aws

使用者指南

Migration Hub 策略建議

Migration Hub 策略建議: 使用者指南

Table of Contents

什麼是 Migration Hub 策略建議？

Migration Hub 策略建議可針對應用程式的可行轉換路徑提供移轉和現代化策略建議，協助您規劃移轉和現代化計劃。

策略建議可以分析您的伺服器清查、執行階段環境，以及 Microsoft IIS 和 Java Tomcat 和 Jboss 應用程式的應用程式二進位檔，以產生反模式報告。此外，您可以設定原始程式碼，讓策略建議執行所有應用程式的原始程式碼和資料庫分析。策略建議會比較此分析與您的業務目標，以及您提供給建議之應用程式和資料庫的轉換偏好設定：

- 為您的每個應用程式提供最有效的移轉策略。
- 您可以使用的移轉和現代化工具或服務。
- 針對特定選項解決的應用程式不相容性和反模式。

Migration Hub 策略建議針對相關聯的部署目的地、工具和程式進行重新裝載、重新架構和重構建議建議的移轉和現代化策略。如需有關重新主控、重新平台和重構的資訊，請參閱規定指引詞彙表中的遷移術語-7 Rs。AWS

策略建議可能會建議簡單的選項，例如使用AWS應用程式遷移服務 (AWSMGN) 在 Amazon 彈性運算雲端 (Amazon EC2) 上重新託管。更優化的建議可能包括使用 AWS App2Container 對容器進行重新平台化，或重構為開放原始碼技術，例如 .NET 核心和 PostgreSQL。

您是第一次使用策略建議的客戶嗎？

如果這是您第一次使用策略建議，建議您先閱讀下列章節：

- 策略建議概述
- 設定策略建議
- 開始使用策略建議

策略建議概述

您可以從AWS Migration Hub主控台使用 Migration Hub 策略建議，為您的伺服器和應用程式產品組合開始評估。您可以使用主控台來設定和執行評估。評估完成後，您可以使用主控台來檢視每個伺服器和應用程式的評估資料，以及建議的轉換工具。

若要接收重構建議和不相容性清單，您可以使用策略建議來評估您的應用程式原始程式碼和資料庫。

您也可以在 Microsoft Excel 檔案中下載建議資料。

相關服務

- AWS Migration Hub— 您可以使用AWS Migration Hub主控台存取 Migration Hub 策略建議主控台。它也會顯示您要從中收集資料之伺服器的相關資訊。
- AWS Application Discovery Service— 在使用策略建議之前，您可以使用 Application Discovery Service 在AWS Migration Hub主控台中收集伺服器和應用程式的相關資料。
- AWS應用程式遷移服務 — AWS 應用程式移轉服務是建議移轉至的 lift-and-shift 主要移轉服務 AWS。
- AWS Database Migration Service— 這AWS Database Migration Service是一種 Web 服務，可用於將資料從現場部署的資料庫、Amazon Relational Database Service (Amazon RDS) 資料庫執行個體或 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的資料庫遷移到AWS服務上的資料庫。
- AWS應用程序容器-AWS 應用程序容器（A2C）是一個命令行工具，用於將 .NET 和 Java 應用程序現代化為容器化應用程序。
- .NET 移植助理 — 用於 .NET 原始程式碼分析。移植助手為 .NET 是一個兼容性掃描儀，減少移植 Microsoft .NET 框架應用程序到 .NET 核心所需的手動工作。.NET 的移植助理員會評估 .NET 應用程式原始程式碼，並識別不相容的 API 和協力廠商套件。
- Windows 伺服器 Support 援終止移轉計畫 — 適用於 Windows 伺服器的終止 Support 援移轉計畫 (EMP) 包含工具，可將舊版應用程式從 Windows 伺服器 2003、2008 年和 2008 R2 遷移至較新、受支援的版本，而無需進行任何重構。AWS
- AWSSchema Conversion Tool — 您可以使用 AWS Schema Conversion Tool (AWS SCT) 將現有的數據庫模式從一個數據庫引擎轉換為另一個數據庫引擎。
- Windows Web 應用程式移轉小幫手 — 的 Windows Web 應用程式移轉輔助程式AWS Elastic Beanstalk是一種互動式 PowerShell 公用程式，可將 ASP.NET 和 ASP.NET 核心應用程式從內部部署的 IIS 視窗伺服器移轉至 Elastic Beanstalk。
- 適用於 Aurora PostgreSQL 的巴貝魚 — 適用於 Aurora Postgre SQL 的巴貝魚是 Amazon Aurora PostgreSQL 相容版本的新功能，可讓 Aurora 瞭解針對 Microsoft SQL 伺服器編寫的應用程式的命令。

設定策略建議

第一次使用 Migration Hub 策略建議之前，請先完成下列工作：

主題

註冊一個 AWS 帳戶

如果您沒有 AWS 帳戶，請完成以下步驟來建立一個。

若要註冊成為 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。

   當您註冊一個時 AWS 帳戶，將創建AWS 帳戶根使用者一個。根使用者有權存取該帳戶中的所有 AWS 服務 和資源。安全性最佳做法是將管理存取權指派給使用者，並僅使用 root 使用者來執行需要 root 使用者存取權的工作。

AWS 註冊過程完成後，會向您發送確認電子郵件。您可以隨時登錄 https://aws.amazon.com/ 並選擇我的帳戶，以檢視您目前的帳戶活動並管理帳戶。

建立具有管理權限的使用者

註冊後，請保護 AWS 帳戶 AWS 帳戶根使用者、啟用和建立系統管理使用者 AWS IAM Identity Center，這樣您就不會將 root 使用者用於日常工作。

保護您的 AWS 帳戶根使用者

1. 選擇 Root 使用者並輸入您的 AWS 帳戶 電子郵件地址，以帳戶擁有者身分登入。AWS Management Console在下一頁中，輸入您的密碼。

如需使用根使用者登入的說明，請參閱 AWS 登入 使用者指南中的以根使用者身分登入。

2. 若要在您的根使用者帳戶上啟用多重要素驗證 (MFA)。

   如需指示，請參閱《IAM 使用者指南》中的為 AWS 帳戶 根使用者啟用虛擬 MFA 裝置 (主控台)。

建立具有管理權限的使用者

1. 啟用 IAM Identity Center。

   如需指示，請參閱 AWS IAM Identity Center 使用者指南中的啟用 AWS IAM Identity Center。

2. 在 IAM 身分中心中，將管理存取權授予使用者。

   若要取得有關使用 IAM Identity Center 目錄 做為身分識別來源的自學課程，請參閱《使用指南》IAM Identity Center 目錄中的「以預設值設定使用AWS IAM Identity Center 者存取」。

以具有管理權限的使用者身分登入

- 若要使用您的 IAM Identity Center 使用者簽署，請使用建立 IAM Identity Center 使用者時傳送至您電子郵件地址的簽署 URL。

  如需使用 IAM 身分中心使用者登入的說明，請參閱使用AWS 登入 者指南中的登入 AWS 存取入口網站。

指派存取權給其他使用者

1. 在 IAM 身分中心中，建立遵循套用最低權限許可的最佳做法的權限集。

   如需指示，請參閱《AWS IAM Identity Center 使用指南》中的「建立權限集」。

2. 將使用者指派給群組，然後將單一登入存取權指派給群組。

   如需指示，請參閱《AWS IAM Identity Center 使用指南》中的「新增群組」。

策略建議使用者和角色

我們建議您為「策略建議」建立兩個角色：

- 若要存取主控台，請建立同時附加AWSMigrationHubFullAccess和受AWSMigrationHubStrategyConsoleFullAccess管理策略的角色。
- 若要存取策略建議應用程式資料收集器，請建立附加受AWSMigrationHubStrategyCollector管理原則的角色。

IAM 受管政策會定義使用者對服務的存取層級。受 AWS Migration Hub AWSMigrationHubFullAccess管理的原則會授與 Migration Hub 主控台的存取權。如需詳細資訊，請參閱 Migration Hub 角色和原則。如需有關AWSMigrationHubStrategyConsoleFullAccess和受AWSMigrationHubStrategyCollector管理策略的資訊，請參閱AWS Migration Hub 策略建議的受管原則。

若要提供存取權，請新增權限至您的使用者、群組或角色：

- 使用者和群組位於 AWS IAM Identity Center：

  建立權限合集。請按照 AWS IAM Identity Center 使用者指南 中的 建立權限合集 說明進行操作。
- 透過身分提供者在 IAM 中管理的使用者：

  建立聯合身分的角色。請按照 IAM 使用者指南 的 為第三方身分提供者 (聯合) 建立角色 中的指示進行操作。
- IAM 使用者：
  - 建立您的使用者可擔任的角色。請按照 IAM 使用者指南 的 為 IAM 使用者建立角色 中的指示進行操作。
  - (不建議) 將政策直接附加至使用者，或將使用者新增至使用者群組。請遵循 IAM 使用者指南的新增許可到使用者 (主控台)中的指示。

開始使用策略建議

本節說明如何開始使用 Migration Hub 策略建議。

主題

策略建議的先決條件

以下是使用 Migration Hub 策略建議的先決條件。

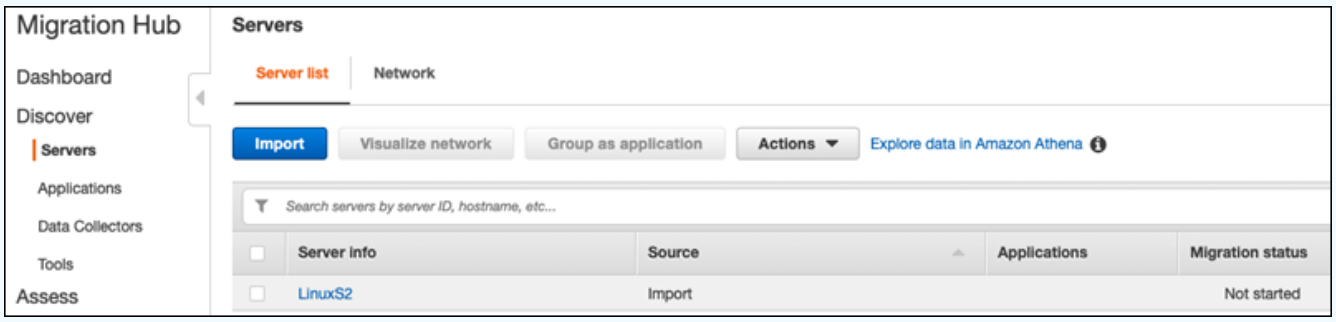
- 您必須擁有一個或多個 AWS 帳戶，並為這些帳戶設定了使用者。如需詳細資訊，請參閱 設定策略建議。
- 策略建議應用程式資料收集器用戶端必須能夠從伺服器遠端收集資料。這需要您使用一組適用於所有 Windows 伺服器的認證，以及一組適用於所有 Linux 伺服器的認證。認證必須具有建立和刪除伺服器中目錄的權限。
- 部署在 vCenter 中的收集器版本支援 VMware vCenter 伺服器版本 6.0、版本 6.5、6.7 或 7.0 版。

  您也可以使用收集器 AMI 在 Amazon EC2 執行個體中部署收集器。
- 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 2008 R1 SP2、2008 R2 SP1
  - Windows Server 2012 R1、2012 R2
  - Windows Server 2016
  - Windows Server 2019
- 若要進行原始程式碼分析，您 GitHub 和 GitHub Enterprise 儲存庫必須具有可與策略建議收集器用戶端共用的存放庫範圍的個人存取權杖。有關使用回購範圍創建個人訪問令牌的更多信息，請參閱在GitHub文檔中創建個人訪問令牌。

  若要針對 .NET 建議分析移植助理程式的 .NET 存放庫，您必須提供使用 .NET 移植評估工具的移植助理設定的 Windows 機器。如需詳細資訊，請參閱 .NET 的移植助理使用者指南中的〈開始使用 .NET 的移植助理員入門〉。
- 若要啟用資料庫分析的策略建議，您必須在中輸入證明資料 AWS Secrets Manager。如需詳細資訊，請參閱 策略建議資料庫分析。
- 在使用 AWS Application Discovery Service 策略建議之前，您必須使用在 AWS Migration Hub 主控台中收集伺服器和應用程式的相關資料。您可以使用下列其中一種方法來收集資料。
  - 遷移中樞匯入 — 透過 Migration Hub 匯入，您可以將內部部署伺服器和應用程式的相關資訊匯入 Migration Hub。如需詳細資訊，請參閱應用 Ap plication Discovery Service 使用者指南中的 Migration Hub 匯入。
  - AWS Application Discovery Service 無代理程式收集器 — 無代理程式收集器是 VMware 應用裝置，可收集 VMware 虛擬機器 (VM) 的相關資訊。如需詳細資訊，請參閱應用程式探索服務使用者指南中的無代理程式收集器。
  - AWS 應用程式探索代理程式 — 探索代理程式是您安裝在內部部署伺服器和 VM 上的 AWS 軟體，可擷取系統資訊和系統之間網路連線的詳細資料。如需詳細資訊，請參閱AWS 應用程式探索服務使用者指南中的應用程式探索代理
- 策略建議資料收集器 — 如果您的伺服器託管在 VMware vCenter 中，且您提供存取權，則策略建議可以自動擷取伺服器詳細目錄。策略建議主控台將使用收集到的資訊來協助評估。

> **Note**
>
> 若要確認 Migration Hub 匯入是否順利完成，請在 Migration Hub 主控台導覽窗格的 [探索] 下，選擇 [伺服器]。應列出所有匯入的伺服器。



步驟 1：下載策略建議收集器

Migration Hub 策略建議應用程式資料收集器是您可以在內部部署 VMware 環境中安裝的虛擬應用裝置。策略建議應用程式資料收集器也以 Amazon 機器映像 (AMI) 的形式提供。如果您想要使用 AMI 版本的收集器來評估 AWS 應用程式或其他原因，您不需要下載收集器。您可以略過本節並移至在 Amazon EC2 執行個體中部署策略建議收集器。

本節說明如何下載收集器開啟虛擬化封存 (OVA) 檔案，以便在 VMware 環境中將收集器部署為虛擬機器 (VM)。

下載收集器 OVA 檔案

1. 使用您建立的 AWS 帳戶登入設定策略建議， AWS Management Console 然後開啟 Migration Hub 主控台，網址為 https://console.aws.amazon.com/migrationhub/。
2. 在 [Migration Hub] 主控台瀏覽窗格中，選擇 [策略]。
3. 在 [Migration Hub 策略建議] 頁面上，選擇 [下載資料收集器]。
4. 或者，如果您要匯入應用程式資料，您可以選擇「下載匯入範本」。如需匯入資料的詳細資訊，請參閱將資料匯入策略建議。
5. 按一下 [取得建議] 按鈕，然後選擇 [同意] 以允許 Migration Hub 在您的帳戶中建立服務連結角色 (SLR)。第一次設定策略建議時，您必須建立 SLR。如需詳細資訊，請參閱 針對策略建議使用服務連結角色。

步驟 2：部署策略建議收集器

本節說明如何部署「策略建議」應用程式資料收集器。應用程式資料收集器是一種無代理程式資料收集器，可識別伺服器上執行中的應用程式、執行原始碼分析，以及分析資料庫。

部署收集器的方式有兩種：

- 在您的 VMware vCenter 伺服器中部署為虛擬機器 (虛擬機器)。如需詳細資訊，請參閱 在 vCenter 中部署策略建議收集器。
- 如果您有要評估的 AWS 應用程式，可以使用策略建議收集器 Amazon 機器映像 (AMI)。如需詳細資訊，請參閱 在 Amazon EC2 執行個體中部署策略建議收集器。

在 vCenter 中部署策略建議收集器

Migration Hub 策略建議應用程式資料收集器是您可以在內部部署 VMware 環境中安裝的虛擬應用裝置。本節說明如何在 VMware 環境中將收集器開放虛擬化封存 (OVA) 檔案部署為虛擬機器 (VM)。

下列程序說明如何在您的 VMware vCenter 伺服器環境中部署策略建議收集器。

若要在 vCenter 中部署收集器

1. 以 VMware 管理員身分登入 vCenter。
2. 部署您在步驟 1 中下載的 OVA 檔案。OVA 項目包括收集器和 CLI，可用於存取策略建議 API。

   您也可以從以下連結下載 OVA 檔案：

   https://application-data-collector-release.s3.us-west-2.amazonaws.com/ova/latest/AWSMHubApplicationDataCollector.ova

我們建議您針對虛擬機器使用下列規格。

策略建議收集器 VM 規格

- 記憶體 — 至少 8 GB
- 中央處理器 — 至少 4 個

> **Note**
>
> 若要確保您使用的是具有所有新功能和錯誤修正的最新版本的收集器，請在部署收集器 OVA 檔案之後升級收集器。如需有關如何升級的指示，請參閱升級策略建議收集器。

在 Amazon EC2 執行個體中部署策略建議收集器

如果您有要評估的 AWS 應用程式，可以使用策略建議應用程式資料收集器 Amazon 機器映像 (AMI)。

下列程序說明如何從收集器 AMI 啟動 Amazon EC2 執行個體。

若要部署收集器亞馬遜 EC2 執行個體

1. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 在畫面上方的導覽列中，會顯示目前的 區域 (例如，美國東部 (俄亥俄))。從「策略建議」使用的「區域」中選擇符合您需求的區域。如需這些區域的清單，請參閱 AWS 一般參考.
3. 在導覽窗格的 [影像] 下，選擇 [AMI]。
4. 從「我擁有」下拉式清單中選擇「公開圖片」。
5. 選擇搜索欄，然後從菜單中選擇 AMI 名稱。
6. 輸入名稱AWSMHubApplicationDataCollector。
7. 若要確保 AMI 來自安全來源，請確認帳戶的擁有者是否為 703163 444405。
8. 若要從此 AMI 啟動執行個體，請選取該執行個體，然後選擇 [啟動]。如需有關使用主控台啟動執行個體的詳細資訊，請參閱 Amazon EC2 使用者指南中的從 AMI 啟動執行個體。

   我們建議使用下列規格適用於 Amazon EC2 執行個體。

   策略建議收集器 Amazon EC2 執行個體規格

   - 記憶體 — 至少 8 GB
   - 中央處理器 — 至少 4 個

策略建議 AMI 包括收集器和 CLI，可用於存取策略建議 API。

> **Note**
>
> 為確保您使用的是具有所有新功能和錯誤修正的最新版本的收集器，請在將策略建議收集器部署為 Amazon EC2 執行個體後升級收集器。如需有關如何升級的指示，請參閱升級策略建議收集器。

步驟 3：登入「策略建議」收集器

本節說明如何登入已部署的 Migration Hub 策略建議應用程式資料收集器。您登入收集器的方式取決於您的部署方式。

- 登入以 vCenter 為基礎的環境中部署的收集器

- 登入部署為 Amazon EC2 執行個體的收集器

登入以 vCenter 為基礎的環境中部署的收集器

登入部署在 vCenter 環境中的策略建議收集器

1. 使用下列命令連線到使用 SSH 用戶端的收集器。

```
ssh ec2-user@CollectorIPAddress
```

2. 當系統提示您輸入密碼時，請輸入預設密碼 aq1 @WSde3。您必須在第一次登入時變更密碼。

登入部署為 Amazon EC2 執行個體的收集器

若要登入部署為 Amazon EC2 執行個體的策略建議收集器

- 使用下列命令連線到使用 SSH 用戶端的收集器。

```
ssh -i "Keyname.pem" ec2-user@CollectorIPAddress
```

金鑰名稱 .pem 是您從收集器 AMI 啟動 Amazon EC2 執行個體時所產生的私密金鑰。

步驟 4：設定策略建議收集器

本節介紹如何使用命令行`collector setup`用於設定移轉中樞策略建議應用程式資料收集器的命令。這些配置存儲在本地。

在您可以使用之前`collector setup`命令，您必須使用以下命令在收集器 Docker 容器中創建一個 bash shell 會話`docker exec`指令。

```
docker exec -it application-data-collector bash
```

該`collector setup`命令會連續執行下列所有指令，但您可以個別執行它們：

- `collector setup --aws-configurations`— 設置AWS配置。
- `collector setup --vcenter-configurations`— 設定 vCenter 組態設定。

> **Note**
>
> 僅當收集器託管在 vCenter 上時，才能使用 vCenter 組態設定。不過，您可以使用指令強制執行 vCenter 組態設定`collector setup --vcenter-configurations`。

- `collector setup --remote-server-configurations`— 設置遠程服務器配置。
- `collector setup --version-control-configurations`-設置版本控制配置。

同時設定所有收集器組態

1. 輸入以下命令。

   ```
   collector setup
   ```

2. 輸入的資訊AWS配置，如中所述設定AWS配置。
3. 輸入 vCenter 組態的資訊，如中所述設定 vCenter 組態。
4. 輸入遠端伺服器組態的資訊，如中所述設定遠端伺服器組態。
5. 輸入版本控制配置的資訊，如中所述設定版本控制組態。
6. 依照中的指示，準備您的 Windows 和 Linux 伺服器以進行收集器資料收集準備遠端視窗和 Linux 伺服器以進行資料收集。

設定AWS配置

若要設定AWS組態, 使用時`collector setup`指令或`collector setup --aws-configurations`指令。

1. 輸入Y對於是您是否設置 IAM 許可...問題。您可以在建立使用者以存取收集器時設定這些權限`AWSMigrationHubStrategyCollector`按照中的步驟進行管理策略策略建議使用者和角色。
2. 輸入您的訪問密鑰和密鑰AWS具有您建立來存取收集器之使用者的帳戶，遵循中的步驟策略建議使用者和角色。
3. 輸入「區域」，例如，`us-west-2`。從「策略建議」使用的「區域」中選擇符合您需求的區域。如需這些區域的清單，請參閱策略建議端點在AWS 一般參考。
4. 輸入Y對於是將收集器相關指標上傳至移轉中樞策略服務？問題。量度資訊有助於AWS為您提供適當的支持。

5. 輸入Y對於是將收集器相關的記錄上傳至移轉中樞策略服務？問題。日誌中的信息有幫助AWS為您提供適當的支持。

下列範例顯示所顯示的內容，包括AWS配置。

```
Have you setup IAM permissions in you AWS account as per the user guide? [Y/N]: Y
Choose one of the following options for providing user credentials:
1. Long term AWS credentials
2. Temporary AWS credentials
Enter your options [1-2]: 2
AWS session token:
AWS access key ID [None]:
AWS secret access Key [None]:
AWS region name [us-west-2]:
AWS configurations are saved successfully
Upload collector related metrics to migration hub strategy service? By default
 collector will upload metrics. [Y/N]: Y
Upload collector related logs to migration hub strategy service? By default collector
 will upload logs. [Y/N]: Y
Application data collector configurations are saved successfully
Start registering application data collector
Application data collector is registered successfully.
```

設定 vCenter 組態

若要設定 vCenter 組態，請在使用`collector setup`指令或`collector setup --vcenter-configurations`命令：

1. 輸入Y對於是您是否要使用 VMware vCenter 認證進行驗證問題，如果您想要使用 VMware vCenter 認證進行驗證。

   > **Note**
   >
   > 使用 VMware vCenter 認證進行驗證時，需要在目標伺服器上安裝 VMware 工具。

   請輸入主持人網址，其可以是 vCenter IP 位址或網址。然後，輸入用户名和密碼適用於 VMware 的 vCenter。

2. 輸入Y對於是您是否有由 VMware vCenter 管理的視窗機器問題，如果你想配置 Windows 服務器。

   請輸入用户名和密碼對於視窗。

   > **Note**
   >
   > 如果您的 Windows 遠端伺服器屬於使用中目錄網域，您必須將使用者名稱輸入為####\###使用 CLI 提供遠端伺服器組態時。例如，如果您的網域名稱是 exampledomain，而您的使用者名稱是管理員，則您在 CLI 中輸入的使用者名稱為範例網域\ 系統管理員。

3. 輸入Y對於是使用 VMware 虛擬中心為 Linux 進行安裝問題，如果你想配置 Linux 服務器。

   請輸入用户名和密碼適用於 Linux 系統。

4. 輸入Y對於是您要使用 NTLM 為 vCenter 外部的伺服器設定認證嗎？和基於 Linux 的 SSH/證書的基礎問題，如果您想要為 vCenter 外部的伺服器設定遠端伺服器認證。

5. 對於您是否要使用 vCenter 安裝期間所使用的相同 Windows 認證問題，輸入Y如果在 vCenter 外部管理的 Windows 機器的身分證明與為 vCenter Windows 機器設定身分證明時提供的身分證明相同，則表示是。否則，請輸入N因為沒有。

   如果你回答Y是的，以下問題。

   a. 輸入Y對於是在與 Windows 服務器首次交互期間，收集器可以代表您接受和本地存儲服務器證書嗎？問題。

   b. 輸入1為了輸入您的選項問題，如果你想配置 SSH 身份驗證。

      如果您選擇使用 SSH 驗證，則必須將產生的金鑰認證複製到 Linux 伺服器。如需詳細資訊，請參閱在 Linux 伺服器上設定金鑰型驗證。

下列範例顯示所顯示的內容，包括 VMware vCenter 組態的範例項目。

```
Your Linux remote server configurations are saved successfully.
collector setup –vcenter-configurations
Start setting up vCenter configurations for remote execution
Note: Authenticating using VMware vCenter credentials requires VMware tools to be
 installed on the target servers
Would you like to authenticate using VMware vCenter credentials? [Y/N]: y
```

```
NOTE: Your vSphere user must have Guest Operations privileges enabled.

Host Url for VMware vCenter: domain-name
Username for VMware vCenter: username
Password for VMware vCenter: password
Reenter password for VMware vCenter: password
Successfully stored vCenter credentials...
Do you have Windows machines managed by VMware vCenter? [Y/N]: y

NOTE: For the best experience, we recommend that you create a new Active Directory user
 in the Domain Admins group.

Username for Windows (Domain\User): username
Password for Windows: password
Reenter password for Windows: password
Successfully stored windows credentials...
You can verify your setup for vCenter windows machines is correct with "collector diag-
check"
Do you have Linux machines managed by VMWare vCenter? [Y/N]: y
Username for Linux: username
Password for Linux: password
Reenter password for Linux: password
Successfully stored linux credentials...
You can verify your setup for vCenter linux machines is correct with "collector diag-
check"
Would you like to setup credentials for servers not managed by vCenter using NTLM for
 windows and SSH/Cert based for Linux? [Y/N]: y
Setting up target server for remote execution:
Would you like to setup credentials for servers not managed by vCenter using NLTM for
 Windows [Y/N]: y
Would you like to use the same Windows credentials used during vCenter setup? [Y/N]: y
Are you okay with collector accepting and locally storing server certificates on your
 behalf during first interaction with windows servers? These certificates will be used
 by collector for secure communication with windows servers [Y/N]: y
Successfully stored windows server credentials...
Please note that all windows server certificates are stored in directory /opt/amazon/
application-data-collector/remote-auth/windows/certs

Please note the IP address of the collector and run the script specified in the user
 documentation on all the windows servers in your inventory
You can verify your setup for remote windows machines is correct with "collector diag-
check"
Would you like to setup credentials for servers not managed by vCenter using SSH/Cert
 based for Linux? [Y/N]: y
```

```
Choose one of the following options for remote authentication:
1. SSH based authentication
2. Certificate based authentication
Enter your options [1-2]: 1
Would you like to use the same Linux credentials used during vCenter setup? [Y/N]: y
Generating SSH key on this machine...
Successfully generated SSH key pair

SSH key pair path: /opt/amazon/application-data-collector/remote-auth/linux/keys/
id_rsa_assessment
Please add the public key "id_rsa_assessment.pub" to the "$HOME/.ssh/authorized_keys"
 file in your remote machines.
You can verify your setup for remote linux machines is correct with "collector diag-
check
```

設定遠端伺服器組態

若要設定遠端伺服器組態，請在使用`collector setup`指令或`collector setup --remote-server-configurations`命令：

1. 輸入Y對於是您要使用 NLTM 為非 vCenter 管理的伺服器設定認證嗎？問題，如果你想配置 Windows 服務器。

   請輸入用户名和密碼適用於 WinRM。

   > **Note**
   >
   > 如果您的 Windows 遠端伺服器屬於使用中目錄網域，您必須將使用者名稱輸入為`####\###`使用 CLI 提供遠端伺服器組態時。例如，如果您的網域名稱是 exampledomain，而您的使用者名稱是管理員，則您在 CLI 中輸入的使用者名稱為範例網域\ 系統管理員。

   輸入Y對於是在與 Windows 服務器首次交互期間，收集器可以代表您接受和本地存儲服務器證書嗎？問題。視窗伺服器憑證儲存在目錄中`/opt/amazon/application-data-collector/remote-auth/windows/certs`。

   您必須將產生的伺服器認證複製到 Windows 伺服器。如需詳細資訊，請參閱在 Windows 伺服器上設定遠端伺服器組態。
2. 輸入Y對於是使用安全殼層或憑證進行 Linux 設定問題，如果你想配置 Linux 服務器。
3. 輸入1為了輸入您的選項問題，如果您想配置基於 SSH 密鑰的身份驗證。

如果您選擇使用 SSH 驗證，則必須將產生的金鑰認證複製到 Linux 伺服器。如需詳細資訊，請參閱在 Linux 伺服器上設定金鑰型驗證。

4. 輸入2為了輸入您的選項問題，如果您要設定以憑證為基礎的驗證。

   如需設定憑證型驗證的相關資訊，請參閱在 Linux 伺服器上設定憑證型驗證。

下列範例顯示顯示的內容，包括遠端伺服器組態的範例項目。

```
Setting up target server for remote execution
Would you like to setup credentials for servers not managed by vCenter using NLTM for
 Windows [Y/N]: y

NOTE: For the best experience, we recommend that you create a new Active Directory user
 in the Domain Admins group.

Username for WinRM (Domain\User): username
Password for WinRM: password
Reenter password for WinRM: password
Are you okay with collector accepting and locally storing server certificates on your
 behalf during first interaction with windows servers? These certificates will be used
 by collector for secure communication with windows servers [Y/N]: Y
Successfully stored windows server credentials...
Please note that all windows server certificates are stored in directory /opt/amazon/
application-data-collector/remote-auth/windows/certs

Please note the IP address of the collector and run the script specified in the user
 documentation on all the windows servers in your inventory
Would you like to setup credentials for servers not managed by vCenter using SSH/Cert
 based for Linux? [Y/N]: Y
Choose one of the following options for remote authentication:
1. SSH based authentication
2. Certificate based authentication
Enter your options [1-2]: 1
User name for remote server: username
Generating SSH key on this machine...
SSH key pair path: /opt/amazon/application-data-collector/remote-auth/linux/keys/
id_rsa_assessment
Please add the public key "id_rsa_assessment.pub" to the "$HOME/.ssh/authorized_keys"
 file in your remote machines.
Your Linux remote server configurations are saved successfully.
```

設定版本控制組態

若要設定版本控制組態，請在使用`collector setup`指令或`collector setup --version-control-configurations`命令：

1. 輸入Y對於是設置源代碼分析？問題。
2. 輸入1為了輸入您的選項問題，如果你想配置 Git 服務器端點。

   輸入吉塔布網為了GIT 服務器端點：。
3. 輸入2為了輸入您的選項問題，如果你想配置 GitHub企業伺服器。

   輸入不含 https://的企業端點，如下所示：GIT 服務器端點： *git-enterprise-endpoint*
4. 輸入你的 Git###和個人訪問##。
5. 輸入Y對於是你有沒有應該在 Windows 機器上分析的任何 csharp 存儲庫？問題，如果你想分析 C # 代碼。

   > **Note**
   >
   > 若要針對 .NET 建議分析移植助理程式的 .NET 存放庫，您必須提供使用 .NET 移植評估工具的移植助理設定的 Windows 機器。如需詳細資訊，請參閱開始使用 .NET 的移植助理在.NET 使用者指南的移植助理。
6. 對於您要重複使用此電腦上現有的 Windows 認證嗎？問題。輸入Y如果用於 C # 源代碼分析的 Windows 機器使用與之前提供的認證相同的憑據作為設置的一部分`--remote-server-configurations`或者`--vcenter-configurations`。

   輸入N如果您要輸入新的認證，則表示「否」。
7. 若要使用VMWARE 視窗機認證, 輸入1為了為 Windows 身份證明選擇下列其中一個選項。
8. 輸入視窗電腦的 IP 位址。

下列範例顯示所顯示的內容，包括版本控制組態的範例項目。

```
Set up for source code analysis [Y/N]: y
Choose one of the following options for version control type:
1. GIT
2. GIT Enterprise
3. Azure DevOps - Git
```

```
Enter your options [1-3]: 3
Your server endpoint: dev.azure.com (http://dev.azure.com/)
Your DevOps Organization name: <Your organization name>
Personal access token [None]:
Your version control credentials are saved successfully.
Do you have any csharp repositories that should be analyzed on a windows machine? [Y/
N]: y
Would you like to reuse existing windows credentials on this machine? [Y/N]: y
Choose one of the following options for windows credentials:
1. VMWare vCenter Windows Machine
2. Standard Windows Machine
Enter your options [1-2]:
1
Windows machine IP Address: <Your windows machine IP address>
Using VMWare vCenter Windows Machine credentials
Successfully stored windows server credentials...
```

準備遠端視窗和 Linux 伺服器以進行資料收集

> **Note**
>
> 如果您使用 vCenter 認證設定策略建議應用程式資料收集器，則不需要執行此步驟。

設定遠端伺服器組態之後，如果您正在使用`collector setup command`或`collector setup --remote-server-configurations`指令時，您必須準備遠端伺服器，以便策略建議應用程式資料收集器可以從這些伺服器收集資料。

> **Note**
>
> 您必須確定可使用其私人 IP 位址存取伺服器。有關如何通過虛擬私有雲（VPC）設置環境的進一步說明AWS如需遠端執行，請參閱亞馬遜虛擬私有雲用戶指南。

若要準備遠端 Linux 伺服器，請參閱準備遠端伺服器。

若要準備遠端 Windows 伺服器，請參閱在 Windows 伺服器上設定遠端伺服器組態。

準備遠端伺服器

在 Linux 伺服器上設定金鑰型驗證

如果您在設定遠端伺服器組態時選擇為 Linux 設定 SSH 金鑰型驗證，則必須執行下列步驟，在伺服器上設定金鑰型驗證，以便 Strategy Recommendations 應用程式資料收集器可以收集資料。

若要在 Linux 伺服器上設定金鑰型驗證

1. 複製使用名稱生成的公鑰酒吧分析評估從容器中的以下文件夾：

   /選擇/亞馬遜/application-data-collector/遠程驗證/鏈條/密鑰。
2. 將複製的公鑰附加到$HOME/.ssh/authorized_keys所有遠程計算機的文件。如果沒有可用的檔案，請使用touch或者vim指令。
3. 確定遠端伺服器上的主資料夾具有權限等級755或更少。如果是777，它不會工作。您可以使用chmod限制權限的命令。

在 Linux 伺服器上設定憑證型驗證

如果您在設定遠端伺服器組態時選擇為 Linux 設定憑證型驗證，則必須執行下列步驟，才能由策略建議應用程式資料收集器收集資料。

如果您已經為應用程式伺服器設定了憑證授權單位 (CA)，我們建議您使用此選項。

若要在 Linux 伺服器上設定憑證型驗證

1. 複製適用於所有遠端伺服器的使用者名稱。
2. 將收集器的公開金鑰複製到 CA。

   您可以在下列位置找到收集器的公開金鑰：

   /選擇/亞馬遜/application-data-collector/遠程驗證/鏈條/密鑰/id_rsa_評估.pub

   此公開金鑰必須新增至您的 CA，才能產生憑證。
3. 將上一個步驟中產生的憑證複製到收集器中的下列位置：

   /選擇/亞馬遜/application-data-collector/遠程驗證/鏈條/密鑰

   證書的名稱必須是瑞典證書評估證書。
4. 在設定步驟中提供憑證檔案名稱。

在 Windows 伺服器上設定遠端伺服器組態

如果您在收集器設定中設定遠端伺服器組態時選擇設定 Windows，則必須執行下列步驟，才能由策略建議收集資料。

> 若要瞭解更多 PowerShell 在遠程服務器上執行的腳本，請閱讀此注意事項。
>
> 該腳本啟用 PowerShell 遠端並停用交涉以外的所有驗證方法。這是用於視窗 NT 局域網管理器（NTLM），並設置」AllowUnencrypted「WSMan 協議為 false，以確保新創建的偵聽器僅接受加密的流量。使用微軟提供的腳本，`New-SelfSignedCertificateEx.ps1`，它會建立自我簽署的憑證。
> 任何具有 HTTP 接聽程式的 WSMan 執行個體都會與現有的 HTTPS 接聽程式一起移除。然後，它會建立新的 HTTPS 接聽程式。它也會為 TCP 連接埠 5986 建立輸入防火牆規則。在最後一個步驟中，WinRM 服務會重新啟動。

透過 Windows 2008 伺服器上的遠端連線設定資料收集

1. 使用下面的命令來檢查版本 PowerShell 安裝在您的服務器上。

   ```
   $PSVersionTable
   ```

2. 如果 PowerShell 版本不是 5.1，然後按照以下說明下載並安裝 WMF 5.1安裝和設定維基媒體基金會 5.1在微軟文檔中。
3. 在一個新的使用以下命令 PowerShell 窗口，以確保 PowerShell 5.1 已安裝。

   ```
   $PSVersionTable
   ```

4. 請遵循下一組步驟，說明如何透過 Windows 2012 及更新版本上的遠端連線設定資料收集。

若要透過 Windows 2012 和更新版本的伺服器上的遠端連線設定資料收集

1. 請從以下網址下載安裝指令碼：

   HTTPS：//application-data-collector-release.s3.us-西部-2. 亞馬遜. COM /腳本/網站設置p.ps1
2. 下載最新版`New-SelfSignedCertificateEx.ps1`從以下 URL 並將腳本粘貼到您下載的同一文件夾中`WinRMSetup.ps1`:

https://github.com/Azure/azure-libraries-for-net/BLOB /主/樣本/資產/新建-SelfSignedCertificateEx.ps1

3. 要完成設置，請運行下載的 PowerShell 所有應用程序服務器上的腳本

```
.\WinRMSetup.ps1
```

> **Note**
>
> 如果 Windows 遠端伺服器上未正確設定 Windows 遠端管理 (WinRM)，嘗試從該伺服器收集資料將會失敗。如果發生這種情況，您必須從容器上的下列位置刪除與該伺服器對應的憑證：/選擇/亞馬遜/application-data-collector/遠端驗證/視窗/證書/***ads-server-id***. CER 刪除憑證後，請等待資料收集程序重試。

確認您的收集器和伺服器已設定進行資料收集

使用下列命令，確認您的收集器和伺服器已正確設定資料收集。

```
collector diag-check
```

此命令會對您的伺服器組態進行一組診斷檢查，並在失敗的檢查時提供輸入。

當您在中使用指令時-a模式下，你得到的輸出DiagnosticCheckResult.txt檢查完成後的檔案。

```
collector diag-check -a
```

您可以對具有該伺服器 IP 位址之單一伺服器的伺服器組態執行診斷檢查。

下列範例顯示成功設定的輸出。

伺服器

```
            Provide your test server IP address: IP address
-----------------------------------------------------------------
Start checking connectivity & credentials...
Connectivity and Credential Checks succeeded
```

```
------------------------------------------------------------
Start checking permissions...
Permission Check succeeded
------------------------------------------------------------
Start checking OS version...
OS version check succeeded
------------------------------------------------------------
Start checking Linux Bash installation...
Linux Bash installation check succeeded
------------------------------------------------------------
All diagnostic checks complete successfully.
This server is correctly set up and ready for data collection.
```

視窗伺服器

```
           Windows PowerShell Version Check succeeded
Provide your test server IP address: IP address
------------------------------------------------------------
Start checking connectivity & credentials...
Connectivity and Credential Checks succeeded
------------------------------------------------------------
Start checking permissions...
Permission Check succeeded
------------------------------------------------------------
Start checking OS version...
OS version check succeeded
------------------------------------------------------------
Start checking Windows architecture type...
Windows Architecture Type Check succeeded
------------------------------------------------------------
All diagnostic checks complete successfully.
This server is correctly set up and ready for data collection.
```

下列範例顯示當您的遠端伺服器認證不正確時所顯示的錯誤訊息。

```
Unable to authenticate the server credentials with IP address ${IPAddress}.
Ensure that your credentials are accurate and the server is configured correctly.
Use the following command to reset incorrect credentials.
collector setup –remote-server-configurations
```

步驟 5：使用 Migration Hub 主控台中的策略建議來取得建議

本節說明如何使用 Migration Hub 主控台中的策略建議，以取得第一次移轉建議。

取得建議

1. 使用您建立的AWS帳戶登入設定策略建議，AWS Management Console然後開啟 Migration Hub 主控台，網址為 https://console.aws.amazon.com/migrationhub/。
2. 在 [Migration Hub] 主控台瀏覽窗格中，選擇 [策略]。
3. 在 [Migration Hub 策略建議] 頁面上，選擇 [取得建議]。
4. 如果您同意允許 Migration Hub 在您的帳戶中建立服務連結角色 (SLR)，請選擇 [同意]。如需 SLR 的詳細資訊，請參閱針對策略建議使用服務連結角色。
5. 設定資料來源

    a. 在 [設定資料來源] 頁面上，您必須從下列選項中選擇要分析的伺服器來源：

        i. 策略建議應用程式資料收集器 — 您可以使用策略建議收集器，自動擷取 VMware vCenter 中託管之虛擬機器的相關資訊。使用此選項，您不需要執行其他設定。

        ii. 手動匯入 — 如果您想要獨立引入伺服器和應用程式的相關資料，您可以使用策略建議匯入範本。匯入範本是 JSON 檔案，您可以在其中填寫 VM 的可用資訊。

        iii. 應用 Ap@@ plication Discovery Service — 您可以使用應用程式探索服務收集有關內部部署應用程式和伺服器的資訊 在 Migration Hub 主控台的 [工具] 區段下，您可以從 [探索工具] 下的多個選項中進行選擇。例如，您可以選擇 Ap plication Discovery Service 無代理程式收集器、AWS探索代理程式或匯入 (針對 CSV 檔案)。

    b. 「伺服器」表格會根據您在資料來源段落中的選擇，列出所有可用的伺服器。

    c. 在 [已註冊的應用程式資料收集器] 底下，會列出您已設定的應用程式資料收集器。如果尚未設定任何資料收集器，則可以下載資料收集器，然後進行部署。如需詳細資訊，請參閱 步驟 1：下載策略建議收集器 及 步驟 2：部署策略建議收集器。

    > **Note**
    >
    > 若要取得策略建議，您必須至少設定一個應用程式資料收集器，或執行應用程式資料匯入。如果您想要在不設定收集器的情況下新增應用程式層級資料，您可以使用應用程式資料匯入範本。您可以稍後新增其他資料來源。

d. 如果您選取「手動匯入」，請在「匯入詳細資訊」下選擇「新增匯入」

e. 在「匯入名稱」 中，輸入匯入的名稱。

f. 對於 S3 儲存貯體 URI，請輸入要上傳到的匯入 JSON 檔案的 S3 儲存貯體 URI。

> **Important**
>
> S3 儲存貯體名稱必須以的前置詞開頭**`migrationhub-strategy`**。

g. 選擇 下一步。

6. 指定偏好

a. 在 「指定偏好設定」 頁面上，設定您的業務目標和移轉偏好設定。策略建議根據您指定的偏好設定，建議移轉及現代化應用程式和資料庫的最佳策略。您可以稍後變更這些偏好設定。

b. 選擇 下一步。

7. 檢閱並提交。

a. 檢閱您設定的資料來源和移轉偏好設定。

b. 如果一切正確，請選擇 [開始資料分析]。這會針對您的 Microsoft IIS 和 Java 應用程式執行伺服器清查和執行階段環境，以及應用程式二進位檔案的分析。

> **Note**
>
> 二進位分析的狀態不會顯示在主控台中。分析完成時，您會看到反病毒碼報表的連結，或是指出分析不成功的訊息。

策略建議

本節說明如何檢視移轉產品組合中伺服器和應用程式的策略建議移轉和現代化建議。

主題

檢視策略建議中的策略建議

本節說明如何使用 AWS Migration Hub 主控台中的策略建議來檢視移轉策略建議。

若要檢視策略建議

1. 使用您建立的 AWS 帳戶登入設定策略建議， AWS Management Console 然後開啟 Migration Hub 主控台，網址為 https://console.aws.amazon.com/migrationhub/。
2. 在 [Migration Hub] 主控台瀏覽窗格中，選擇 [策略]，然後選擇 [建議]
3. 在「建議」頁面上，您可以檢視及匯出產品組合的摘要建議，以及詳細的移轉「R」策略建議。您也可以檢視遷移和現代化工具和目的地，以及伺服器和應用程式元件的反模式。

   反模式是在產品組合中找到的已知問題清單，依嚴重性分類。高嚴重性反模式表示需要解決的不兼容性，中等嚴重性反模式代表警告，低嚴重性反模式代表信息問題。如需有關「R」策略的資訊，請參閱AWS 規定指引詞彙表中的移轉詞彙-7 Rs。

   - 如果您的資料中心發生變更，或是您更新偏好設定，我們建議您重新分析您的資料。若要重新分析資料以取得新建議，請選擇「重新分析資料」。

     在重新分析程序完成之前，您的建議資料結果可能會混合先前的資料和新資料。

     若要下載包含建議的報告檔案，請選擇 [匯出建議]。
4. 在 [應用程式元件] 索引標籤上，您可以檢視移轉組合中應用程式元件的建議。如需詳細資訊，請參閱 策略建議應用程式元件建。
5. 在 [伺服器] 索引標籤上，您可以檢視移轉產品組合中伺服器的建議。如需詳細資訊，請參閱 策略建議伺服器建議。

6. 在「偏好設定」頁籤上，您可以編輯您在中指定的偏好設定步驟 5：取得建議。如需有關編輯偏好設定的資訊，請參閱策略建議偏好。

策略建議應用程式元件建

本節說明如何使用 Migration Hub 主控台中的策略建議，來檢視和分析應用程式元件的移轉策略建議。

主題

- 在策略建議中使用應用程式元件
- 策略建議源代碼分析
- 策略建議資料庫分析
- 策略建議二進制分析

在策略建議中使用應用程式元件

本節說明如何使用 Migration Hub 主控台中的 Migration Hub 策略建議來檢視和設定移轉和現代化策略建議。

主題

- 檢視應用程式元件建
- 設定應用程式元件的原始程式碼分析
- 設定應用程式元件的資料庫分析

檢視應用程式元件建

本節說明如何使用 Migration Hub 主控台中的策略建議，檢視應用程式元件的移轉策略建議。

檢視應用程式元件的建議詳細資訊

1. 使用您建立的 AWS 帳戶登入設定策略建議， AWS Management Console 然後開啟 Migration Hub 主控台，網址為 https://console.aws.amazon.com/migrationhub/。
2. 在 [Migration Hub] 主控台瀏覽窗格中，選擇 [策略]，然後選擇 [建議]
3. 在「建議」頁面上，選擇「應用程式元件」頁籤。

    a. 在 [應用程式元件摘要] 底下，是您在伺服器產品組合中執行之各種應用程式元件類型的概觀。

b. 在「應用程式元件」下，您可以檢視元件名稱、元件類型和移轉「R」策略建議。您也可以檢視移轉目的地，以及用於伺服器產品組合中執行的各種應用程式元件的移轉和現代化工具。如需有關「R」策略的資訊，請參閱AWS 規定指引詞彙表中的移轉詞彙-7 Rs。

4. 若要檢視應用程式元件的詳細資訊，請選取應用程式元件，然後選擇檢視詳細資訊。
5. 在應用程式元件詳細資訊頁面 (以元件名稱作為標題的頁面) 上，您可以檢視應用程式元件的建議。您也可以檢視已識別的反模式。反模式是在產品組合中找到的已知問題清單，依嚴重性分類。
6. 選擇策略選項頁籤，以檢視應用程式元件的移轉建議。您可以選取不同的策略，然後選擇設定偏好來覆寫建議的策略。
7. 視您檢視的應用程式元件類型而定，會有 [來源] 組態或 [資料庫組態] 索引標籤。如需有關來源組態的資訊，請參閱設定應用程式元件的原始程式碼分析。如需有關資料庫組態的資訊，請參閱設定應用程式元件的資料庫分析。

設定應用程式元件的原始程式碼分析

本節說明如何使用 Migration Hub 主控台中的策略建議來設定應用程式元件的原始程式碼分析。

設定應用程式元件的原始程式碼分析

1. 在 [Migration Hub] 主控台瀏覽窗格中，選擇 [策略]，然後選擇 [建議]
2. 在「建議」頁面上，選擇「應用程式元件」頁籤。
3. 從 [應用程式元件] 下的元件清單中，選取元件類型為 java、dotnetframework 或 IIS 的應用程式元件，然後選擇 [檢視詳細資料]。
4. 在應用程式元件詳細資訊頁面 (以元件名稱作為標題的頁面) 上，選擇 [原始程式碼組態] 索引標籤。
5. 在 [原始程式碼組態詳細資料] 下，選擇 [分析原始
6. 在 [分析原始程式碼] 頁面上，提供儲存應用程式元件之原始程式碼的儲存庫名稱、分支名稱和專案名稱 (如果適用)。選取您要使用的 GitHub 原始程式碼版本控制項類型，然後選擇 [分析]。

   分析完成後，您可以在應用程式元件詳細資訊頁面檢視更新的建議。

如需原始程式碼分析的詳細資訊，請參閱策略建議源代碼分析。

設定應用程式元件的資料庫分析

本節說明如何使用 Migration Hub 主控台中的策略建議來設定應用程式元件的資料庫分析。

設定應用程式元件的資料庫分析

1. 在 [Migration Hub] 主控台瀏覽窗格中，選擇 [策略]，然後選擇 [建議]
2. 在「建議」頁面上，選擇「應用程式元件」頁籤。
3. 從應用程式元件底下的元件清單中，選取元件類型為 SQLServer 的應用程式元件，然後選擇檢視詳細資訊。
4. 在應用程式元件詳細資訊頁面 (以元件名稱作為標題的頁面) 上，選擇資料庫組態頁籤。
5. 在 [資料庫組態詳細資訊] 底下，選擇 [分析資
6. 從您在 Sec AWS rets Manager 中建立的下拉式功能表中選擇用於資料庫認證的密碼名稱，然後選擇 [分析]。

   分析完成後，您可以在應用程式元件詳細資訊頁面檢視更新的建議。

如需有關資料庫分析和設定密碼名稱的更多資訊，請參閱策略建議資料庫分析。

策略建議源代碼分析

Migration Hub 策略建議會自動識別產品組合中的應用程式，並為其建立應用程式元件。例如，如果您的產品組合中有 Java 應用程式，則會將其識別為具有 Java 元件類型的應用程式元件。

如果您設定應用程式元件的原始程式碼，策略建議會分析它。如需設定應用程式元件以進行原始程式碼分析的資訊，請參閱設定應用程式元件的原始程式碼分析。

策略建議執行 Java 和 C# 程式設計語言的原始程式碼分析。

如需使用策略建議原始程式碼分析之先決條件的相關資訊，請參閱策略建議的先決條件。

策略建議資料庫分析

策略建議會自動識別產品組合中的資料庫伺服器，並為其建立應用程式元件。例如，如果您的產品組合中有 SQL Server 資料庫，就會識別為應用程式元件 sqlservr.exe。

策略建議會使用 S AWS chema Conversion Tool 來分析已識別 SQL Server 應用程式元件 sqlservr.exe 中的個別資料庫。策略建議也會識別將資料庫遷移到 AWS 資料庫時的不相容性，例如 Amazon Aurora MySQL 相容版本、Amazon Aurora PostgreSQL 相容版本、Amazon RDS for MySQL 版和適用 Amazon RDS for PostgreSQL。

目前，策略建議資料庫分析僅適用於 SQL Server。

若要設定策略建議以分析資料庫，您必須提供「策略建議」應用程式資料收集器的證明資料，才能連線至您的資料庫。要做到這一點，在您的帳戶中的秘 AWS Secrets Manager 中創建一個秘 AWS 密。

如需您提供之認證之權限和權限的相關資訊，請參閱AWS Schema Conversion Tool 認證所需的權限。如需使用認證建立密碼的相關資訊，請參閱在密碼管理員中建立資料庫認證的密碼。

設定認證和密碼之後，您可以在資料庫伺服器上設定 AWS Schema Conversion Tool 分析。如需詳細資訊，請參閱 設定應用程式元件的資料庫分析。

設定應用程式元件的資料庫分析之後，就會排程 AWS 結構描述轉換工具詳細目錄工作。完成此任務後，您將看到為該數據庫服務器上的每個單獨數據庫創建新的應用程序組件。例如，如果您的 SQL 伺服器有兩個資料庫 (例如資料庫 1 和範例 dbs2)，就會為每個資料庫建立一個應用程式元件，名稱為例子 dbs1 和範例 dbs2。

如果您希望在將每個已識別的 AWS 資料庫移轉至資料庫時看到反模式，請按照中設定應用程式元件的資料庫分析的步驟為每個資料庫設定分析。

AWS Schema Conversion Tool 認證所需的權限

您提供給 AWS Secrets Manager 的登入認證只需要`VIEW SERVER STATE`和`VIEW ANY DEFINITION`權限。或者，您也可以使用 https://gitlab.aws.dev/dmaf-pub/dmaf/-/blob/master/create_mssql_ro_user.sql 提供的指令碼建立新的登入。

您可以在建立 SQL Server 登入時提供任何想要的登入名稱和密碼。

在密碼管理員中建立資料庫認證的密碼

在認證準備好讓策略建議應用程式資料收集器連線到資料庫之後，請在您 AWS 帳戶的 AWS Secrets Manager 中建立密碼，如下列程序所述。

在您的 AWS 帳戶中使用 AWS Secrets Manager 建立密碼

1. 使用您建立的 AWS 帳戶登入 AWS Management Console 並開啟 AWS Secrets Manager 主控台設定策略建議，網址為 https://console.aws.amazon.com/secretsmanager/。
2. 選擇儲存新機密。
3. 將密碼類型選取為「其他類型的密碼」。
4. 在「鍵/值配對」下，輸入下列資訊。

   用戶名-##用戶名

   然後選擇 + 添加行並輸入以下信息。

密碼-##密碼

5. 選擇下一步。
6. 輸入密碼名稱作為具有前綴遷移中心- 策略-的任何字符串。例如，遷移中心戰略之一。

> **Note**
>
> 將您的秘密名稱存儲在安全的地方以備以後使用。

7. 選擇 [下一步]，然後再選擇 [下一步]。
8. 選擇儲存。

在策略建議中設定資料庫分析時，您可以使用為資料庫認證建立的密碼。

策略建議二進制分析

Migration Hub 策略建議會自動識別產品組合中的應用程式以及屬於這些應用程式的應用程式元件。例如，如果您的產品組合中有 Java 應用程式，則「策略建議」會將其識別為具有元件類型 java 的應用程式元件。如果您未設定原始程式碼的存取權限，策略建議可以執行二進位分析。藉由檢查 Windows 上的 IIS 應用程式 DLL 或 Linux 上的應用程式 JAR 檔案，並提供反病毒碼報告或不相容報告。反模式報告是「策略建議」在您的產品組合中找到的已知問題清單，依嚴重性分類。不兼容報告包含反模式的子集，這是 API 兼容性，Nuget Package 和移植操作。

策略建議執行分析視窗 IIS 和 Java Tomcat 和 Jboss 應用程式。如果您有 IIS 應用程式，「策略建議」預設會產生不相容性報告；您必須設定原始碼存取權，才能接收完整的反病毒碼報告。如果您有 Java 應用程式，則「策略建議」會依預設產生完整的反病毒碼報表。

分析完成後，會顯示不相容或反病毒碼報告。如果分析不成功，您可以嘗試通過提供源代碼訪問來運行源代碼分析，如中所述設定版本控制組態。

策略建議伺服器建議

本節說明如何使用 Migration Hub 主控台中的 Migration Hub 策略建議，檢視移轉組合中伺服器的移轉策略建議。

若要檢視伺服器的建議

1. 使用您建立的 AWS 帳戶登入設定策略建議， AWS Management Console 然後開啟 Migration Hub 主控台，網址為 https://console.aws.amazon.com/migrationhub/。

2. 在 [Migration Hub] 主控台瀏覽窗格中，選擇 [策略]，然後選擇 [建議]
3. 在 [建議] 頁面上，選擇 [伺服器] 索引標籤。
   a. 在「伺服器摘要」下，您可以檢視產品組合中所執行之各種伺服器類型的概觀。
   b. 在「伺服器」下，您可以檢視伺服器和作業系統詳細資料，以及移轉「R」策略建議 您也可以檢視移轉目的地，以及伺服器上識別的反病毒碼數目，這些反病毒碼是根據建議而定的。如需有關「R」策略的資訊，請參閱AWS 規定指引詞彙表中的移轉詞彙-7 Rs。
4. 若要檢視伺服器的深入建議詳細資料，請從清單中選取伺服器，然後選擇 [檢視詳細資料]。您可以檢視為伺服器收集的中繼資料，以及其深入的分析和建議，這些資料是根據伺服器上執行的應用程式元件而定。
5. 在伺服器詳細資料頁面 (以伺服器名稱作為標題的頁面) 的「建議摘要」下，您可以查看伺服器之策略建議的概觀。您也可以檢視已識別的反模式。反模式是在產品組合中找到的已知問題清單，依嚴重性分類。
6. 選擇策略選項標籤，以檢視伺服器的移轉建議。您可以選取不同的策略，然後選擇設定偏好來覆寫建議的策略。
7. 選擇應用程式元件頁籤，即可檢視與伺服器相關的應用程式元件清單。
8. 若要檢視應用程式元件的詳細資訊，請從清單中選取元件，然後選擇檢視詳細資訊。如需應用程式元件的詳細資訊，請參閱使用應用程式元件。

策略建議偏好

本節說明如何在 Migration Hub 主控台中檢視及編輯 Migration Hub 策略建議偏好設定。

您可以在第一次設定策略建議時選擇您的建議偏好設定，如中所述步驟 5：取得建議。您可以編輯這些偏好設定。

編輯建議偏好設定

1. 使用您建立的 AWS 帳戶登入設定策略建議， AWS Management Console 然後開啟 Migration Hub 主控台，網址為 https://console.aws.amazon.com/migrationhub/。
2. 在 [Migration Hub] 主控台瀏覽窗格中，選擇 [策略]，然後選擇 [建議]
3. 在「建議」頁面上，選擇「偏好設定」頁籤。
4. 在「優先順序的業務目標」下，您可以拖放業務目標以重新排列它們。
5. 選擇您想要的應用程式偏好設定和資料庫偏好設定，然後選擇 [儲存變更]。

如果您變更偏好設定，則會顯示橫幅提醒您選擇「重新分析資料」。

策略建議資料來源

本節說明「策略建議」使用的資料來源。

主題

檢視策略建議資料來源

本節說明如何檢視中的「策略建議」資料來源 AWS Management Console。

若要檢視資料來源

1. 使用您建立的 AWS 帳戶登入設定策略建議， AWS Management Console 然後開啟 Migration Hub 主控台，網址為 https://console.aws.amazon.com/migrationhub/。
2. 在 [Migration Hub] 主控台瀏覽窗格中，選擇 [策略]，然後選擇 [資料來源]
3. 在「收集器」標籤上，您可以檢視您設定的「策略建議」應用程式資料收集器。如需有關收集器的詳細資訊，請參閱策略建議應用程式資料收。
4. 在 [匯入] 索引標籤上，您可以匯入資料並檢視匯入的資料。如需詳細資訊，請參閱 將資料匯入策略建議。
5. 在工具標籤上，您可以下載收集器和應用程式匯入資料範本。

策略建議應用程式資料收

本節說明如何使用策略建議應用程式資料收集器。

如需有關下載和設定應用程式資料收集器的資訊，請參閱步驟 1：下載策略建議收集器。

主題

策略建議收集器所收集的資料

本節說明「Migration Hub 策略建議」應用程式資料收集器所收集的資料類型。應用程式資料收集器是一種無代理程式資料收集器，可識別伺服器上執行中的應用程式、執行原始碼分析，以及分析資料庫。

資料欄位	描述
作業系統型	視窗或 Linux
作業系統版本	作業系統的特定版本。例如，視窗服務器 2003，RHEL 5.2。
OS 架構	32 位或 64 位操作系統
是伺服器虛擬機	伺服器是 VM 或實體機器。
虛擬化軟體	例如，vCenter，超 V。
位置	例如，亞馬遜彈性運算雲端主控台 (Amazon EC2) 或現場部署。
是雙啟動	允許開機到多個作業系統
韌體類型	BIOS, UEFI
开机加载器	，2
分區表類型	MBR, GPT
處理器速度	CPU 速度，單位為千兆赫。例如，2.4 千兆赫。
Windows OS data	
視窗版	標準、資料中心、企業
. NET 框架版本	已安裝的 .NET 架構版本。
. NET 核心版本	已安裝 .NET 核心的版本。
Linux data	
作業系統發行版	RHEL、CentOS、SUSE 等等。

資料欄位	描述
核心版本	無名-r 輸出，如 `4.9.217-0.1.ac.205.84.332.metal1.x86_64`
For each disk volume	
檔案系統類型。	FAT32、NTFS、ReFS、Ext4、JFS 等等。
磁碟區大小	磁碟總大小
磁碟區可用空間	可用磁碟空間
虛擬磁碟映像檔格式	VMDK, vhd, vhdx
磁碟類型	基本、動態
Application level data	
應用程式名稱	執行中處理程序的名稱。例如，SQLServr.exe、MSdtsservr.exe 等等。
應用程式類型	IIS，JBoss，湯姆貓，等等。
程式語言與版本	C＃, 爪哇
JDK 版本	已安裝的 JDK 版本。
源代碼是否可用	如果您提供原始程式碼儲存庫，則表示原始程式碼可供使用。
應用位元大小	16 位元、32 位元、64 位元
Windows	
應用程序使用的 .NET 框架版本	在執行階段為應用程式載入的 .NET 架構 DLL 版本。
. NET 核心版本	在執行階段為應用程式載入的 .NET 核心 DLL 版本。

資料欄位	描述
使用 WPF 框架？	確定基於 .NET 的應用程序是否是 WPF 應用程序的類型。
使用 WCF 框架？	確定基於 .NET 的應用程序是否為 WCF 應用程序的類型。
ASP.NET 版本	ASP.NET 的版本。
IIS 版本	安裝在視窗電腦上的 IIS 伺服器版本。
應用程式 OS 驅動程式位元	32 位元、64 位元
視窗登錄使用	查詢機器的登錄機碼，以尋找資料庫版本、Java 版本、.NET 版本等資訊。
應用程式使用的所有 DLL	獲取 Windows 進程在運行時加載的所有 DLL 的列表。
PowerShell 版本	檢查電腦上安裝的 PowerShell 版本 (應為 5.1 或更新版本)。
Linux	
應用程式架構型	小貓, 春季啟動, JBoss, WebLogic WebSphere
應用程式架構版	應用程式架構的版本。
Database	
資料庫類型	MS SQL，甲骨文，MySQL，等等。
資料庫版本	資料庫的版本。

從策略建議中移除您的資料

要從策略建議中刪除所有數據，請聯繫AWS Support並請求完全刪除數據。

升級策略建議收集器

Migration Hub 策略建議應用程式資料收集器會自動升級。如有需要，您可以使用下列程序手動升級收集器。

若要升級「策略建議」收集器

1. 使用下列命令，透過 SSH 用戶端連線至收集器虛擬機器。

```
ssh ec2-user@CollectorIPAddress
```

2. 變更至收集器虛擬機器中的升級目錄，如下列範例所示。

```
cd  /home/ec2-user/collector/upgrades
```

3. 使用下列命令執行升級指令碼。

```
bash application-data-collector-upgrade
```

將資料匯入策略建議

除了使用應用程式資料收集器之外，您還可以匯入要移轉和現代化建議之應用程式和伺服器的相關資訊。

匯入資料時，建議的深度不如使用資料收集器時的深度。例如，您無法對匯入的資料使用原始程式碼分析。

本節說明如何使用應用程式匯入範本，將資料匯入 Migration Hub 主控台中的策略建議。

若要匯入資料

1. 使用您建立的 AWS 帳戶登入設定策略建議， AWS Management Console 然後開啟 Migration Hub 主控台，網址為 https://console.aws.amazon.com/migrationhub/。
2. 在 [Migration Hub] 主控台瀏覽窗格中，選擇 [策略]，然後選擇 [資料來源]
3. 選擇「匯入」頁標。
4. 選擇 [下載匯入範本] 以下載應用程式匯入範本。
5. 填寫範本並將其上傳到 Amazon S3 儲存貯體。請確定值區的名稱以前置字元開頭`migrationhub-strategy`。

6. 返回「匯入」標籤，然後選擇「匯入」。
7. 輸入匯入名稱，輸入已填寫資料範本的 Amazon S3 物件 URI，然後選擇「開始匯入」。

策略建議匯入範本

您下載的匯入範本是.json檔案，如以下範例所示。

```
{
    "ImportFormatVersion": 1,
    "Resources": [
        {
            "ResourceType": "SERVER",
            "ResourceName": "",
            "ResourceId": "",
            "IpAddress": "",
            "OSDistribution": "",
            "OSType": "",
            "HostName": "",
            "OSVersion": "",
            "CPUArchitecture": ""
        },
        {
            "ResourceType": "PROCESS",
            "ResourceName": "",
            "ResourceId": "",
            "ApplicationType": "",
            "DotNetFrameworkVersion": "",
            "ApplicationVersion": "",
            "DotNetCoreVersion": "",
            "JdkVersion": "",
            "ProgrammingLanguage": "",
            "DatabaseType": "",
            "DatabaseVersion": "",
            "DatabaseEdition": "",
            "AssociatedServerIds": []
        }
    ]
}
```

為了協助您填寫匯入範本，下表列出了資料欄位的有效值。

下表列出伺服器的必要欄位。

名稱	Description (描述)	Type	必要	有效值
ResourceId	資源的唯一 ID	字串	是	任何唯一字串
ResourceName	資源的名稱	字串	是	任何字串
ResourceType	要匯入的資源類型	字串	是	「伺服器」、「處理程序」
作業系統分	視窗, 視窗服務器, Ubuntu	字串	是	視窗：「視窗電腦」、「視窗伺服器」 Linux:「Ubuntu 的」,「瑞爾」,「Amazon Linux」,「DEBIAN」,「SLES」,「中心」,「LINUX」,「軟呢」,「卡利」
OSType	操作系統的類型	字串	是	「視窗」、「Linux 系統」
版本	內核版本	字串	是	請參閱 HTML 版本的文檔。
CPU 架構	中央處理器架構	字串	否	「32 位元」、「64 位元」
IpAddress	伺服器的 IP 位址	陣列	否	格式為 XXXXX
MacAddresses	與伺服器相關聯的 Mac 位址	陣列	否	格式為三十：三十：三十：三十：XX
Hostname (主機名稱)	主機的名稱	字串	否	任何字串

下表列出處理程序的必要欄位。

名稱	Description (描述)	Type	必要	有效值
ResourceId	資源的唯一 ID	字串	是	任何唯一字串
ResourceName	資源的名稱	字串	是	任何字串
ResourceType	要匯入的資源類型	字串	是	「伺服器」、「處理程序」
AssociatedServer身份證	執行處理序的伺服器 ID 清單。	字串	是	您定義的 ResourceId 來自「」：「服務器」。ResourceType
ApplicationType	應用程序的類型	字串	是	「湯姆貓」,「JBoss」,「春天」,「IIS」,「蒙戈數據庫」,「DB2」,「瑪麗亞數據庫」,「MySQL」,「甲骨文」,「SQL 服務器」,「系統」,「郵政服務器」,「卡桑德拉」,「IBM「,「甲骨文「,「通用 Java」 WebSphere WebLogic
ApplicationVersion	應用程式的版本	字串	是	「IIS 1.0」，「IIS 2.0」，「IIS 3.0」，「IIS 4.0」，「IIS 5.0」，「IIS 5.1」，「IIS 6.0」，「IIS 7.0」，「IIS 7.0」，「IIS 7.5」，「IIS 8.0」，「IIS 8.0」，「IIS 8.0」，「IIS 8.0」
ProgrammingLanguage	應用程式的程式設計語言	字串	否	「爪哇」,「夏普」

名稱	Description (描述)	Type	必要	有效值
DotNetFrameworkVersion	如果應用程序是基於 .NET 框架的 .NET 框架的版本	字串	否	「DotnetFramework 1.0」、「1.0 SP2」、「DotnetFramework 1.0 SP2」、「DotnetFramework DotnetFramework 1.0 SP3」、「1.1」、「DotnetFramework 1.1 規則 DotnetFramework 1」、「DotnetFramework2.1」、「DotnetFramework 2.0 SP2」、「3.2」、「3.0 SP2」、「DotnetFramework 3.0 SP2」DotnetFramework、「3.5」、「DotnetFramework DotnetFramework 3.5」、「4.0」、「4.0」、「4.5.1」、「4.5.1」DotnetFramework、「4.6.5」、「4.5.1」、「4. DotnetFramework 6.5」、「4. DotnetFramework 5.1」、「DotnetFramework 4.6.5」「」,「DotnetFramework 4.7」,「4.7.1」,「DotnetFramework 4.7.2 英寸」,「4.8」DotnetFramework DotnetFramework DotnetFramework DotnetFramework DotnetFramework DotnetFramework DotnetFramework DotnetFramework

名稱	Description (描述)	Type	必要	有效值
DotNetCoreVersion	.NET 核心的版本，如果應用程式是以 .NET 核心為基礎	字串	否	「淨網核心 1.0」，「淨網核心 1.1」，「淨網核心 2.0」，「淨網核心 2.1」，「淨網核心 2.0」，「淨網核心 3.0」，「淨網核心 3.1」
JdkVersion	JDK 的版本 (如果應用程式使用 JDK)	字串	否	「JDK1.0」，「JDK2.0」，「JDK3.0」，...，「JDK1.0」
DatabaseType	型別資料庫	字串	否	「SQL 服務器」，「甲骨文」，「系統」，「蒙戈數據庫」，「瑪麗亞數據庫」，「阿帕奇卡桑德拉」，「MySQL 的」，「IBM DB2」，「郵政服務器」
DatabaseEdition	資料庫的版本	字串	否	
DatabaseVersion	資料庫的版本	字串	否	請參閱 HTML 版本的文檔。

從策略建議中移除您的資料

若要從 Migration Hub 策略建議移除所有資料，請連絡AWS Support。

Migration Hub 的安全性策略建議

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。

安全性是 AWS 與您共同肩負的責任。共同的責任模式將其稱為雲端的安全性和雲端中的安全性：

- 雲端本身的安全 – AWS 負責保護執行 AWS 雲端 內 AWS 服務的基礎設施。AWS 提供的服務，也可讓您安全使用。第三方稽核人員會定期測試和驗證我們安全性的有效性，作為 AWS 合規計畫的一部分。若要了解適用於 Migration Hub 策略建議的符合性計劃，請參閱合規計劃AWS服務範圍內的AWS服務，遵的服務。
- 雲端內部的安全 – 您的責任取決於所使用的 AWS 服務。您也必須對其他因素負責，包括資料的機密性、您公司的請求和適用法律和法規。

本文件可協助您瞭解如何在使用策略建議時套用共同的責任模型。下列主題說明如何設定「策略建議」，以符合您的安全性與合規性目標。您也會學到如何使用其他AWS服務來協助您監控和保護您的策略建議資源。

主題

- Migration Hub 策略建議中的資料保護
- Migration Hub 的身分識別與存取管理策略建議
- Migration Hub 策略建議的合規性驗證

Migration Hub 策略建議中的資料保護

AWS共同責任模型適用於 Migration Hub 策略建議中的資料保護。如此模型所述，AWS 負責保護執行所有 AWS 雲端 的全球基礎設施。您負責維護在此基礎設施上託管內容的控制權。您也必須負責您所使用 AWS 服務 的安全組態和管理任務。如需有關資料隱私權的更多相關資訊，請參閱資料隱私權常見問答集。如需有關歐洲資料保護的相關資訊，請參閱 AWS 安全性部落格上的 AWS 共同的責任模型和 GDPR 部落格文章。

基於資料保護目的，建議您使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 保護 AWS 帳戶 憑證，並設定個人使用者。如此一來，每個使用者都只會獲得授與完成其任務所必須的許可。我們也建議您採用下列方式保護資料：

- 每個帳戶均要使用多重要素驗證 (MFA)。

- 使用 SSL/TLS 與 AWS 資源通訊。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 使用 AWS CloudTrail 設定 API 和使用者活動日誌記錄。
- 使用 AWS 加密解決方案，以及 AWS 服務 內的所有預設安全控制項。
- 使用進階的受管安全服務（例如 Amazon Macie），協助探索和保護儲存在 Amazon S3 的敏感資料。
- 如果您在透過命令列介面或 API 存取 AWS 時，需要 FIPS 140-2 驗證的加密模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的更多相關資訊，請參閱聯邦資訊處理標準 (FIPS) 140-2 概觀。

我們強烈建議您絕對不要將客戶的電子郵件地址等機密或敏感資訊，放在標籤或自由格式的文字欄位中，例如 Name (名稱) 欄位。這包括當您使用主控台、API 或 AWS SDK AWS 服務 使用策略建議或其他策略建議時。AWS CLI您在標籤或自由格式文字欄位中輸入的任何資料都可能用於計費或診斷日誌。如果您提供外部伺服器的 URL，我們強烈建議請勿在驗證您對該伺服器請求的 URL 中包含憑證資訊。

靜態加密

所有儲存在策略建議資料庫中的資料都經過加密處理。

傳輸中加密

策略建議網路間通訊支援所有元件和用戶端之間的 TLS 1.2 加密。

Migration Hub 的身分識別與存取管理策略建議

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) 以使用策略建議資源。IAM 是您可以使用的 AWS 服務 ，無需額外付費。

主題

- 物件
- 使用身分驗證
- 使用政策管理存取權
- Migration Hub 策略建議如何與 IAM 搭配使用

- AWS Migration Hub 策略建議的受管原則
- Migration Hub 策略建議的身分識別型原則範例
- 疑難排解 Migration Hub 策略建議識別與存取
- 針對策略建議使用服務連結角色
- Migration Hub 戰略建議和介面 VPC 端點 (AWS PrivateLink)

物件

您使用 AWS Identity and Access Management (IAM) 的方式會因您在策略建議中所做的工作而有所不同。

服務使用者 — 如果您使用策略建議服務執行工作，則管理員會為您提供所需的認證和權限。當您使用更多策略建議功能來完成工作時，您可能需要其他權限。了解存取許可的管理方式可協助您向管理員請求正確的許可。如果您無法存取策略建議中的功能，請參閱疑難排解 Migration Hub 策略建議識別與存取。

服務管理員 — 如果您負責公司的策略建議資源，您可能擁有「策略建議」的完整存取權。決定您的服務使用者應存取哪些策略建議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。若要深入了解貴公司如何搭配策略建議使用 IAM，請參閱Migration Hub 策略建議如何與 IAM 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策略建議存取權限的詳細資訊。若要檢視可在 IAM 中使用的策略建議以身分識別為基礎的政策範例，請參閱。Migration Hub 策略建議的身分識別型原則範例

使用身分驗證

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您的要求。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。如需詳細資訊，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。

聯合身分

最佳作法是要求人類使用者 (包括需要系統管理員存取權的使用者) 使用與身分識別提供者的同盟，才能使用臨時登入資料進行存取 AWS 服務 。

聯合身分識別是來自企業使用者目錄的使用者、Web 身分識別提供者、Identi ty Center 目錄，或使用透過身分識別來源提供的認證進行存取 AWS 服務 的任何使用者。 AWS Directory Service同盟身分存取時 AWS 帳戶，他們會假設角色，而角色則提供臨時認證。

對於集中式存取權管理，我們建議您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中建立使用者和群組，也可以連線並同步到自己身分識別來源中的一組使用者和群組，以便在所有應用程式 AWS 帳戶 和應用程式中使用。如需 IAM Identity Center 的詳細資訊，請參閱《AWS IAM Identity Center 使用者指南》中的什麼是 IAM Identity Center？。

IAM 使用者和群組

IAM 使用者是您內部的身分，具 AWS 帳戶 有單一人員或應用程式的特定許可。建議您盡可能依賴臨時憑證，而不是擁有建立長期憑證 (例如密碼和存取金鑰) 的 IAM 使用者。但是如果特定使用案例需要擁有長期憑證的 IAM 使用者，建議您輪換存取金鑰。如需詳細資訊，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。您無法以群組身分簽署。您可以使用群組來一次為多名使用者指定許可。群組可讓管理大量使用者許可的程序變得更為容易。例如，您可以擁有一個名為 IAMAdmins 的群組，並給予該群組管理 IAM 資源的許可。

使用者與角色不同。使用者只會與單一人員或應用程式建立關聯，但角色的目的是在由任何需要它的人員取得。使用者擁有永久的長期憑證，但角色僅提供暫時憑證。若要進一步了解，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 – 若要向聯合身分指派許可，請建立角色，並為角色定義許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並獲授予由角色定義的許可。如需聯合角色的相關資訊，請參閱《IAM 使用者指南》中的為第三方身分供應商建立角色。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：您可以使用 IAM 角色，允許不同帳戶中的某人 (信任的主體) 存取您帳戶的資源。角色是授予跨帳户存取權的主要方式。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）。若要了解跨帳户存取權和資源型政策間的差異，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。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 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 執行個體內存放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臨時性憑證。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。

若要了解是否要使用 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 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相關資訊，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，哪個主體在什麼条件下可以對什麼資源執行哪些動作。

預設情況下，使用者和角色沒有許可。若要授予使用者對其所需資源執行動作的許可，IAM 管理員可以建立 IAM 政策。然後，管理員可以將 IAM 政策新增至角色，使用者便能擔任這些角色。

IAM 政策定義該動作的許可，無論您使用何種方法來執行操作。例如，假設您有一個允許 `iam:GetRole` 動作的政策。具有該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

身分型政策是可以連接到身分 (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。若要了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限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中指定主體。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) 可控制哪些主體 (帳戶成員、使用者或角色) 擁有存取某資源的許可。ACL 類似於資源型政策，但它們不使用 JSON 政策文件格式。

Amazon S3 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予您的最大許可。

- 許可界限：許可界限是一種進階功能，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的限制。所有這類政策中的明確拒絕都會覆寫該允許。如需許可邊界的相關資訊，請參閱《IAM 使用者指南》中的 IAM 實體許可邊界。
- 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 AWS Organizations 是一種用於分組和集中管理您企業擁 AWS 帳戶 有的多個服務。若您啟用組織中的所有功能，您可以將服務控制政策 (SCP) 套用到任何或所有帳戶。SCP 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 Organizations 和 SCP 的詳細資訊，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身分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。如需詳細資訊，請參閱《IAM 使用者指南》中的工作階段政策。

多種政策類型

將多種政策類型套用到請求時，其結果形成的許可會更為複雜、更加難以理解。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。

Migration Hub 策略建議如何與 IAM 搭配使用

在您使用 IAM 管理策略建議的存取權限之前，請先了解哪些 IAM 功能可與策略建議搭配使用。

可搭配 Migration Hub 策略建議使用的 IAM 功能

IAM 功能	策略建議支援
身分型政策	是
資源型政策	否
政策動作	是
政策資源	否
政策條件索引鍵	否
ACL	否
ABAC(政策中的標籤)	否
臨時憑證	是
主體許可	是
服務角色	否
服務連結角色	是

若要取得策略建議和其他 AWS 服務如何搭配大多數 IAM 功能運作的高階檢視，請參閱 IAM 使用者指南中的搭配 IAM 使用的AWS 服務。

策略建議的身分識別原則

支援身分型政策	是

身分型政策是可以連接到身分 (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。

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。您無法在身分型政策中指定主體，因為這會套用至連接的使用者或角色。如要了解您在 JSON 政策中使用的所有元素，請參閱《IAM 使用者指南》中的 IAM JSON 政策元素參考。

策略建議的身分識別原則範例

若要檢視以身分識別為基礎的策略範例，請參閱。Migration Hub 策略建議的身分識別型原則範例

策略建議中的資源型政策

支援以資源基礎的政策	否

資源型政策是附加到資源的 JSON 政策文件。資源型政策的最常見範例是 IAM 角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中指定主體。主參與者可以包括帳戶、使用者、角色、同盟使用者或。 AWS 服務

若要啟用跨帳戶存取，您可以指定在其他帳戶內的所有帳戶或 IAM 實體，作為資源型政策的主體。新增跨帳戶主體至資源型政策，只是建立信任關係的一半。當主體和資源位於不同時 AWS 帳戶，受信任帳戶中的 IAM 管理員也必須授與主體實體 (使用者或角色) 權限，才能存取資源。其透過將身分型政策連接到實體來授與許可。不過，如果資源型政策會為相同帳戶中的主體授予存取，這時就不需要額外的身分型政策。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM 角色與資源型政策有何差異。

策略建議的政策行動

支援政策動作	是

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個主體在什麼条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。也有一些作業需要政策中的多個動作。這些額外的動作稱為相依動作。

政策會使用動作來授予執行相關聯動作的許可。

若要查看策略建議動作清單，請參閱服務授權參考資料中的 Migration Hub 策略建議所定義的動作。

策略建議中的原則動作會在動作之前使用下列前置詞：

```
migrationhub-strategy
```

若要在單一陳述式中指定多個動作，請用逗號分隔。

```
"Action": [
      "migrationhub-strategy:action1",
      "migrationhub-strategy:action2"
         ]
```

若要檢視以身分識別為基礎的策略範例，請參閱。Migration Hub 策略建議的身分識別型原則範例

策略建議的政策資源

支援政策資源	否

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。

Resource JSON 政策元素可指定要套用動作的物件。陳述式必須包含 Resource 或 NotResource 元素。最佳實務是使用其 Amazon Resource Name (ARN) 來指定資源。您可以針對支援特定資源類型的動作 (稱為資源層級許可) 來這麼做。

對於不支援資源層級許可的動作 (例如列出操作)，請使用萬用字元 (*) 來表示陳述式適用於所有資源。

```
"Resource": "*"
```

若要查看策略建議資源類型及其 ARN 的清單，請參閱服務授權參考資料中由 Migration Hub 策略建議定義的資源。若要瞭解可以使用哪些動作指定每個資源的 ARN，請參閱 Migration Hub 策略建議定義的動作。

若要檢視以身分識別為基礎的策略範例，請參閱。Migration Hub 策略建議的身分識別型原則範例

策略建議的政策條件索引鍵

支援服務特定政策條件金鑰	否

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。

Condition 元素 (或 Condition 區塊) 可讓您指定使陳述式生效的條件。Condition 元素是選用項目。您可以建立使用條件運算子的條件運算式 (例如等於或小於)，來比對政策中的條件和請求中的值。

若您在陳述式中指定多個 Condition 元素，或是在單一 Condition 元素中指定多個索引鍵， AWS 會使用邏輯 AND 操作評估他們。如果您為單一條件索引鍵指定多個值，請使用邏輯OR運算來 AWS 評估條件。必須符合所有條件，才會授與陳述式的許可。

您也可以在指定條件時使用預留位置變數。例如，您可以只在使用者使用其 IAM 使用者名稱標記時，將存取資源的許可授予該 IAM 使用者。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM 政策元素：變數和標籤。

AWS 支援全域條件金鑰和服務特定條件金鑰。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。

若要查看策略建議條件金鑰清單，請參閱服務授權參考中的適用於 Migration Hub 策略建議的條件金鑰。若要了解可以使用條件金鑰的動作和資源，請參閱由 Migration Hub 策略建議定義的動作。

若要檢視以身分識別為基礎的策略範例，請參閱。Migration Hub 策略建議的身分識別型原則範例

策略建議中的存取控制清單 (ACL)

支援 ACL	否

存取控制清單 (ACL) 可控制哪些主體 (帳戶成員、使用者或角色) 擁有存取某資源的許可。ACL 類似於資源型政策，但它們不使用 JSON 政策文件格式。

以屬性為基礎的存取控制 (ABAC) 與策略建議

支援 ABAC (政策中的標籤)	否

屬性型存取控制 (ABAC) 是一種授權策略，可根據屬性來定義許可。在中 AWS，這些屬性稱為標籤。您可以將標籤附加到 IAM 實體 (使用者或角色) 和許多 AWS 資源。為實體和資源加上標籤是 ABAC 的第一步。您接著要設計 ABAC 政策，允許在主體的標籤與其嘗試存取的資源標籤相符時操作。

ABAC 在成長快速的環境中相當有幫助，並能在政策管理變得繁瑣時提供協助。

若要根據標籤控制存取，請使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 條件金鑰，在政策的條件元素中，提供標籤資訊。

如果服務支援每個資源類型的全部三個條件金鑰，則對該服務而言，值為 Yes。如果服務僅支援某些資源類型的全部三個條件金鑰，則值為 Partial。

如需 ABAC 的詳細資訊，請參閱《IAM 使用者指南》中的什麼是 ABAC?。如要查看含有設定 ABAC 步驟的教學課程，請參閱《IAM 使用者指南》中的使用屬性型存取控制 (ABAC)。

搭配策略建議使用臨時登入資

支援臨時憑證	是

當您使用臨時憑據登錄時，某些 AWS 服務 不起作用。如需其他資訊，包括哪些 AWS 服務 與臨時登入資料搭配AWS 服務 使用，請參閱 IAM 使用者指南中的 IAM。

如果您使用除了使用者名稱和密碼以外的任何方法登入，則您正在 AWS Management Console 使用臨時認證。例如，當您 AWS 使用公司的單一登入 (SSO) 連結存取時，該程序會自動建立暫時認證。當您以使用者身分登入主控台，然後切換角色時，也會自動建立臨時憑證。如需切換角色的詳細資訊，請參閱《IAM 使用者指南》中的切換至角色 (主控台)。

您可以使用 AWS CLI 或 AWS API 手動建立臨時登入資料。然後，您可以使用這些臨時登入資料來存取 AWS。 AWS 建議您動態產生臨時登入資料，而不是使用長期存取金鑰。如需詳細資訊，請參閱 IAM 中的暫時性安全憑證。

策略建議的跨服務主體權限

支援轉寄存取工作階段 (FAS)	是

當您使用 IAM 使用者或角色在中執行動作時 AWS，您會被視為主體。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 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》。

策略建議的服務角色

支援服務角色	否

服務角色是服務擔任的 IAM 角色，可代您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需詳細資訊，請參閱《IAM 使用者指南》中的建立角色以委派許可給 AWS 服務服務。

> **Warning**
>
> 變更服務角色的權限可能會中斷策略建議功能。只有在策略建議提供指引時，才編輯服務角色。

策略建議的服務連結角色

支援服務連結角色	是

服務連結角色是一種連結至. 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。

如需有關建立或管理策略建議服務連結角色的詳細資訊，請參閱針對策略建議使用服務連結角色。

AWS Migration Hub 策略建議的受管原則

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。服務有時會將其他權限新增至受 AWS 管理的策略，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)。當新功能啟動或新作業可用時，服務最有可能更新 AWS 受管理的策略。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： AWSMigrationHubStrategyConsoleFullAccess

您可將 `AWSMigrationHubStrategyConsoleFullAccess` 政策連接到 IAM 身分。

此原`AWSMigrationHubStrategyConsoleFullAccess`則會透過授與使用者對策略建議服務的完整存取權 AWS Management Console。

許可詳細資訊

此政策包含以下許可。

- `discovery`— 授予使用者存取權，以取得應用程式探索服務中的探索摘要。
- `iam`— 允許為使用者建立服務連結角色，這是使用策略建議的必要條件。
- `migrationhub-strategy`— 授與使用者對策略建議的完整存取權限。
- `s3`— 允許使用者建立和讀取策略建議所使用的 S3 儲存貯體。
- `secretsmanager`— 允許使用者在密碼管理員中列出密碼存取權限。

若要檢視此策略的權限，請參閱AWS 受管理AWSMigrationHubStrategyConsoleFullAccess的策略參考指南中的。

AWS 受管理的策略： AWSMigrationHubStrategyCollector

您可將 `AWSMigrationHubStrategyCollector` 政策連接到 IAM 身分。

許可詳細資訊

此政策包含以下許可。

- `application-transformation`— 授與上傳應用程式轉換作業的記錄檔和指標資料的權限，並與移植相容性評估和建議搭配使用。
- `execute-api`— 允許使用者存取 Amazon API Gateway，將日誌和指標上傳到 AWS。
- `migrationhub-strategy`— 授與使用者註冊訊息、傳送訊息、上傳記錄資料以及將量度資料上傳至策略建議的存取權。
- `s3`— 授與使用者清單值區及其位置的存取權。使用者也可以存取寫入、擷取物件、將物件新增至、傳回存取控制清單 (ACL)、建立、存取、設定加密、修改`PublicAccessBlock`組態、設定其版本控制狀態，以及建立或取代 Strategy Recommendations 所使用之 S3 儲存貯體的生命週期組態。
- `secretsmanager`— 允許使用者存取「策略建議」所使用之 Secrets Manager 中的密碼。

若要檢視此策略的權限，請參閱AWS 受管理AWSMigrationHubStrategyCollector的策略參考指南中的。

AWS 受管理策略的策略建議更新

檢視由於此服務開始追蹤這些變更以來，策略建議的 AWS 受管原則更新詳細資訊。如需有關此頁面變更的自動警示，請訂閱「策略建議文件歷史記錄」頁面上的 RSS 摘要。

變更	描述	日期
AWSMigrationHubStrategyCollector – 更新現有政策	此原則已更新，以包含`PutLogData StartPortingCompatibilityAssessment GetPortingCompatibilityAssessment 、StartPortingRecommendationAssessment 和GetPortingRecommendationAssessment` 應用程式轉換動作，以允許應用程式轉換服務將記錄檔和指標傳送至服	2024年4月1日

變更	描述	日期
	務。亞馬遜簡單存儲服務（Amazon S3）添加GetBucketLocation 了和，以支持日誌和指標上傳。ListBucket 還新增PutMetricData 了PutLogData 和，以允許「策略建議」收集器將日誌和指標傳送到服務的端點。	
AWSMigrationHubStrategyCollector – 更新現有政策	此原則會使用PutMetricData 和動PutLogData 作更新。這些動作會授與應用程式轉換作業的上傳日誌和測量結果資料 此更新還新增條件，以確保等同aws:ResourceAccount 於使用隨附 Amazon 簡單儲存服務和 AWS Secrets Manager 動作的許可。aws:PrincipalAccount	2024年2月5 日
AWSMigrationHubStrategyCollector – 更新現有政策	此政策已使用下列 Amazon S3 API 進行更新 — CreateBucket PutEncryptionConfiguration PutBucketPublicAccessBlock 、PutBucketPolicy 、PutBucketVersioning 、和PutLifecycleConfiguration 。	2023 年 9 月 15 日
AWSMigrationHubStrategyCollector – 更新現有政策	此原則更新會授與允許分析原始程式碼的權限。	2023 年 3 月 8 日

變更	描述	日期
AWSMigrationHubStrategyConsoleFullAccess – 更新現有政策	此原則已更新為三個 AWS Application Discovery Service API — `DescribeConfigurations` `DescribeTags` 、和`ListConfigurations` 。	2022 年 11 月 10 日
AWSMigrationHubStrategyCollector – 更新現有政策	此原則會以`UpdateCollectorConfiguration` 動作更新。此動作會儲存收集器的組態，以便於擷取。	2022年9月7日
AWSMigrationHubStrategyConsoleFullAccess— 新政策在推出時提供	`AWSMigrationHubStrategyConsoleFullAccess` 授與使用者透過「策略建議」服務的完整存取權 AWS Management Console。	2021 年 10 月 25 日
AWSMigrationHubStrategyCollector— 新政策在推出時提供	`AWSMigrationHubStrategyCollector` 授與使用者對策略建議服務的存取權，以及與服務相關之 S3 儲存貯體的讀取/寫入存取權。它還授予 Amazon API Gateway 存取權，以便將日誌和指標上傳到 AWS，以及獲取登入資料的 AWS Secrets Manager 存取權。	2021 年 10 月 25 日

變更	描述	日期
AWSMigrationHubStrategyServiceRolePolicy— 新政策在推出時提供	`AWSMigrationHubStrategyServiceRolePolicy` 服務連結的角色原則提供對 AWS Migration Hub 和 AWS Application Discovery Service的存取。此政策還授予在 Amazon 簡單儲存服務 (Amazon S3) 中存放報告的許可。	2021 年 10 月 25 日
策略建議開始追蹤變更	策略建議開始追蹤其 AWS 受管理策略的變更。	2021 年 10 月 25 日

Migration Hub 策略建議的身分識別型原則範例

依預設，使用者和角色沒有建立或修改策略建議資源的權限。他們也無法使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 或 AWS API 來執行工作。若要授予使用者對其所需資源執行動作的許可，IAM 管理員可以建立 IAM 政策。然後，管理員可以將 IAM 政策新增至角色，使用者便能擔任這些角色。

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》中的建立 IAM 政策。

如需策略建議所定義之動作和資源類型的詳細資訊，包括每個資源類型的 ARN 格式，請參閱服務授權參考中的適用於 Migration Hub 策略建議的動作、資源和條件索引鍵。

主題

- 政策最佳實務
- 使用策略建議主控台
- 允許使用者檢視他們自己的許可
- 存取一個 Amazon S3 儲存貯體

政策最佳實務

以身分識別為基礎的政策會決定使用者是否可以在您的帳戶中建立、存取或刪除策略建議資源。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。如需詳細資訊，請參閱《IAM 使用者指南〉中的 AWS 受管政策或工作職能的AWS 受管政策。
- 套用最低權限許可：設定 IAM 政策的許可時，請僅授予執行任務所需的許可。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低許可許可。如需使用 IAM 套用許可的詳細資訊，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。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM JSON 政策元素：條件。
- 使用 IAM Access Analyzer 驗證 IAM 政策，確保許可安全且可正常運作 – IAM Access Analyzer 驗證新政策和現有政策，確保這些政策遵從 IAM 政策語言 (JSON) 和 IAM 最佳實務。IAM Access Analyzer 提供 100 多項政策檢查及切實可行的建議，可協助您編寫安全且實用的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的 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。若要在呼叫 API 操作時請求 MFA，請將 MFA 條件新增至您的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的設定 MFA 保護的 API 存取。

如需 IAM 中最佳實務的相關資訊，請參閱 IAM 使用者指南中的 IAM 安全最佳實務。

使用策略建議主控台

若要存取「Migration Hub 策略建議」主控台，您必須擁有最少一組權限。這些權限必須允許您列出和檢視有關 AWS 帳戶. 如果您建立比最基本必要許可更嚴格的身分型政策，則對於具有該政策的實體（使用者或角色）而言，主控台就無法如預期運作。

您不需要為僅對 AWS CLI 或 AWS API 進行呼叫的使用者允許最低主控台權限。反之，只需允許存取符合他們嘗試執行之 API 操作的動作就可以了。

若要確保使用者和角色仍可使用策略建議主控台，請同時將策略建議`ConsoleAccess`或`ReadOnly` AWS 受管理的原則附加至實體。如需詳細資訊，請參閱《IAM 使用者指南》中的新增許可到使用者。

允許使用者檢視他們自己的許可

此範例會示範如何建立政策，允許 IAM 使用者檢視附加到他們使用者身分的內嵌及受管政策。此原則包含在主控台上或以程式設計方式使用 AWS CLI 或 AWS API 完成此動作的權限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

存取一個 Amazon S3 儲存貯體

在此範例中，您想要授與 IAM 使用者存 AWS 帳戶 取其中一個 Amazon S3 儲存貯體的存取權限`examplebucket`。您也希望允許使用者新增、更新和刪除物件。

除了授予使用者 s3:PutObject、s3:GetObject 與 s3:DeleteObject 許可之外，政策也會授予 s3:ListAllMyBuckets、s3:GetBucketLocation 與 s3:ListBucket 許可。這些是主控台需要的額外許可。還需要 s3:PutObjectAcl 與 s3:GetObjectAcl 動作才能在主控台中複製、剪下與貼上物件。如需授與使用者權限並使用主控台測試權限的範例逐步解說，請參閱逐步解說範例：使用使用者政策控制值區的存取權。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"ListBucketsInConsole",
         "Effect":"Allow",
         "Action":[
            "s3:ListAllMyBuckets"
         ],
         "Resource":"arn:aws:s3:::*"
      },
      {
         "Sid":"ViewSpecificBucketInfo",
         "Effect":"Allow",
         "Action":[
            "s3:ListBucket",
            "s3:GetBucketLocation"
         ],
         "Resource":"arn:aws:s3:::examplebucket"
      },
      {
         "Sid":"ManageBucketContents",
         "Effect":"Allow",
         "Action":[
            "s3:PutObject",
            "s3:PutObjectAcl",
            "s3:GetObject",
            "s3:GetObjectAcl",
            "s3:DeleteObject"
         ],
         "Resource":"arn:aws:s3:::examplebucket/*"
      }
   ]
}
```

疑難排解 Migration Hub 策略建議識別與存取

使用下列資訊可協助您診斷並修正使用策略建議和 IAM 時可能會遇到的常見問題。

主題

我沒有在策略建議中執行動作的權限

如果 AWS Management Console 告訴您您沒有執行動作的授權，則您必須聯絡您的管理員以尋求協助。您的管理員是提供您使用者名稱和密碼的人員。

以下範例錯誤會在 `mateojackson` IAM 使用者嘗試使用主控台檢視虛構 *`my-example-widget`* 資源的詳細資訊，但卻沒有虛構 `migrationhub-strategy:`*`GetWidget`* 許可時發生。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 migrationhub-strategy:GetWidget on resource: my-example-widget
```

在此情況下，Mateo 會請求管理員更新他的政策，允許他使用 *`my-example-widget`* 動作存取 `migrationhub-strategy:`*`GetWidget`* 資源。

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，您必須更新原則，才能讓您將角色傳遞給策略建議。

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`嘗試使用主控台執行策略建議中的動作時，會發生下列範例錯誤。但是，動作請求服務具備服務角色授予的許可。Mary 沒有將角色傳遞至該服務的許可。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

在這種情況下，Mary 的政策必須更新，允許她執行 `iam:PassRole` 動作。

如果您需要協助，請聯絡您的 AWS 系統管理員。您的管理員提供您的登入憑證。

我想要檢視我的存取金鑰

在您建立 IAM 使用者存取金鑰後，您可以隨時檢視您的存取金鑰 ID。但是，您無法再次檢視您的私密存取金鑰。若您遺失了密碼金鑰，您必須建立新的存取金鑰對。

存取金鑰包含兩個部分：存取金鑰 ID (例如 `AKIAIOSFODNN7EXAMPLE`) 和私密存取金鑰 (例如 `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`)。如同使用者名稱和密碼，您必須一起使用存取金鑰 ID 和私密存取金鑰來驗證您的請求。就如對您的使用者名稱和密碼一樣，安全地管理您的存取金鑰。

> **Important**
>
> 請勿將您的存取金鑰提供給第三方，甚至是協助尋找您的標準使用者 ID。通過這樣做，您可能會讓某人永久訪問您的 AWS 帳戶.

建立存取金鑰對時，您會收到提示，要求您將存取金鑰 ID 和私密存取金鑰儲存在安全位置。私密存取金鑰只會在您建立它的時候顯示一次。若您遺失了私密存取金鑰，您必須將新的存取金鑰新增到您的 IAM 使用者。您最多可以擁有兩個存取金鑰。若您已有兩個存取金鑰，您必須先刪除其中一個金鑰對，才能建立新的金鑰對。若要檢視說明，請參閱《IAM 使用者指南》中的管理存取金鑰。

我是系統管理員，想要允許其他人存取策略建議

若要允許其他人存取策略建議，您必須為需要存取的人員或應用程式建立 IAM 實體 (使用者或角色)。他們將使用該實體的憑證來存取 AWS。然後，您必須將原則附加至實體，以便在策略建議中授與其正確權限。

若要立即開始使用，請參閱《IAM 使用者指南》中的建立您的第一個 IAM 委派使用者及群組。

我想讓我以外的人員存 AWS 帳戶 取我的策略建議資源

您可以建立一個角色，讓其他帳戶中的使用者或您組織外部的人員存取您的資源。您可以指定要允許哪些信任物件取得該角色。針對支援基於資源的政策或存取控制清單 (ACL) 的服務，您可以使用那些政策來授予人員存取您資源的許可。

如需進一步了解，請參閱以下內容：

- 若要瞭解策略建議是否支援這些功能，請參閱Migration Hub 策略建議如何與 IAM 搭配使用。

- 若要了解如何提供您所擁有資源 AWS 帳戶 的存取權，請參閱《IAM 使用者指南》中的另一個您擁有 AWS 帳戶 的 IAM 使用者提供存取權限。
- 若要了解如何將資源存取權提供給第三方 AWS 帳戶，請參閱 IAM 使用者指南中的提供第三方 AWS 帳戶 擁有的存取權。
- 若要了解如何透過聯合身分提供存取權，請參閱《IAM 使用者指南》中的將存取權提供給在外部進行身分驗證的使用者 (聯合身分)。
- 若要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 角色與資源型政策的差異。

針對策略建議使用服務連結角色

Migration Hub 策略建議使用 AWS Identity and Access Management (IAM) 服務連結角色。服務連結角色是直接連結至策略建議的唯一 IAM 角色類型。服務連結角色由策略建議預先定義，並包含服務代表您呼叫其他服 AWS 務所需的所有權限。

服務連結角色可讓您更輕鬆地設定策略建議，因為您不需要手動新增必要的權限。策略建議會定義其服務連結角色的權限，除非另有定義，否則只有策略建議可以擔任其角色。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。

如需其他支援服務連結角色之服AWS 務的相關資訊，請參閱搭配 IAM 使用的服務，並在服務連結角色欄中尋找具有是的服務。選擇具有連結的是，以檢視該服務的服務連結角色文件。

策略建議的服務連結角色權限

策略建議使用名為的服務連結角色，AWSServiceRoleForMigrationHubStrategy並將其與 AWSMigrationHubStrategyServiceRolePolicyIAM 政策相關聯 — 提供 AWS Migration Hub 和 AWS Application Discovery Service的存取權。此政策還授予在 Amazon 簡單儲存服務 (Amazon S3) 中存放報告的許可。

AWSServiceRoleForMigrationHubStrategy 服務連結角色信任下列服務以擔任角色：

- `migrationhub-strategy.amazonaws.com`

角色權限原則允許策略建議完成下列動作。

AWS Application Discovery Service 動作

```
discovery:ListConfigurations
```

```
discovery:DescribeConfigurations
```

AWS Migration Hub 動作

```
mgh:GetHomeRegion
```

Amazon S3 動作

```
s3:GetBucketAcl

s3:GetBucketLocation

s3:GetObject

s3:ListAllMyBuckets

s3:ListBucket

s3:PutObject

s3:PutObjectAcl
```

若要檢視此策略的權限，請參閱AWS 受管理AWSMigrationHubStrategyServiceRolePolicy的策略參考指南中的。

若要檢視此原則的更新記錄，請參閱AWS 受管理策略的策略建議更新。

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。

建立策略建議的服務連結角色

您不需要手動建立一個服務連結角色。當您同意允許 Migration Hub 在您的帳戶中建立服務連結角色 (SLR) 時 AWS Management Console，策略建議會為您建立服務連結角色。

若您刪除此服務連結角色，之後需要再次建立，您可以在帳戶中使用相同程序重新建立角色。當您同意允許 Migration Hub 在您的帳戶中建立服務連結角色 (SLR) 時，策略建議會再次為您建立服務連結角色。

編輯策略建議的服務連結角色

策略建議不允許您編輯AWSServiceRoleForMigrationHubStrategy服務連結角色。因為有各種實體可能會參考服務連結角色，所以您無法在建立角色之後變更角色名稱。不過，您可以使用策略建議主控台、CLI 或 API 編輯角色的說明。

刪除策略建議的服務連結角色

使用 IAM 手動刪除服務連結角色

使用 IAM 主控台或 AWS API 刪除 AWSServiceRoleForMigrationHubStrategy服務連結角色。 AWS CLI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。

刪除 AWSServiceRoleForMigrationHubStrategySLR 使用的策略建議資源時，您不能有任何執行中的評量 (產生建議的工作)。也無法執行背景評估。如果評估正在執行，則在 IAM 主控台中刪除 SLR 會失敗。如果 SLR 刪除失敗，您可以在所有背景工作完成後重試刪除作業。刪除單鏡反光相機之前，您不需要清理任何創建的資源。

策略建議服務連結角色的支援區域

策略建議支援在提供服務的所有區域中使用服務連結角色。如需詳細資訊，請參閱 AWS 區域與端點。

Migration Hub 戰略建議和介面 VPC 端點 (AWS PrivateLink)

您可以在 VPC 與 Migration Hub 政策建議之間建立私有連線，方法是在界面 VPC 端點。界面端點是採用 AWS PrivateLink 技術。搭配AWS PrivateLink，您可以私有方式存取政策建議 API 操作，無需透過網際網際網路閘道、NAT 裝置、VPN 連接或AWS Direct Connect連線。您的 VPC 中的實例不需要公有 IP 地址，即能與政策建議 API 操作通訊。Amazon 網路的 VPC 與政策建議之間的流量都會在 Amazon 網路的範圍內。

每個介面端點都是由您子網路中的一或多個彈性網路介面表示。

如需詳細資訊，請參閱「」介面 VPC 端點 (AWS PrivateLink)中的Amazon VPC User Guide。

策略建議 VPC 終端的注意事項

在設定界面 VPC 端點前，請務必檢界面端點屬性和限制和AWS PrivateLink配額中的Amazon VPC User Guide。

政策建議支援從您的 VPC 呼叫其所有 API 動作。若要使用所有政策建議，您必須建立 VPC 端點。

為政策建議建議建議建立介面 VPC 端點

您可以使用 Amazon VPC 主控台或AWS Command Line Interface(AWS CLI。如需詳細資訊，請參閱 Amazon VPC 使用者指南中的建立介面端點。

使用下列服務名稱建立政策建議的 VPC 端點：

- com.amazonaws.*region*.migrationhub-strategy

如果您對該端點使用私有 DNS，您可以使用其區域的預設 DNS 名稱向政策建議發出 API 請求。例如，您可以使用migrationhub-strategy.us-east-1.amazonaws.com。

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

為政策建議建議建議建立 VPC 端點政策

您可以將端點政策連接至控制存取政策的存取權限的 VPC 端點。此政策會指定下列資訊：

- 可執行動作的委託人。
- 可執行的動作。
- 可供執行這些動作的資源。

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

範例：政策建議動作的 VPC 端點政策

以下是政策建議的端點政策的範例。連接至端點後，此政策會針對所有資源上的所有委託人，授予列出的「政策建議」動作的存取權限。

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "migrationhub-strategy:ListContacts",
         ],
         "Resource":"*"
      }
   ]
}
```

Migration Hub 策略建議的合規性驗證

若要瞭解 AWS 服務 是否屬於特定規範遵循方案的範圍內，請參閱AWS 服務 遵循規範計劃方案中的，並選擇您感興趣的合規方案。如需一般資訊，請參閱AWS 規範計劃AWS。

您可以使用下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱下載中的報告中的 AWS Artifact。

您在使用時的合規責任取決 AWS 服務 於資料的敏感性、公司的合規目標以及適用的法律和法規。AWS 提供下列資源以協助遵循法規：

- 安全性與合規性快速入門指南 — 這些部署指南討論架構考量，並提供部署以安全性和合規性 AWS 為重點的基準環境的步驟。
- 在 Amazon Web Services 上架構 HIPAA 安全性與合規性 — 本白皮書說明公司如何使用建立符合 HIPAA 資格的應 AWS 用程式。

> **Note**
>
> 並非所有人 AWS 服務 都符合 HIPAA 資格。如需詳細資訊，請參閱 HIPAA 資格服務參照。

- AWS 合規資源AWS — 此工作簿和指南集合可能適用於您的產業和所在地。
- AWS 客戶合規指南 — 透過合規的角度瞭解共同的責任模式。這份指南總結了在多個架構 (包括美國國家標準技術研究所 (NIST)、支付卡產業安全標準委員會 (PCI) 和國際標準化組織 (ISO)) 中，保 AWS 服務 護指引並對應至安全控制的最佳實務。
- 使用AWS Config 開發人員指南中的規則評估資源 — 此 AWS Config 服務會評估您的資源組態符合內部實務、產業準則和法規的程度。
- AWS Security Hub— 這 AWS 服務 提供了內部安全狀態的全面視圖 AWS。Security Hub 使用安全控制，可評估您的 AWS 資源並檢查您的法規遵循是否符合安全業界標準和最佳實務。如需支援的服務和控制清單，請參閱 Security Hub controls reference。
- Amazon GuardDuty — 透過監控環境中的 AWS 帳戶可疑和惡意活動，藉此 AWS 服務 偵測您的工作負載、容器和資料的潛在威脅。 GuardDuty 可協助您因應各種合規性需求，例如 PCI DSS，滿足特定合規性架構所規定的入侵偵測需求。
- AWS Audit Manager— 這 AWS 服務 有助於您持續稽核您的 AWS 使用情況，以簡化您管理風險的方式，以及遵守法規和業界標準的方式。

使用其他 服務

本節將介紹其他AWS服務與 Migration Hub 策略建議交互。

主題

- 使用記錄策略建議 API 呼叫AWS CloudTrail

使用記錄策略建議 API 呼叫AWS CloudTrail

Migration Hub 策略建議與AWS CloudTrail，是一種提供記錄使用者、角色或AWS策略建議中的服務。CloudTrail 會捕獲戰略建議的 API 呼叫當作事件。該呼叫的捕獲包括從策略建議主控台進行的呼叫，以及對策略建議 API 操作發出的程式碼呼叫。

如果您建立追蹤記錄，就可以持續傳送 CloudTrail 事件至 Amazon S3 儲存儲體，包括策略建議的事件。即使您未設定追蹤，依然可以透過 CloudTrail 主控台中的 Event history (事件歷史記錄) 檢視最新事件。您可以使用由 CloudTrail 收集的資訊來判斷對策略建議提出的請求、提出請求的 IP 地址、提出請求的人員、提出請求的時間，以及其他詳細資訊。

若要進一步了解 CloudTrail，請參閱《AWS CloudTrail 使用者指南》。

CloudTrail 中的策略建議資訊

當您建立帳戶時，系統即會在 AWS 帳戶 中啟用 CloudTrail。此外，策略建議中發生活動時，系統便會將該活動記錄至 CloudTrail 事件，並將其他AWS服務事件事件歷史記錄。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「」使用 CloudTrail 蹤事件歷史記錄查看事件。

若要持續記錄事件，請AWS 帳戶（包括策略建議事件），請建立線索。追蹤能讓 CloudTrail 將日誌檔交付至 Amazon S3 儲存貯體。依預設，當您在主控台中建立追蹤時，該追蹤會套用至所有的 AWS 區域。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 CloudTrail 日誌中所收集的事件資料。如需詳細資訊，請參閱下列內容：

- 建立追蹤的概觀
- CloudTrail 支援的服務和整合
- 設定 CloudTrail 的 Amazon SNS 通知
- 接收多個區域的 CloudTrail 日誌檔案和接收多個帳戶的 CloudTrail 日誌檔案

CloudTrail 日誌檔支援將下列動作記錄為 CloudTrail 日誌檔的事件：

- 獲取應用程序組件策略
- 獲取應用程序組件詳細信息
- 獲取
- 獲取時間端口文件詢問
- 獲取產品組合引用
- 獲取產品組合摘要
- 獲取服務器詳細信息
- 獲取服務器策略
- 列出應用程序組件
- 列表收集者
- 列表文件詢問
- ListServers
- 推出組合引用
- 開始評估
- 起始時間文件詢問
- 停止評估
- 更新應用程序組件配置
- 更新服務器配置

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：

- 該請求是否使用根或 AWS Identity and Access Management (IAM) 使用者登入資料提出
- 提出該請求時，是否使用了特定角色或聯合身分使用者的暫時安全登入資料
- 該請求是否由另一項 AWS 服務提出

如需詳細資訊，請參閱 CloudTrail userIdentity 元素。

了解策略建議案日誌檔案項目

追蹤是一種組態，能讓事件以日誌檔案的形式交付到您指定的 Amazon S3 儲存貯體。CloudTrail 日誌檔包含一或多個日誌項目。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 CloudTrail 的是展示獲取服務器詳細信息動作。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "777777777777",
        "arn": "arn:aws:sts::111122223333:assumed-role/myUserName/...",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "777777777777",
                "arn": "arn:aws:iam::111122223333:role/myUserName",
                "accountId": "111122223333",
                "userName": "myUserName"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2021-09-20T01:07:16Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2021-09-20T01:07:43Z",
    "eventSource": "migrationhub-strategy.amazonaws.com",
    "eventName": "GetServerDetails",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "",
    "userAgent": "",
    "requestParameters": {
        "serverId": "ads-server-006"
    },
    "responseElements": null,
    "requestID": "07D681279BD94AED",
    "eventID": "cdc4b7ed-e171-4cef-975a-ad829d4123e8",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
```

```
    "eventCategory": "Management"
}
```

Migration Hub 策略的配額建議

對於每個 AWS 服務，您的 AWS 帳戶有預設配額，先前稱為限制。除非另有說明，否則每個配額都是區域特定規定。您可以要求提高某些配額，而其他配額無法提高。

若要查看 Migration Hub 策略建議的配額列表，請參閱策略建議服務配額。

您也可以通過打開Service Quotas 控制台。在導覽窗格中，選擇AWS服務，然後選擇Migration Hub 戰略建議。

若要請求增加配額，請參閱 Service Quotas 使用者指南中的請求提高配額。如果 Service Quotas 中尚未提供配額，請使用增加服務配額表單。

版本備註

主題

2023 年 11 月 17 日

新功能

- 收藏家
- Support .NET 8 應用程式。

2023 年 10 月 12 日

新功能

- 收藏家

- Support 多資料來源。

2023 年 4 月 17 日

新功能

- 收藏家
- 升級腳本增強功能。這需要最新版本的收集器。

2023 年 3 月 17 日

新功能

新增二進位分析，提供反模式與不相容性偵測，而無需原始碼。

2022年11月7日

新功能

- 應用程式篩選
- 依AWS Application Discovery Service標籤篩選伺服器

2022 年 9 月 27 日

新功能

- 收藏家
  - 索引標準測試版本 667
  - 空氣分析儀 2.2.0.368
- 新增伺服器見解的`diag check`命令。
- 已新增對潛在建議的支援。
- 增強的用戶界面，可檢查配置和評估狀態。

錯誤修正

- 移植助理翻譯和其他修復程序。

2022 年 6 月 30 日

新功能

- 收藏家
  - 新增 VMware API 支援。
  - A2C 在下載二進製文件時請求更改以添加用戶標頭。
  - 增加了 Linux 主路徑，默認外殼和所有 shell 的遠程終止。
- 公共二進制
  - 已新增 Azure DevOps 做為管線部署目標的支援。

2022 年 4 月 18 日

新功能

- 收藏家
- 新增從公用 URL 動態下載 A2C 二進位檔的功能。

錯誤修正

- A2C

2022 年 2 月 25 日

錯誤修正

- SCT V5.6.9
- A2C
- 收藏家

2022 年 2 月 10 日

錯誤修正

- SCT v5.6.8

- A2C
  - 在 Linux 上添加了對該tar命令的檢查。
  - 修復了在 Amazon ECR 中檢查應用程序映像的問題。
  - 修正需要移除容器以進行預先驗證的問題。
- 收藏家
  - 修復了遠程 32 位計算機的 4xx 錯誤。
  - 更新了 A2C 錯誤代碼。
  - 驗證中的 IP 位址，以C#便分析遠端機器的原始程式碼。

2022 年 1 月 28 日

新功能

- 收藏家
- 已新增 Azure DevOps Git 儲存庫的原始程式碼分析支援。

2022 年 1 月 14 日

新功能

- 收藏家
- 已新增 SQL 資料庫的巴別魚建議。

2021 年 12 月 21 日

問題已解決

- 收藏家
- 資料庫分析已恢復。

2021 年 12 月 15 日

已知問題

- 收藏家
- 目前不支援資料庫分析 (CVE-2021-44228)。

2021 年 10 月 25 日

新功能

- 收集器
- Migration Hub 策略建議使用者指南的初始版本。

文件和版本記錄

下表說明「策略建議」的文件版本。如需詳細資訊，請參閱 版本備註。

變更	Description	日期
AWS 受管策略更新-更新至 AWSMigrationHubStrategyCollector	已更新AWSMigrationHubStrategyCollector策略以包含新的s3application-transformation 、和migrationhub-strategy 動作。	2024年4月1日
AWS 受管策略更新-更新至 AWSMigrationHubStrategyCollector	已更新AWSMigrationHubStrategyCollector政策以包含新application-transformation 動作。此更新還新增條件，以限制各種動作，其中aws:ResourceAccount 必須等於aws:PrincipalAccount .	2024年2月5 日
新功能	策略建議應用程式資料收集器用戶端 v1.1.47 可支援 .NET 8 應用程式。	2023 年 11 月 17 日
新功能	策略建議應用程式資料收集器用戶端 v1.1.45 可支援多個資料來源。	2023 年 10 月 12 日
AWS 受管策略更新-更新至 AWSMigrationHubStrategyCollector	更新政AWSMigrationHubStrategyCollector策以包含新的 Amazon S3 API。	2023 年 9 月 15 日
AWS 受管策略更新-更新至 AWSMigrationHubStrategyCollector	已更新原AWSMigrationHubStrategyCollector則，以包含新的原始程式碼分析器。	2023 年 3 月 8 日

IAM 最佳實務更新	如需更多詳細資訊，請參閱 IAM 中的安全最佳實務。	2023年2月25日
AWS 受管策略更新-現有策略的更新	Migration Hub 策略建議將三個 AWS Application Discovery Service API 新增至現有原則。	2022 年 11 月 10 日
安全性更新	建立與介面 VPC 端點的私人連線。	2022年3月7日
新功能	已新增 Azure DevOps Git 儲存庫的原始程式碼分析支援。	2022 年 1 月 28 日
新功能	已新增 SQL 資料庫的巴別魚建議。	2022 年 1 月 14 日
初始版本	Migration Hub 策略建議使用者指南的初始版本。	2021 年 10 月 25 日

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。