovery Service 中的記錄和監控

AWS Application Discovery Service 已與 AWS CloudTrail 整合。您可以使用 CloudTrail 記錄、持續監控和保留帳戶活動以進行故障排除和審核。CloudTrail 提供了 AWS 帳戶活動，包括通過 AWS 管理主控台、AWS 軟體開發套件和命令列工具。本節中的主題說明如何將使用 CloudTrail 使用 Application Discovery Service。

主題

- [使用記錄 Application Discovery Service API 呼叫 AWS CloudTrail](#)

使用記錄 Application Discovery Service API 呼叫 AWS CloudTrail

AWS Application Discovery Service 整合 AWS CloudTrail，提供使用者、角色或角色所採取之動作的服務 AWS Application Discovery Service 中的服務。CloudTrail 擷取 Application Discovery Service 的 API 呼叫當作事件。擷取的呼叫包括來自 Application Discovery Service 的呼叫，以及對 Application Discovery Service API 作業進行的程式碼呼叫。

如果您建立追蹤，就可以啟用持續交付 CloudTrail Amazon S3 儲存貯體的事件，包括 Application Discovery Service 的事件。如果您不設定追蹤記錄，仍然可以檢視最新的事件 CloudTrail 主控台事件歷史。使用所收集的資訊 CloudTrail，您就可以判斷傳送至 Application Discovery Service 的請求、提出請求的對象、提出請求的對象、提出請求的對象、提出請求的時間，以及其他詳細資訊。

進一步了解 CloudTrail，請參閱 [AWS CloudTrail 使用者指南](#)。

Application Discovery Service CloudTrail

CloudTrail 已在您的 AWS 當您建立帳戶時的帳戶。Application Discovery Service 中發生活動時，該活動會記錄在 CloudTrail 與其他一起事件 AWS 服務事件事件歷史。您可以檢視、搜尋和下載 AWS 帳戶的最新事件。如需詳細資訊，請參閱《》[檢視事件 CloudTrail 事件歷史](#)。

如需您的正在進行事件的記錄 AWS 帳戶 (包含 Application Discovery Service 的事件) 會建立線索。一個線索啟用 CloudTrail 將日誌檔案傳送至 Amazon S3 儲存貯體。根據預設，當您在主控台建立線索時，線索會套用到所有 AWS 區域。該追蹤會記錄來自 AWS 分割區中所有區域的事件，並將日誌檔案交付到您指定的 Amazon S3 儲存貯體。此外，您可以設定其他 AWS 服務，以進一步分析和處理收集的事件資料 CloudTrail 日誌。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](#)
- [設定的 Amazon SNS 通知 CloudTrail](#)
- [接收 CloudTrail 來自多個區域的日誌檔案](#)和[接收 CloudTrail 來自多個帳戶的日誌檔案](#)

會記錄所有 Application Discovery Service 動作 CloudTrail 並記錄在[Application Discovery Service API 參考](#)。例如，呼叫CreateTags、DescribeTags，以及GetDiscoverySummary動作會產生項目 CloudTrail 日誌檔案。

每一筆事件或日誌項目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：

- 該請求是否透過根或 AWS Identity and Access Management (IAM) 使用者憑證來提出。
- 提出該要求時，是否使用了特定角色或聯合身分使用者的暫時安全憑證。
- 該請求是否由另一項 AWS 服務提出。

如需詳細資訊，請參閱 [CloudTrail 使用者身分元素](#)。

瞭解 Application Discovery Service 記錄檔項目

追蹤是一種組態，能讓事件以日誌檔案的形式交付至您指定的 Amazon S3 儲存貯體。CloudTrail 記錄檔案包含一個或多個日誌項目。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 日誌檔案並非依公有 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 CloudTrail 示範的記錄項目DescribeTags動作。

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAJBHC4H6EKEXAMPLE: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 配額

Service Quotas 主控台提供了有關 AWS Application Discovery Service 配額的資訊。您可以使用 Service Quotas 主控台來檢視預設服務配額，或者[請求提高配額](#)以獲得可調整的配額。

目前，唯一可以增加的配額是匯入的服務器每個帳號。

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，而且想要匯入新的應用程式，您可以利用DeleteApplicationsAPI 動作。如需詳細資訊，請參閱「[DeleteApplications](#)」中的Application Discovery Service API 參考。

- 每個匯入檔案的最大檔案大小為 10 MB。
- 每個帳號 25,000 筆匯入的伺服器記錄。
- 每天 25,000 筆刪除匯入記錄。
- 每個帳戶 10,000 個導入的服務器（您可以請求增加此配額）。
- 1,000 個活動代理程式，它們收集資料並將資料傳送至 Application Discovery Service。
- 10,000 個停用的代理程式，回應但不收集資料的代理程式。
- 每個應用程式 400 個伺服器。
- 每台服務器 30 個標籤。

疑難排 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

- [透過資料探索停止資料收集](#)
- [移除資料探索所收集的資料](#)
- [修正 Amazon Athena 資料探索的常見問題](#)
- [排解匯入失敗記錄](#)

透過資料探索停止資料收集

若要停止資料探索，您可以在 Migration Hub 主控台的 [探索] > [資料收集器] > [代理程式] 索引標籤下，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 叫用會將資料探索狀態顯示為「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「數據探索」仍然顯示錯誤並且無法成功停止，請聯繫 AWS 支持。

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：刪除資料探索的 Amazon Kinesis Data Streams

如果您想繼續由 ADS 資料儲存庫中的代理程式收集資料，但不想使用資料探索收集 Amazon S3 儲存貯體中的資料，您可以手動刪除資料探索所建立的 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「資料 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`

移除資料探索所收集的資料

若要移除資料探索所收集的資料

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-discovery-service-uniqueid`。

Note

啟用 Amazon Athena 中的資料探索時，刪除 Amazon S3 儲存貯體或其中的任何物件會導致錯誤。它會繼續將新的探索代理程式資料傳送至 S3。已刪除的資料也將無法在 Athena 存取。

2. 移除 AWS Glue Data Catalog。

開啟 Amazon Athena 中的資料探索時，它會在您的帳戶中建立一個 Amazon S3 儲存貯體，以固定時間間隔存放 ADS 代理程式收集的資料。此外，它還創建了一個 AWS Glue Data Catalog 允許您從亞馬遜 Amazon Athena 查詢存儲在 Amazon S3 存儲桶中的數據。當您在 Amazon Athena

關閉資料探索時，Amazon S3 儲存貯體中不會存放新資料，但先前收集的資料仍會持續存放。如果您不再需要這些資料，而且想要在開啟 Amazon Athena 的資料探索之前將帳戶返回該州。

- a. 從 AWS 主控台造訪 Amazon S3，並手動刪除名為「aws-application-discover-discovery-服務唯一 ID」的儲存貯體
- b. 您可以刪除資料庫和所有下列表格，以手動移除資料 application-discovery-service-database 料探索 AWS Glue 資料目錄：
 - os_info_agent
 - network_interface_agent
 - sys_performance_agent
 - processes_agent
 - inbound_connection_agent
 - outbound_connection_agent
 - id_mapping_agent

從中移除您的資料 AWS Application Discovery Service

要從 Application Discovery Service 中刪除所有數據，請聯繫 Sup [AWS port](#) 並要求完全刪除數據。

修正 Amazon Athena 資料探索的常見問題

在本節中，您可以找到有關如何在 Amazon Athena 修正資料探索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的 AWS 資源](#)
- [新的代理程式資料不會顯示在 Amazon Athena](#)
- [您沒有足夠的權限可以訪問 Amazon S3，Amazon 數據 Firehose 件，或 AWS Glue](#)

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的 AWS 資源

當您在 Amazon Athena 開啟資料探索時，它會在您的帳戶中建立服務連結角色 `AWSRoleForApplicationDiscoveryServiceContinuousExport`，以建立必要的 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 建立此角色的資料探索權限，將無法初始化。請參閱 [AWS 受管理的政策 AWS Application Discovery Service](#)。

新的代理程式資料不會顯示在 Amazon Athena

如果新資料未流入 Athena，則代理程式啟動後已超過 30 分鐘，且資料探索狀態為作用中，請查看下列解決方案：

- AWS 探索代理

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 狀況

請確定下列 Firehose 傳送串流正常運作：

- `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

請確定資料 `application-discovery-service-database` 資料庫位於中 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

確保您的帳戶中有一個名為 `aws-application-discovery-service-uniqueid` 的 Amazon S3 儲存貯體。如果值區中的物件已移動或刪除，它們將無法正確顯示在 Athena 中。

- 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。

您沒有足夠的權限可以訪問 Amazon S3，Amazon 數據 Firehose 件，或 AWS Glue

如果您正在使用 AWS Organizations，並且在 Amazon Athena 進行資料探索的初始化失敗，可能是因為您沒有存取 Amazon S3、Amazon 資料 Firehose、Athena 或 AWS Glue。

您需要具有管理員許可的 IAM 使用者，才能授與您存取這些服務。管理員可以使用其帳戶來授予此存取權限。請參閱 [AWS 受管理的政策 AWS Application Discovery Service](#)。

為確保 Amazon Athena 中的資料探索能正常運作，請勿修改或刪除 Amazon Athena 中的資料探索所建立的 AWS 資源，包括 Amazon S3 儲存貯體、Amazon 資料 Firehose 串流和 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。如果刪除資料探索所建立的 Amazon S3 儲存貯體，可能會遺失儲存貯體中收集的資料。

排解匯入失敗記錄

Migration Hub 匯入可讓您將內部部署環境的詳細資料直接匯入 Migration Hub，而無需使用探索連接器或探索代理程式。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：

- 已達到與匯入相關的配額 — 有與匯入任務相關聯的配額。如果您發出的匯入工作要求會超過配額，則要求將失敗並傳回錯誤。如需詳細資訊，請參閱 [AWS Application Discovery Service 配額](#)。
- 在匯入檔案中插入了一個額外的逗號 (,) — 使用 .CSV 檔案中的逗號來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模式錯誤。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。
- 欄位的值超出其支援範圍 — 某些欄位 (例如 `CPU.NumberOfCores` 必須具有它們所支援的值範圍)。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，然後開啟 Migration Hub 主控台，位於 <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` — 這個檔案是您的錯誤記錄，它會追蹤每個失敗項目之每個失敗記錄的行ExternalId、欄名稱和描述性錯誤訊息。
- `failed-entries-file.csv` — 此檔案僅包含原始匯入檔案中失敗的項目。

若要更正您遇到的 `non-limit-based` 錯誤，請使用 `errors-file.csv` 來更正 `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](#)。

AWS Application Discovery Service 的文件歷史記錄

最新的使用者指南文件更新：2023 年 5 月 16 日

下表說明 2019 年 1 月之後 Application Discovery Service 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
介紹無代理程式收集器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應用程式探索服務無代理程式收集器 (無代理程式收集器) 的新模組。您可以使用此資料收集模組連線至您的環境，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
引入 Application Discovery Service 無代理程式收集	Application Discovery Service 無代理程式收集器 (無代理程式收集器) 是新的AWS Application Discovery Service內部部署應用程式，可透過無代理程式方法收集有關內部部署環境的資訊，以協助您有效地規劃移轉至 AWS 雲端。如需詳細資訊，請參閱 無代理程式收集器 。	2022 年 8 月 16 日
IAM 更新	建立身分型政策時，現在可使用 AWS Identity and Access Management (IAM) <code>discovery:GetNetworkConnectionGraph</code> 動作來授與AWS Migration Hub主控台網路圖的存取權。如需詳	2022 年 5 月 24 日

細資訊，請參閱[授與使用網狀圖](#)的權限。

[介紹家鄉地區](#)

Migration Hub 本地區域為您的整個產品組合提供單一的探索和移轉規劃資訊儲存庫，以及移轉至多個區AWS域的單一檢視。

2019 年 11 月 20 日

[介紹遷移中心匯入功能](#)

Migration Hub 匯入可讓您將內部部署伺服器 and 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 discovery Service](#)

2019 年 1 月 18 日

下表說明 2019 年 1 月 18 日之前的 Application Discovery Service 使用者指南的文件發行版本：

變更	描述	日期
新功能	更新文件以支援 Amazon Athena 中的資料探索，並新增了疑難排解章節。	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
主控台	已新增 AWS Management Console。	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

變更	描述	日期
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	此為 Application Discovery Service	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](#)。

附錄

本節包含有關的補充資訊 AWS Application Discovery Service。

主題

- [附錄：從探索連接器轉換至無代理程式收集器](#)
- [附錄：AWS 無代理程式探查連接器](#)

附錄：從探索連接器轉換至無代理程式收集器

本節說明如何從 AWS 無代理程式探索連接器 (探索連接器) 轉換至 Application Discovery Service 無代理程式收集器 (無代理程式收集器)。

我們建議目前使用探索連接器轉換至新的無代理程式收集器的客戶。

若要瞭解如何開始使用無代理程式收集器，請參閱 [開始使用無代理程式收集器](#)

部署無代理程式收集器之後，您可以刪除探索連接器虛擬機器。先前收集的所有資料將繼續在 AWS Migration Hub (Migration Hub) 中提供。

附錄：AWS 無代理程式探查連接器

Important

我們建議目前使用探索連接器轉換至新的無代理程式收集器的客戶。如需詳細資訊，請參閱 [附錄：從探索連接器轉換至無代理程式收集器](#)。

主題

- [探索連接器所收集的資料](#)
- [探索連接器資料收集](#)
- [疑難排解探查連接器](#)

探索連接器所收集的資料

探索連接器會收集 VMware vCenter 伺服器主機和虛擬機器的相關資訊。不過，必須安裝 VMware vCenter Server 工具，才能擷取此資料。若要確定您使用的 AWS 帳戶具有此工作所需的權限，請參閱 [AWS 受管理的政策 AWS Application Discovery Service](#)。

接下來，您可以找到探索連接器所收集之資訊的清單。

探索連接器收集資料的表格圖例：

- 收集的資料是以千位元組 (KB) 為單位 (除非另有指明)。
- Migration Hub 主控台對等的資料會以 MB 為單位報告。
- 以星號 (*) 表示的資料欄位只能在從連接器的 API 匯出功能產生的 .csv 檔案中使用。
- 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
avgCpuUsage百分比	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	Application Discovery Service 指派給探查到的虛擬機器

資料欄位	描述
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 ID
hostName	執行虛擬化軟體的主機名稱
hypervisor	Hypervisor 的類型
id	伺服器的 ID
lastModifiedTime 郵票*	資料匯出之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
maxCpuUsage 百分比	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

資料欄位	描述
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
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 指派給探查到的虛擬機器
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 檢視和排序資料收集器)。
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

資料欄位	描述
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

探索連接器資料收集

在 VMware 環境中部署並設定探索連接器之後，如果資料收集停止，您可以重新啟動它。您可以透過主控台開始或停止資料收集，或透過 AWS CLI。下列程序會描述這兩種方法。

Using the Migration Hub Console

下列程序顯示如何在 Migration Hub 主控台的 [資料收集器] 頁面上啟動或停止探索連接器資料收集程序。

若要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

若要從啟動探索連接器資料收集程序 AWS CLI，AWS CLI 必須先在您的環境中安裝，然後您必須將 CLI 設定為使用選取的 [Migration Hub 本位目錄區域](#)。

若要安裝 AWS CLI 並開始資料收集

1. 安裝 AWS CLI 適用於您的作業系統 (Linux、macOS 或視窗)。如需指示，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 秘密存取金鑰。
 - c. 在「預設區域名稱」中輸入您的首頁「區域」。例如 `us-west-2`。
 - d. 輸入預設輸出格式的 `text`。
3. 若要尋找您要啟動或停止資料收集的連接器識別碼，請輸入下列命令以查看連接器的識別碼：

```
aws discovery describe-agents --filters  
condition=EQUALS,name=hostName,values=connector
```

4. 若要透過連接器開始資料收集，請鍵入下列命令：

```
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。

若要停止連接器收集資料，請輸入下列命令：

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

疑難排解探查連接器

本節包含的主題可協助您疑難排解 Application Discovery Service 連接器的已知問題。

修復探索連接器 AWS 在安裝期間無法達

在主控台中設定 AWS 無代理程式探索連接器時，您可能會收到下列錯誤訊息：

無法到達 AWS

AWS 無法到達 (連線重設)。請確認網路和代理伺服器設定。

發生此錯誤的原因是探索連接器嘗試建立 HTTPS 連線至連接器需要在安裝程序期間進行通訊的 AWS 網域失敗。如果無法建立連線，探查連接器組態就會失敗。

若要修正連線 AWS

1. 請洽詢您的 IT 管理員，瞭解貴公司的防火牆是否封鎖連接埠 443 上的輸出流量，傳送至任何需要輸出存取的 AWS 網域。

下列 AWS 網域需要輸出存取：

- `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了輸出流量，請將其解除封鎖。更新防火牆之後，請重新設定連接器。

2. 如果更新防火牆無法解決連線問題，請檢查以確定連接器虛擬機器具有對列出網域的輸出網路連線。如果虛擬機器具有輸出連線，請在連接埠 443 上執行 telnet，測試與列出網域的連線，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輸出連線，您必須連絡 Sup [AWS port](#) 部門以進一步疑難排解。

固定不健康的連接器

您可以在 Migration Hub 主控台的 [[資料收集器](#)] 頁面中找到每個探索連接器的 Health 全狀況資訊。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. 在網頁瀏覽器中開啟 Migration Hub 主控台，然後從左側導覽中選擇 [資料收集器]。
2. 從 [連接器] 索引標籤中，記下每個健全狀況狀態為「不良」之連接器的 IP 位址。
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` 是狀態不良的連接器的 IP 位址。
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。您可以在此處選擇 vCenter 連線的檢視資訊，然後您會看到一個包含診斷訊息的對話方塊。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 Sup [AWS port](#) 部門。

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 位址問題](#)
- [認證問題](#)

IP 位址問題

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 vCenter 連線的檢視資訊時，會出現一個對話方塊，其中顯示「確認 vCenter 伺服器的作業狀態，或選擇編輯設定以更新 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. 使用單獨的命令列工具 (例如 ping 或 traceroute)，驗證關聯的 vCenter 伺服器處於作用中狀態，並且可從連接器虛擬機器存取 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。

認證問題

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 vCenter 連線的檢視資訊時，您會看到一個對話方塊，其中顯示「選擇編輯設定，以使用讀取和檢視權限更新帳戶的 vCenter 使用者名稱和密碼」訊息。

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。

獨立式 ESX 主機支援

探索連接器不支援獨立 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

如果您遇到問題並需要協助，請聯絡 Sup [AWS port](#) 部門。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 無代理程式探索連接器主控台，然後選擇 [下載記錄檔服務包]。
- 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。