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 策略建議為應用程式的可行轉換路徑提供遷移和現代化策略建議，協助規劃遷移和現代化措施。

策略建議可以分析您的伺服器庫存、執行期環境，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，以允許 Strategy Recommendations 執行所有應用程式的原始程式碼和資料庫分析。Strategy Recommendations 會將此分析與您的業務目標，以及您提供建議的應用程式和資料庫的轉換偏好設定進行比較：

- 每個應用程式最有效的遷移策略。
- 您可以使用的遷移和現代化工具或服務。
- 要針對特定選項解析的應用程式不相容和反模式。

Migration Hub Strategy Recommendations 建議遷移和現代化策略，以重新託管、轉譯和重構相關聯的部署目的地、工具和程式。如需有關重新託管、轉譯和重構的資訊，請參閱 AWS 規範性指導詞彙表中的遷移術語 - 7 Rs。

策略建議可能會建議直接的選項，例如使用 AWS Application Migration Service (AWS MGN) 在 Amazon Elastic Compute Cloud (Amazon EC2) 上重新託管。更最佳化的建議可能包括使用 AWS App2Container 對容器進行複寫，或對 .NET Core 和 PostgreSQL 等開放原始碼技術進行重構。

您是第一次使用策略建議客戶嗎？

如果這是您第一次使用策略建議，建議您先閱讀以下章節：

- 策略建議概觀
- 設定策略建議
- 策略建議入門

策略建議概觀

您可以從 AWS Migration Hub 主控台使用 Migration Hub Strategy Recommendations，開始評估您的伺服器和應用程式產品組合。您可以使用 主控台來設定和執行評估。評估之後，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的清單，您可以使用策略建議來評估您的應用程式原始碼和資料庫。

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 主控台來存取 Migration Hub Strategy Recommendations 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 – 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資料。
- AWS Application Migration Service - AWS Application Migration Service 是建議用於lift-and-shift遷移至 的主要遷移服務 AWS。
- AWS Database Migration Service – AWS Database Migration Service 是一種 Web 服務，可用來將資料從內部部署、Amazon Relational Database Service (Amazon RDS) 資料庫執行個體或 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體上的資料庫中遷移到服務 AWS 上的資料庫。
- AWS App2Container – AWS App2Container (A2C) 是命令列工具，可將 .NET 和 Java 應用程式現代化為容器化應用程式。
- 適用於 .NET 的 Porting Assistant – 用於 .NET 原始程式碼分析。Porting Assistant for .NET 是一種相容性掃描器，可減少將 Microsoft .NET Framework 應用程式移植到 .NET Core 所需的手動工作。.NET 的 Porting Assistant 會評估 .NET 應用程式原始碼，並識別不相容APIs 和第三方套件。
- 適用於 Windows Server End-of-Support遷移計劃 – 適用於 Windows Server End-of-Support遷移計劃 (EMP) 包含將舊版應用程式從 Windows Server 2003、2008 和 2008 R2 遷移到其上較新的支援版本的工具 AWS，無需任何重構。
- AWS Schema Conversion Tool – 您可以使用 AWS Schema Conversion Tool (AWS SCT)，將現有的資料庫結構描述從一個資料庫引擎轉換為另一個。
- Windows Web Application Migration Assistant – 適用於 的 Windows Web Application Migration Assistant AWS Elastic Beanstalk 是互動式 PowerShell 公用程式，可將 ASP.NET 和 ASP.NET Core 應用程式從內部部署 IIS Windows 伺服器遷移至 Elastic Beanstalk。
- Babelfish for Aurora PostgreSQL – Babelfish for Aurora PostgreSQL 是 Amazon Aurora PostgreSQL 相容版本的新功能，可讓 Aurora 了解針對 Microsoft SQL 伺服器寫入之應用程式的命令。

設定策略建議

首次使用 Migration Hub 策略建議之前，請先完成下列任務：

主題

註冊 AWS 帳戶

如果您沒有 AWS 帳戶，請完成下列步驟來建立一個。

註冊 AWS 帳戶

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

   部分註冊程序需接收來電或簡訊，並在電話鍵盤輸入驗證碼。

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

AWS 會在註冊程序完成後傳送確認電子郵件給您。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。

建立具有管理存取權的使用者

註冊 後 AWS 帳戶，請保護 AWS 帳戶根使用者、啟用 AWS IAM Identity Center和建立 管理使用者，以免將根使用者用於日常任務。

保護您的 AWS 帳戶根使用者

1. 選擇根使用者並輸入 AWS 帳戶 您的電子郵件地址，以帳戶擁有者AWS Management Console身分登入 。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)。

   如需說明，請參閱《IAM 使用者指南》中的為您的 AWS 帳戶 根使用者 （主控台） 啟用虛擬 MFA 裝置。

建立具有管理存取權的使用者

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 Identity Center 中，將管理存取權授予使用者。

   如需使用 IAM Identity Center 目錄 做為身分來源的教學課程，請參閱AWS IAM Identity Center 《 使用者指南》中的使用預設值設定使用者存取 IAM Identity Center 目錄。

以具有管理存取權的使用者身分登入

- 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 Identity Center 使用者登入的說明，請參閱AWS 登入 《 使用者指南》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 Identity Center 中，建立一個許可集來遵循套用最低權限的最佳實務。

   如需指示，請參閱《AWS IAM Identity Center 使用者指南》中的建立許可集。

2. 將使用者指派至群組，然後對該群組指派單一登入存取權。

   如需指示，請參閱《AWS IAM Identity Center 使用者指南》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，請建立同時連接 AWSMigrationHubFullAccess和 AWSMigrationHubStrategyConsoleFullAccess受管政策的角色。
- 若要存取策略建議應用程式資料收集器，請建立已連接 AWSMigrationHubStrategyCollector受管政策的角色。

IAM 受管政策會定義使用者對服務的存取層級。AWSMigrationHubFullAccess 受管 AWS Migration Hub 政策會授予 Migration Hub 主控台的存取權。如需詳細資訊，請參閱 Migration Hub 角色和政策。如需 AWSMigrationHubStrategyConsoleFullAccess和 AWSMigrationHubStrategyCollector受管政策的相關資訊，請參閱 AWS Migration Hub 策略建議的 受管政策。

若要提供存取權，請新增權限至您的使用者、群組或角色：

- 中的使用者和群組 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。遵循「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。
- 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。
  - (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。

策略建議入門

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。

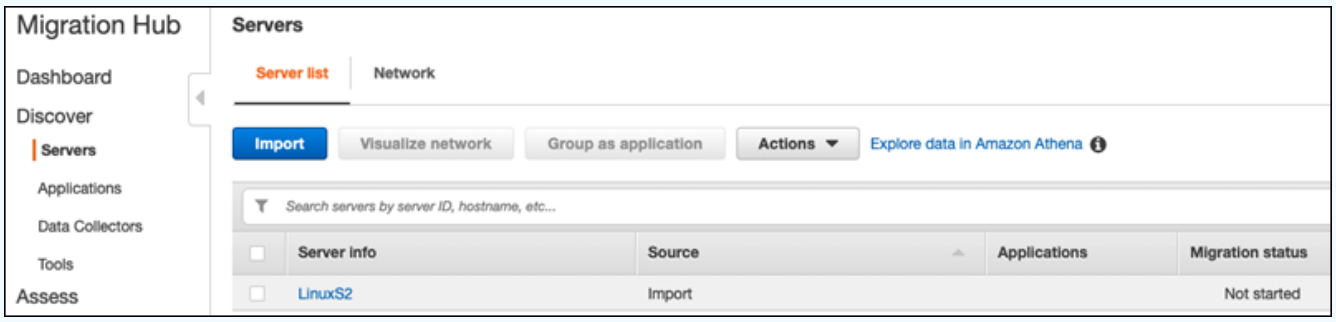
- 您必須有一或多個 AWS 帳戶，且使用者為這些帳戶設定 。如需詳細資訊，請參閱設定策略建議。
- Strategy Recommendations 應用程式資料收集器用戶端必須能夠從伺服器遠端收集資料。這需要您使用一組適用於所有 Windows 伺服器的登入資料，以及一組適用於所有 Linux 伺服器的登入資料。登入資料必須具有在您的伺服器中建立和刪除目錄的許可。
- 在 vCenter 中部署的收集器版本支援 VMware vCenter Server V6.0、V6.5、6.7 或 7.0。

  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 12.04、14.04、16.04、18.04、20.04
    - Red Hat Enterprise Linux 5.11、6.10、7.3、7.7、8.1
    - CentOS 5.11、6.9、7.3
    - SUSE 11 SP4、12 SP5
  - Windows

  - Windows Server 2008 R1 SP2、2008 R2 SP1
  - Windows Server 2012 R1、2012 R2
  - Windows Server 2016
  - Windows Server 2019
- 對於原始碼分析，您的 GitHub 和 GitHub Enterprise 儲存庫必須具有個人存取字符，其具有可與 Strategy Recommendations 收集器用戶端共用的儲存庫範圍。如需使用儲存庫範圍建立個人存取權杖的詳細資訊，請參閱 GitHub 文件中的建立個人存取權杖。

  若要分析適用於 .NET 建議的 Porting Assistant 的 .NET 儲存庫，您必須提供使用適用於 .NET 連接埠評估工具的 Porting Assistant 設定的 Windows 機器。如需詳細資訊，請參閱《適用於 .NET 的 Porting Assistant 使用者指南》中的適用於 .NET 的 Porting Assistant 入門。
- 若要啟用資料庫分析的策略建議，您必須在 中輸入登入資料 AWS Secrets Manager。如需詳細資訊，請參閱策略建議資料庫分析。
- 在使用策略建議之前，您必須使用 AWS Application Discovery Service 在 AWS Migration Hub 主控台中收集伺服器和應用程式的資料。您可以使用下列其中一種方法來收集資料。
  - Migration Hub 匯入 – 使用 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《應用程式探索服務使用者指南》中的遷移中樞匯入。
  - AWS Application Discovery Service Agentless Collector – Agentless Collector 是一種 VMware 設備，可收集 VMware 虛擬機器 VMs) 的相關資訊。如需詳細資訊，請參閱《Application Discovery Service 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 – Discovery Agent 是您安裝在內部部署伺服器和VMs上的 AWS 軟體，用於擷取系統間網路連線的系統資訊和詳細資訊。如需詳細資訊，請參閱《AWS Application Discovery Service 使用者指南》中的 Application Discovery Agent。
- 策略建議資料收集器 – 如果您的伺服器託管在 VMware vCenter 中，而且您提供存取權，則策略建議可以自動擷取您的伺服器庫存。Strategy Recommendations 主控台將使用收集的資訊來協助評估。

> **Note**
>
> 若要驗證 Migration Hub 匯入是否成功完成，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 Strategy Recommendations 應用程式資料收集器是一種虛擬設備，您可以在內部部署 VMware 環境中安裝。Strategy Recommendations 應用程式資料收集器也可以做為 Amazon Machine Image (AMI) 使用。如果您想要使用收集器的 AMI 版本來評估 AWS 應用程式或基於其他原因，則不需要下載收集器。您可以略過本節，並前往 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 Open Virtualization Archive (OVA) 檔案，用來將收集器部署為 VMware 環境中的虛擬機器 (VM)。

下載收集器 OVA 檔案

1. 使用您在 中建立的 AWS 帳戶設定策略建議，登入 AWS Management Console 並開啟位於 https：//https://console.aws.amazon.com/migrationhub/ 的 Migration Hub 主控台。
2. 在 Migration Hub 主控台導覽窗格中，選擇策略。
3. 在遷移中樞策略建議頁面上，選擇下載資料收集器。
4. 或者，如果您想要匯入應用程式資料，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 Strategy Recommendations 應用程式資料收集器。應用程式資料收集器是無代理程式的資料收集器，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 VMware vCenter Server 中部署為虛擬機器 (VM)。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 AWS 的應用程式，您可以使用策略建議收集器 Amazon Machine Image (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 Strategy Recommendations 應用程式資料收集器是一種虛擬設備，您可以在內部部署 VMware 環境中安裝。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 Server 環境中部署策略建議收集器。

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 檔案包含收集器和 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 VM 採用下列規格。

策略建議收集器 VM 規格

- RAM – 至少 8 GB
- CPUs – 至少 4 個

> **Note**
>
> 為了確保您使用最新版本的收集器搭配所有新功能和錯誤修正，請在部署收集器 OVA 檔案後升級收集器。如需如何升級的說明，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

如果您有想要評估 AWS 的應用程式，您可以使用 Strategy Recommendations 應用程式資料收集器 Amazon Machine Image (AMI)。

下列程序說明如何從收集器 AMI 啟動 Amazon EC2 執行個體。

部署收集器 Amazon 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 中的策略建議端點AWS 一般參考。
3. 在導覽窗格中，在影像下選擇 AMIs。
4. 從「由我擁有」下拉式清單中選擇公有映像。
5. 選擇搜尋列，然後從功能表中選取 AMI 名稱。
6. 輸入名稱 AWSMHubApplicationDataCollector。
7. 為了確保 AMI 來自安全來源，請確認帳戶的擁有者為 703163444405。
8. 若要從此 AMI 啟動執行個體，請選取執行個體，然後選擇啟動。如需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 Amazon EC2 執行個體採用下列規格。

   策略建議收集器 Amazon EC2 執行個體規格

   - RAM – 至少 8 GB
   - CPUs – 至少 4 個

策略建議 AMI 包含收集器和 CLI，可用於存取策略建議 API。

> **Note**
>
> 為了確保您使用最新版本的收集器搭配所有新功能和錯誤修正，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。如需如何升級的說明，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 Strategy Recommendations 應用程式資料收集器。登入收集器的方式取決於您部署的方式。

- 登入部署在 vCenter 型環境中的收集器
- 登入部署為 Amazon EC2 執行個體的收集器

登入部署在 vCenter 型環境中的收集器

登入部署在 vCenter 型環境中的策略建議收集器

1. 使用下列命令，使用 SSH 用戶端連線至收集器。

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

2. 出現密碼提示時，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

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，使用 SSH 用戶端連線至收集器。

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

Keyname.pem 是在您從收集器 AMI 啟動 Amazon EC2 執行個體時產生的私有金鑰。

步驟 4：設定策略建議收集器

本節說明如何使用命令列`collector setup`命令來設定 Migration Hub Strategy Recommendations 應用程式資料收集器。這些組態存放在本機。

您必須先使用下列`collector setup`命令，在收集器 Docker 容器中建立 bash shell 工作階段，才能使用`docker exec`命令。

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

`collector setup` 命令會連續執行下列所有命令，但您可以個別執行這些命令：

- `collector setup --aws-configurations` – 設定 AWS 組態。
- `collector setup --vcenter-configurations` – 設定 vCenter 組態。

> **Note**
>
> 只有在集合器託管在 vCenter 上時，才能使用 vCenter 組態設定。不過，您可以使用命令 強制設定 vCenter 組態`collector setup --vcenter-configurations`。

- `collector setup --remote-server-configurations` – 設定遠端伺服器組態。
- `collector setup --version-control-configurations` – 設定版本控制組態。

同時設定所有收集器組態

1. 輸入以下命令。

```
collector setup
```

2. 輸入 AWS 組態的資訊，如 中所述設定 AWS 組態。
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. 輸入版本控制組態的資訊，如中所述設定版本控制組態。
6. 遵循 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您的遠端 Windows 和 Linux 伺服器以進行資料收集。

設定 AWS 組態

若要設定 AWS 組態，請使用 `collector setup`命令或 `collector setup --aws-configurations`命令。

1. 輸入 Y 表示是，表示是否設定 IAM 許可...問題。當您依照 中的步驟，建立使用 `AWSMigrationHubStrategyCollector` 受管政策存取收集器的使用者時，您可以設定這些許可策略建議使用者和角色。
2. 依照 中的步驟，輸入您建立來存取收集器之使用者 AWS 的帳戶中的存取金鑰和私密金鑰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 中的策略建議端點AWS 一般參考。
4. 將上傳收集器相關指標上傳到遷移中樞策略服務？問題輸入 Y 表示是。指標資訊可協助您 AWS 獲得適當的支援。
5. 上傳收集器相關日誌到遷移中樞策略服務？問題，請輸入 Y 表示是。日誌中的資訊可協助您 AWS 獲得適當的支援。

下列範例顯示顯示的內容，包括組態的範例項目 AWS 。

```
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，使用 collector setup命令或 collector setup --vcenter-configurations命令時：

1. 輸入 Y 表示是。如果您想要使用 VMware vCenter 登入資料進行身分驗證，是否要使用 VMware vCenter 登入資料問題進行身分驗證。

> **Note**
>
> 使用 VMware vCenter 登入資料進行驗證時，需要在目標伺服器上安裝 VMware 工具。

輸入 Host Url，可以是 vCenter IP 地址或 URL。然後，輸入 VMware vCenter 的使用者名稱和密碼。

2. 如果您想要設定 Windows 伺服器，請在 VMware VMware vCenter 問題中，輸入 Y 表示是。

   輸入 Windows 的使用者名稱和密碼。

   > **Note**
   >
   > 如果您的 Windows Remote Server 屬於 Active Directory 網域，則必須在使用 CLI 提供遠端伺服器組態時，將使用者名稱輸入為 *domain-name**username*。例如，如果您的網域名稱是範例網域，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是範例網域\管理員。

3. 如果您想要設定 Linux 伺服器，請使用 VMware vCenter 問題輸入 Linux 設定 Y for yes。VMware vCenter

   輸入 Linux 的使用者名稱和密碼。

4. 輸入 Y 表示是。如果您想要為 vCenter 外部的伺服器設定遠端伺服器憑證，您是否想要使用 NTLM for Windows 和 SSH/Cert based for Linux 問題來設定 vCenter 外部的伺服器憑證。

5. 對於 您是否希望使用與 vCenter 設定問題期間相同的 Windows 登入資料，如果在 vCenter 外部管理的 Windows 機器登入資料與設定 vCenter Windows 機器登入資料時提供的登入資料相同，請輸入 Y for yes。否則，請輸入 N 表示否。

   如果您回答是 Y，則會詢問下列問題。

   a. 輸入 Y 表示同意 收集器在第一次與 Windows 伺服器互動期間接受和本機儲存伺服器憑證是否正常？問題。

   b. 如果您想要設定 SSH 身分驗證，請在 輸入您的選項問題中輸入 1。

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

下列範例顯示顯示的內容，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，使用 `collector setup`命令或 `collector setup --remote-server-configurations`命令時：

1. 輸入 Y 表示是。如果您想要設定 Windows 伺服器，是否要使用 NLTM for Windows 問題為非 vCenter 管理的伺服器設定登入資料。

   輸入 WinRM 的使用者名稱和密碼。

   > **Note**
   >
   > 如果您的 Windows Remote Server 屬於 Active Directory 網域，則必須在使用 CLI 提供遠端伺服器組態時，將使用者名稱輸入為 *domain-name**username*。例如，如果您的網域名稱是範例網域，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是範例網域\管理員。

輸入 Y 表示 是 。在第一次與 Windows 伺服器互動期間，您是否可以接受收集器並代表您本機儲存伺服器憑證？問題。Windows Server 憑證存放在 目錄中/opt/amazon/application-data-collector/remote-auth/windows/certs。

您必須將產生的伺服器憑證複製到 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. 如果您想要設定 Linux 伺服器，請使用 SSH 或 Cert 問題在 Linux 設定中為是輸入 Y。
3. 如果您想要設定 SSH 金鑰型身分驗證，請在 輸入您的選項問題中輸入 1。

   如果您選擇使用 SSH 身分驗證，則必須將產生的金鑰憑證複製到 Linux 伺服器。如需詳細資訊，請參閱在 Linux 伺服器上設定金鑰型身分驗證。
4. 如果您想要設定 以進行以憑證為基礎的身分驗證，請在 輸入您的選項問題中輸入 2。

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

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，使用 `collector setup`命令或 `collector setup --version-control-configurations`命令時：

1. 在設定原始碼分析？問題中輸入 Y 表示是。
2. 如果您想要設定 Git 伺服器端點，請在輸入選項問題中輸入 1。

   輸入 GIT 伺服器端點的 github.com。
3. 如果您想要設定 GitHub Enterprise Server，請在 輸入您的選項問題中輸入 2。

   輸入不含 https：// 的企業端點，如下所示：GIT 伺服器端點：*git-enterprise-endpoint*
4. 輸入您的 Git *#####*和個人存取權*#*。
5. 輸入 Y 表示 是。您是否有任何 csharp 儲存庫應該在 Windows 機器上分析？如果您想要分析 C# 程式碼，請提問。

   > **Note**
   >
   > 若要分析適用於 .NET 建議的 Porting Assistant 的 .NET 儲存庫，您必須提供使用適用於 .NET 連接埠評估工具的 Porting Assistant 設定的 Windows 機器。如需詳細資訊，請參閱《適用於 .NET 的 Porting Assistant 使用者指南》中的適用於 .NET 的 Porting Assistant 入門。
6. 對於 是否要在此機器上重複使用現有的 Windows 登入資料？問題。如果 Windows Machine for C# 原始碼分析使用與先前在設定 `--remote-server-configurations`或 時提供的登入資料相同的登入資料，請輸入 Y for yes`--vcenter-configurations`。

如果您想要輸入新的登入資料，請輸入 N 表示否。

7. 若要使用 VMWare vCenter Windows Machine 登入資料，請在選擇下列其中一個 Windows 登入資料選項時輸入 1。
8. 輸入 Windows 機器的 IP 地址。

下列範例顯示顯示的內容，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...
```

準備您的遠端 Windows 和 Linux 伺服器以進行資料收集

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

設定遠端伺服器組態之後，如果您使用 `collector setup command`或 `collector setup --remote-server-configurations`命令，則必須準備遠端伺服器，以便 Strategy Recommendations 應用程式資料收集器可以從中收集資料。

> **Note**
>
> 您必須確定可使用其私有 IP 地址來連線伺服器。如需如何在 上透過虛擬私有雲端 (VPC) 設定環境 AWS 以進行遠端執行的進一步說明，請參閱 Amazon Virtual Private Cloud 使用者指南。

若要準備遠端 Linux 伺服器，請參閱 準備遠端 Linux 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 Linux 伺服器

在 Linux 伺服器上設定金鑰型身分驗證

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

在 Linux 伺服器上設定金鑰型身分驗證

1. 從容器中的下列資料夾複製以名稱 id_rsa_ assessment.pub 產生的公有金鑰：

   /opt/amazon/application-data-collector/remote-auth/linux/keys。
2. 在所有遠端機器的 `$HOME/.ssh/authorized_keys` 檔案中附加複製的公有金鑰。如果沒有可用的檔案，請使用 `touch`或 `vim`命令建立該檔案。
3. 請確定遠端伺服器上的主資料夾具有許可層級`755`或更少。如果是 `777`，則無法運作。您可以使用 `chmod`命令來限制許可。

在 Linux 伺服器上設定憑證型身分驗證

如果您在設定遠端伺服器組態時選擇為 Linux 設定憑證型身分驗證，則必須執行下列步驟，以便 Strategy Recommendations 應用程式資料收集器可以收集資料。

如果您已經為應用程式伺服器設定憑證授權機構 (CA)，建議您使用此選項。

在 Linux 伺服器上設定憑證型身分驗證

1. 複製適用於所有遠端伺服器的使用者名稱。

2. 將收集器的公有金鑰複製到 CA。

   您可以在下列位置找到收集器的公有金鑰：

   /opt/amazon/application-data-collector/remote-auth/linux/keys/id_rsa_assessment.pub

   必須將此公有金鑰新增至您的 CA 以產生憑證。
3. 將上一個步驟產生的憑證複製到收集器中的下列位置：

   /opt/amazon/application-data-collector/remote-auth/linux/keys

   憑證的名稱必須是 id_rsa_assessment-cert.pub。
4. 在設定步驟期間提供憑證檔案名稱。

在 Windows 伺服器上設定遠端伺服器組態

如果您選擇在收集器設定中設定遠端伺服器組態時設定 Windows，則必須執行下列步驟，以便 Strategy Recommendations 收集資料。

> 若要進一步了解在遠端伺服器上執行的 PowerShell 指令碼，請閱讀此備註。
>
> 指令碼會啟用 PowerShell 遠端，並停用交涉以外的所有身分驗證方法。這用於 Windows NT LAN Manager (NTLM)，並將 "AllowUnencrypted" WSMan 通訊協定設定為 false，以確保新建立的接聽程式只接受加密的流量。使用 Microsoft 提供的指令碼 `New-SelfSignedCertificateEx.ps1`建立自我簽署憑證。
> 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 建立傳入防火牆規則。在最後一個步驟中，WinRM 服務會重新啟動。

在 Windows 2008 伺服器上透過遠端連線設定資料收集

1. 使用下列命令來檢查安裝在伺服器上的 PowerShell 版本。

   ```
   $PSVersionTable
   ```
2. 如果 PowerShell 版本不是 5.1，請依照 Microsoft 文件中的安裝和設定 WMF 5.1 的指示下載並安裝 WMF 5.1。
3. 在新的 PowerShell 視窗中使用以下命令，以確保 PowerShell 5.1 已安裝。

```
$PSVersionTable
```

4. 請遵循下一組步驟，其中說明如何在 Windows 2012 及更高版本上透過遠端連線設定資料收集。

在 Windows 2012 和更新版本的伺服器上透過遠端連線設定資料收集

1. 從下列 URL 下載設定指令碼：

   https://application-data-collector-release.s3.us-west-2.amazonaws.com/scripts/WinRMSetup.ps1

2. `New-SelfSignedCertificateEx.ps1` 從下列 URL 下載 ，並將指令碼貼到您下載 的相同資料夾`WinRMSetup.ps1`：

   https://github.com/Azure/azure-libraries-for-net/blob/master/Samples/Asset/New-SelfSignedCertificateEx.ps1

3. 若要完成設定，請在所有應用程式伺服器上執行下載的 PowerShell 指令碼。

   ```
   .\WinRMSetup.ps1
   ```

> **Note**
>
> 如果 Windows Remote Management (WinRM) 未在 Windows Remote Server 上正確設定，則從該伺服器收集資料的嘗試將會失敗。如果發生這種情況，您必須從容器上的下列位置刪除對應至該伺服器的憑證：
> /opt/amazon/application-data-collector/remote-auth/windows/certs/***ads-server-id***.cer
> 刪除憑證後，請等待重試資料收集程序。

確認您的收集器和伺服器已設定用於資料收集

使用以下命令，確認您的收集器和伺服器已正確設定資料收集。

```
collector diag-check
```

此命令會對伺服器組態執行一組診斷檢查，並對失敗的檢查提供輸入。

當您在 `-a` 模式下使用 命令時，您可以在檢查完成後，在 DiagnosticCheckResult.txt 檔案中取得輸出。

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

您可以對具有該伺服器的 IP 地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。

Linux 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.
```

Windows 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.
```

下列範例顯示錯誤訊息，會在遠端伺服器登入資料不正確時顯示。

```
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：在 Migration Hub 主控台中使用策略建議來取得建議

本節說明如何在 Migration Hub 主控台中使用 Strategy Recommendations 來首次取得遷移建議。

取得建議

1. 使用您在 中建立的 AWS 帳戶設定策略建議，登入 AWS Management Console 並開啟位於 https：//https://console.aws.amazon.com/migrationhub/ 的 Migration Hub 主控台。
2. 在 Migration Hub 主控台導覽窗格中，選擇策略。
3. 在遷移中樞策略建議頁面上，選擇取得建議。
4. 若您同意允許 Migration Hub 在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VMs 相關資訊。使用此選項，您不需要執行額外的設定。

        ii. 手動匯入：如果您想要獨立匯入伺服器和應用程式的資料，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 VMs 的可用資訊。

        iii. Application Discovery Service – 您可以使用 Application Discovery Service 來收集內部部署應用程式和伺服器的相關資訊。在遷移中樞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 Application Discovery Service Agentless Collector、AWS Discover Agent 或 Import （適用於 CSV 檔案）。

b. 伺服器資料表會根據您在資料來源區段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下，會列出您已設定的應用程式資料收集器。如果您尚未設定任何資料收集器，您可以下載資料收集器，然後部署它。如需詳細資訊，請參閱 步驟 1：下載策略建議收集器 和 步驟 2：部署策略建議收集器。

> **Note**
>
> 若要取得策略建議，您必須設定至少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。您可以稍後再新增其他資料來源。

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. 針對匯入名稱，輸入匯入的名稱。

f. 針對 S3 儲存貯體 URI，輸入要上傳匯入 JSON 檔案的 S3 儲存貯體 URI。

> **Important**
>
> S3 儲存貯體名稱必須以 的字首開頭**migrationhub-strategy**。

g. 選擇 Next (下一步)。

6. 指定偏好設定

a. 在指定偏好設定頁面上，設定您的業務目標和遷移偏好設定。Strategy Recommendations 建議根據您指定的偏好設定遷移和現代化應用程式和資料庫的最佳策略。您可以稍後再變更這些偏好設定。

b. 選擇 Next (下一步)。

7. 檢閱並提交。

a. 檢閱您設定的資料來源和遷移偏好設定。

b. 如果一切看起來都正確，請選擇開始資料分析。這將分析您的伺服器庫存和執行期環境，以及 Microsoft IIS 和 Java 應用程式的應用程式二進位檔。

> **Note**
>
> 二進位分析的狀態不會在主控台中顯示。當分析完成時，您會看到反模式報告的連結，或指出分析未成功的訊息。

策略建議建議

本節說明如何檢視遷移產品組合中伺服器和應用程式的策略建議遷移和現代化建議。

主題

在策略建議中檢視策略建議

本節說明如何在 AWS Migration Hub 主控台中使用策略建議來檢視遷移策略建議。

檢視策略建議

1. 使用您在 中建立 AWS 的帳戶設定策略建議，登入 AWS Management Console 並開啟位於 https：//https://console.aws.amazon.com/migrationhub/ 的 Migration Hub 主控台。
2. 在 Migration Hub 主控台導覽窗格中，選擇策略，然後選擇建議。
3. 在建議頁面上，您可以檢視和匯出產品組合的摘要建議，以及詳細的遷移「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。

   反模式是依嚴重性分類的產品組合中發現的已知問題清單。高嚴重性反模式表示需要解決的不相容，中嚴重性反模式表示警告，低嚴重性反模式表示資訊性問題。如需 "R" 策略的資訊，請參閱 AWS 規範性指導詞彙表中的遷移術語 - 7 R。

   - 如果您的資料中心發生變更，或如果您更新偏好設定，建議您重新分析資料。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以是先前資料和新資料的混合。

     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，您可以檢視遷移產品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 應用程式元件建議。
5. 在伺服器索引標籤上，您可以檢視遷移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. 在偏好設定索引標籤上，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 策略建議偏好設定。

策略建議 應用程式元件建議

本節說明如何在 Migration Hub 主控台中使用策略建議來檢視和分析應用程式元件的遷移策略建議。

主題

- 在策略建議中使用應用程式元件
- 策略建議原始程式碼分析
- 策略建議資料庫分析
- 策略建議二進位分析

在策略建議中使用應用程式元件

本節說明如何在 Migration Hub 主控台中使用 Migration Hub 策略建議來檢視和設定遷移和現代化策略建議。

主題

- 檢視應用程式元件建議
- 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議

本節說明如何在 Migration Hub 主控台中使用策略建議來檢視應用程式元件的遷移策略建議。

檢視應用程式元件的建議詳細資訊

1. 使用您在 中建立 AWS 的帳戶設定策略建議，登入 AWS Management Console 並開啟位於 https：//https://console.aws.amazon.com/migrationhub/ 的 Migration Hub 主控台。
2. 在 Migration Hub 主控台導覽窗格中，選擇策略，然後選擇建議。
3. 在建議頁面上，選擇應用程式元件索引標籤。

    a. 在應用程式元件摘要下， 是您在伺服器產品組合中執行的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、元件類型和遷移 "R" 策略建議。您也可以檢視遷移目的地，以及用於伺服器產品組合中執行之各種應用程式元件的遷移和現代化工具。如需有關 "R" 策略的資訊，請參閱 AWS 規範性指導詞彙表中的遷移術語 - 7 個 R。

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. 在建議摘要下的應用程式元件詳細資訊頁面（以元件名稱做為標題的頁面），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。反模式是依嚴重性分類的產品組合中發現的已知問題清單。
6. 選擇策略選項索引標籤，以檢視應用程式元件的遷移建議。您可以透過選取不同的策略，然後選擇設定偏好來覆寫建議的策略。
7. 根據您正在檢視的應用程式元件類型，有來源組態或資料庫組態索引標籤。如需來源組態的詳細資訊，請參閱 設定應用程式元件的原始程式碼分析。如需資料庫組態的相關資訊，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

本節說明如何在 Migration Hub 主控台中使用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 主控台導覽窗格中，選擇策略，然後選擇建議。
2. 在建議頁面上，選擇應用程式元件索引標籤。
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訊。
4. 在應用程式元件詳細資訊頁面上（以元件名稱做為標題的頁面），選擇來源碼組態索引標籤。
5. 在來源碼組態詳細資訊下，選擇分析來源碼。
6. 在分析來源碼頁面上，提供儲存應用程式元件來源碼的儲存庫名稱、分支名稱和專案名稱（如適用）。選取您要使用的 GitHub 原始程式碼版本控制類型，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上檢視更新後的建議。

如需來源碼分析的詳細資訊，請參閱 策略建議原始程式碼分析。

設定應用程式元件的資料庫分析

本節說明如何在 Migration Hub 主控台中使用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 主控台導覽窗格中，選擇策略，然後選擇建議。
2. 在建議頁面上，選擇應用程式元件索引標籤。
3. 從應用程式元件下的元件清單中，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上（以元件名稱做為標題的頁面），選擇資料庫組態索引標籤。
5. 在資料庫組態詳細資訊下，選擇分析資料庫詳細資訊。
6. 從您在 Secrets Manager 中 AWS 建立用於資料庫登入資料的下拉式選單中選擇秘密名稱，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上檢視更新後的建議。

如需資料庫分析和設定秘密名稱的詳細資訊，請參閱 策略建議資料庫分析。

策略建議原始程式碼分析

Migration Hub 策略建議會自動識別您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，則會將其識別為元件類型為 Java 的應用程式元件。

策略建議會在您設定應用程式元件時分析其原始程式碼。如需設定應用程式元件以進行原始程式碼分析的詳細資訊，請參閱 設定應用程式元件的原始程式碼分析。

策略建議會針對 Java 和 C# 程式設計語言執行原始程式碼分析。

如需使用策略建議原始程式碼分析的先決條件資訊，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，則會將其識別為應用程式元件 sqlservr.exe。

策略建議會使用 AWS Schema Conversion Tool，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至 AWS 資料庫時的不相容，例如 Amazon Aurora MySQL 相容版本、Amazon Aurora PostgreSQL 相容版本、Amazon RDS for MySQL 和 Amazon RDS for PostgreSQL。

目前，Strategy Recommendations 資料庫分析僅適用於 SQL Server。

若要設定策略建議來分析資料庫，您必須提供策略建議應用程式資料收集器的登入資料，才能連線至資料庫。若要這樣做，請在您 AWS 帳戶中的 AWS Secrets Manager 中建立秘密。

如需有關您提供的登入資料的許可和權限的資訊，請參閱 AWS Schema Conversion Tool 登入資料所需的權限。如需使用 登入資料建立秘密的詳細資訊，請參閱 在 Secrets Manager 中為資料庫登入資料建立秘密。

設定登入資料和秘密之後，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後，會排程 a AWS Schema Conversion Tool 清查任務。此任務完成後，您會看到為該資料庫伺服器上的每個個別資料庫建立新的應用程式元件。例如，如果您的 SQL Server 有兩個資料庫 (exampledbs1 和 exampledbs2)，則會為名稱為 exampledbs1 和 exampledbs2 的每個資料庫建立應用程式元件。

如果您想要在將每個已識別的資料庫遷移至 AWS 資料庫時看到反模式，請依照中的步驟設定每個資料庫的分析設定應用程式元件的資料庫分析。

AWS Schema Conversion Tool 登入資料所需的權限

您提供給 AWS Secrets Manager 的登入憑證僅需要 `VIEW SERVER STATE` 和 `VIEW ANY DEFINITION` 權限。

您可以在建立 SQL Server 登入時，提供您想要的任何登入名稱和密碼。

在 Secrets Manager 中為資料庫登入資料建立秘密

登入資料準備好讓策略建議應用程式資料收集器連線至資料庫後，請在您 AWS 帳戶中的 AWS Secrets Manager 中建立秘密，如下列程序所述。

在 AWS 帳戶中使用 AWS Secrets Manager 建立秘密

1. 使用您在 中建立 AWS 的帳戶設定策略建議，登入 AWS Management Console 並開啟 AWS Secrets Manager 主控台，網址為 https：//https://console.aws.amazon.com/secretsmanager/。
2. 選擇儲存新機密。
3. 選取秘密類型做為其他類型的秘密。
4. 在鍵/值對下，輸入下列資訊。

   username - *your-username*

然後選擇 + 新增列，然後輸入下列資訊。

password - ####

5. 選擇下一步。
6. 輸入秘密名稱做為任何字首為 migrationhub-strategy- 的字串。例如， migrationhub-strategy-one。

> **Note**
>
> 將您的秘密名稱存放在安全的地方，以供日後使用。

7. 選擇下一步，然後再次選擇下一步。
8. 選擇儲存。

您可以在策略建議中設定資料庫分析時，使用您為資料庫登入資料建立的秘密。

策略建議二進位分析

Migration Hub 策略建議會自動識別您產品組合中的應用程式，以及屬於它們的應用程式元件。例如，如果您的產品組合中有 Java 應用程式，Strategy Recommendations 會將其識別為具有元件類型 java 的應用程式元件。如果不設定對原始程式碼的存取，策略建議可以執行二進位分析。 透過檢查 Windows 上的 IIS 應用程式 DLLs或 Linux 上的應用程式 JAR 檔案，並提供反模式報告或不相容報告。反模式報告是策略建議在您的產品組合中發現的已知問題清單，依嚴重性分類。不相容報告包含反模式的子集，即 API 相容性、模組套件和移植動作。

策略建議會針對 Windows IIS、Java Tomcat 和 Jboss 應用程式執行分析。如果您有 IIS 應用程式，Strategy Recommendations 預設會產生不相容的報告；您必須設定原始碼存取，才能接收完整的反模式報告。如果您有 Java 應用程式，根據預設，策略建議會產生完整的反模式報告。

不相容或反模式報告會在分析完成後顯示。如果分析不成功，您可以嘗試執行原始程式碼分析，方法是提供原始程式碼存取，如 中所述設定版本控制組態。

策略建議 伺服器建議

本節說明如何在 Migration Hub 主控台中使用 Migration Hub 策略建議，來檢視遷移產品組合中伺服器的遷移策略建議。

檢視伺服器的建議

1. 使用您在 中建立 AWS 的帳戶設定策略建議，登入 AWS Management Console 並開啟位於 https：//https://console.aws.amazon.com/migrationhub/ 的 Migration Hub 主控台。
2. 在 Migration Hub 主控台導覽窗格中，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，您可以檢視您在產品組合中執行的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訊，以及遷移 "R" 策略建議。您也可以檢視遷移目的地，以及根據建議在伺服器上識別的反模式數量。如需 "R" 策略的相關資訊，請參閱 AWS 規範性指導詞彙表中的遷移術語 - 7 個 R。
4. 若要檢視伺服器的深入建議詳細資訊，請從清單中選擇伺服器，然後選擇檢視詳細資訊。您可以檢視為伺服器收集的中繼資料，以及其深入分析和建議，這些都是以伺服器上執行的應用程式元件為基礎。
5. 在伺服器詳細資訊頁面 （以伺服器名稱做為標題的頁面） 的建議摘要下，您可以查看伺服器的策略建議概觀。您也可以檢視已識別的反模式。反模式是依嚴重性分類的產品組合中發現的已知問題清單。
6. 選擇策略選項索引標籤，以檢視伺服器的遷移建議。您可以透過選取不同的策略，然後選擇設定偏好來覆寫建議的策略。
7. 選擇應用程式元件索引標籤，以檢視與伺服器相關聯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，請從清單中選擇元件，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。

策略建議偏好設定

本節說明如何在 Migration Hub 主控台中檢視和編輯 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. 使用您在 中建立 AWS 的帳戶設定策略建議，登入 AWS Management Console 並開啟位於 https：//https://console.aws.amazon.com/migrationhub/ 的 Migration Hub 主控台。
2. 在 Migration Hub 主控台導覽窗格中，選擇策略，然後選擇建議。
3. 在建議頁面上，選擇偏好設定索引標籤。

4. 在優先順序業務目標下，您可以拖放業務目標來重新排列目標。
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

本節說明如何在 中檢視策略建議資料來源 AWS Management Console。

檢視資料來源

1. 使用您在 中建立 AWS 的帳戶設定策略建議，登入 AWS Management Console 並開啟位於 https：//https://console.aws.amazon.com/migrationhub/ 的 Migration Hub 主控台。
2. 在 Migration Hub 主控台導覽窗格中，選擇策略，然後選擇資料來源。
3. 在收集器索引標籤上，您可以檢視您設定的策略建議應用程式資料收集器。如需收集器的詳細資訊，請參閱 策略建議應用程式資料收集器。
4. 在匯入索引標籤上，您可以匯入資料並檢視資料匯入。如需詳細資訊，請參閱將資料匯入策略建議。
5. 在工具索引標籤上，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集器

本節說明如何使用策略建議應用程式資料收集器。

如需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無代理程式的資料收集器，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
作業系統類型	Windows 或 Linux
作業系統版本	作業系統的特定版本。例如，Windows Server 2003、RHEL 5.2。
作業系統架構	32 位元或 64 位元作業系統
是伺服器 VM	伺服器是 VM 或實體機器。
虛擬化軟體	例如，vCenter、Hyper-V。
位置	例如，Amazon Elastic Compute Cloud 主控台 (Amazon EC2) 或內部部署。
是 dualBoot	允許開機至多個OSs
韌體類型	BIOS、UEFI
開機載入器	GRUB、GRUB 2
分割區資料表類型	MBR、GPT
CPU 速度	CPU 速度，以 GHz 為單位。例如，2.4 GHz。
Windows OS data	
Windows Edition	標準、資料中心、企業
.NET 架構版本	已安裝的 .NET 架構版本。
.NET Core 版本	已安裝的 .NET Core 版本。
Linux data	
Linux 作業系統發行版本	RHEL、CentOS、SUSE 等。

資料欄位	描述
核心版本	uname -r 輸出，例如 `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。
磁碟區大小	磁碟大小總計
磁碟區可用空間	可用磁碟空間
虛擬磁碟映像格式	vmdk、vhd、vhdx
磁碟類型 (Windows)	基本、動態
Application level data	
應用程式名稱	執行中程序的名稱。例如，SQLServr.exe,MS dtsservr.exe, 等。
應用程式類型	IIS、JBoss、Tomcat 等。
程式設計語言和版本	C#、Java
JDK 版本	安裝的 JDK 版本。
來源碼是否可用	如果您提供原始碼儲存庫，則表示有可用的原始碼。
應用程式位元大小	16 位元、32 位元、64 位元
Windows	
應用程式使用的 .NET 架構版本	要在應用程式執行時間載入的 .NET 架構 DLL 版本。
.NET Core 版本	要在應用程式執行時間載入的 .NET Core DLL 版本。

資料欄位	描述
使用 WPF 架構 ？	決定以 .NET 為基礎的應用程式是否為 WPF 應用程式類型。
使用 WCF 架構 ？	決定以 .NET 為基礎的應用程式是否為 WCF 應用程式類型。
ASP.NET 版本	ASP.NET 的版本。
IIS 版本	Windows 機器上安裝的 IIS 伺服器版本。
應用程式作業系統驅動程式位元大小	32 位元、64 位元
Windows 登錄檔用量	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 DLLs	擷取 Windows 程序在執行時間載入的所有 DLLs 清單。
PowerShell 版本	檢查安裝在機器上的 PowerShell 版本，應為 5.1 或更新版本。
Linux	
應用程式架構類型	Tomcat、Spring Boot、JBoss、WebLogic、WebSphere
應用程式架構版本	應用程式架構的版本。
Database	
資料庫類型	MS SQL、Oracle、MySQL 等。
資料庫版本	資料庫的版本。

從策略建議中移除您的資料

若要從策略建議中移除所有資料，請聯絡 AWS 支援並請求完整刪除資料。

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。

升級策略建議收集器

1. 使用下列命令，使用 SSH 用戶端連線至收集器 VM。

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

2. 變更為收集器 VM 中的升級目錄，如下列範例所示。

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

3. 使用下列命令來執行升級指令碼。

```
sudo 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，您也可以匯入您要遷移和現代化建議之應用程式和伺服器的相關資訊。

當您匯入資料時，建議不會像使用資料收集器時那樣深入。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。

匯入資料

1. 使用您在 中建立 AWS 的帳戶設定策略建議，登入 AWS Management Console 並開啟位於 https：//https://console.aws.amazon.com/migrationhub/ 的 Migration Hub 主控台。
2. 在 Migration Hub 主控台導覽窗格中，選擇策略，然後選擇資料來源。
3. 選擇匯入索引標籤。
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至 Amazon S3 儲存貯體。確定儲存貯體的名稱開頭為字首 `migrationhub-strategy`。

6. 返回匯入索引標籤，然後選擇匯入。
7. 輸入匯入的名稱，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，如下列範例所示。

```
{
    "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，資料欄位的有效值會列在下表中。

伺服器的必要欄位列在下表中。

名稱	Description (描述)	Type	必要	有效值
ResourceId	資源的唯一 ID	字串	是	任何唯一的字串
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」、「程序」
OSDistribution	Windows、Windows Server、Ubuntu	字串	是	Windows：「Windows PC」、「Windows Server」 Linux："Ubuntu"、"RHEL"、"Amazon Linux"、"DEBIAN"、"SLES"、"CENT_OS"、"ORACLE_LINUX"、"FEDORA"、"KALI"
OSType	作業系統的類型	字串	是	"Windows"、"Linux"
OSVersion	核心版本	字串	是	請參閱文件的 HTML 版本。
CPUArchitecture	CPU 架構	字串	否	"32 位元"、"64 位元"
IpAddress	伺服器 IP 地址	陣列	否	格式為 https：//xxx.xxx.xxx.xxx
MacAddresses	與伺服器相關聯的 Mac 地址	陣列	否	格式為 xx：xx：xx：xx：xx：xx
Hostname (主機名稱)	主機的名稱	字串	否	任何字串

程序的必要欄位列在下表中。

名稱	Description (描述)	Type	必要	有效值
ResourceId	資源的唯一 ID	字串	是	任何唯一的字串
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」、「程序」
AssociatedServerIds	正在執行程序 IDs 清單。	字串	是	您定義的「ResourceType」：「SERVER」中的 ResourceId。
ApplicationType	應用程式類型	字串	是	"Tomcat"、"JBoss"、"Spring"、"IIS"、"Mongo 資料庫"、"DB2"、"Maria 資料庫"、"MySQL"、"Oracle"、"SQLServer"、"Sybase"、"PostgreSQL Server"、"Cassandra"、"IBM WebSphere"、"Oracle WebLogic"、"Java Generic"
ApplicationVersion	應用程式版本	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 7.5」、「IIS 8.0」、「IIS 8.5」、「IIS 10.0」
ProgrammingLanguage	應用程式的程式設計語言	字串	否	"Java"、"CSharp"

名稱	Description (描述)	Type	必要	有效值
DotNetFrameworkVersion	如果應用程式是以 .NET Framework 為基礎的 .NET Framework 版本	字串	否	「DotnetFramework 1.0」，「DotnetFramework 1.0 SP1」，「DotnetFramework 1.0 SP2」，「DotnetFramework 1.0 SP3」，「DotnetFramework 1.1」，「DotnetFramework 1.1 SP1」，「DotnetFramework 2.0」，「DotnetFramework 2.0 SP1」，「DotnetFramework 2.0 SP2」，「DotnetFramework 3.0」，「DotnetFramework 3.0 SP1」，「DotnetFramework 3.0 SP2」，「DotnetFramework 3.5」，「DotnetFramework 3.5 SP1」，「DotnetFramework 4.0」，「DotnetFramework 4.5」，「DotnetFramework 4.5.1」，「DotnetFramework 4.5.2」，「DotnetFramework 4.6」，「DotnetFramework 4.6.1」，「DotnetFramework 4.6.2」，「DotnetFramework 4.7」，「DotnetFramework 4.7.1」，「DotnetFramework 4.7.2」，「DotnetFramework 4.8」

名稱	Description (描述)	Type	必要	有效值
DotNetCoreVersion	如果應用程式是以 .NET Core 為基礎的 .NET Core 版本	字串	否	".NET Core 1.0"、".NET Core 1.1"、".NET Core 2.0"、".NET Core 2.1"、".NET Core 2.2"、".NET Core 3.0"、".NET Core 3.1"
JdkVersion	如果應用程式使用 JDK，則為 JDK 的版本	字串	否	"JDK1.0"、"JDK2.0"、"JDK3.0"、...、"JDK11.0"
DatabaseType	類型資料庫	字串	否	"SQLServer"、"Oracle"、"Sybase"、"Mongo 資料庫"、"Maria 資料庫"、"Apache Cassandra"、"MySQL"、"IBM DB2"、"PostgreSQLServer"
DatabaseEdition	資料庫的版本	字串	否	
DatabaseVersion	資料庫的版本	字串	否	請參閱文件的 HTML 版本。

從策略建議中移除您的資料

若要從 Migration Hub 策略建議中移除所有資料，請聯絡 AWS 支援。

Migration Hub 策略建議的安全性

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

安全性是 AWS 和 之間的共同責任。共同責任模型將其描述為雲端的安全性和雲端中的安全性：

- 雲端的安全性 – AWS 負責保護在 中執行 AWS 服務的基礎設施 AWS 雲端。 AWS 也為您提供可安全使用的服務。第三方稽核人員會定期測試和驗證我們的安全有效性，做為AWS 合規計畫的一部分。若要了解適用於 Migration Hub 策略建議的合規計劃，請參閱AWS 合規計劃範圍內的服務。
- 雲端的安全性 – 您的責任取決於您使用 AWS 的服務。您也必須對其他因素負責，包括資料的機密性、您公司的要求和適用法律和法規。

本文件可協助您了解如何在使用策略建議時套用共同責任模型。下列主題說明如何設定策略建議，以符合您的安全和合規目標。您也會了解如何使用其他 AWS 服務來協助您監控和保護 Strategy Recommendations 資源。

主題

- Migration Hub 策略建議中的資料保護
- Migration Hub 策略建議的身分和存取管理
- Migration Hub 策略建議的合規驗證

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 的全域基礎設施 AWS 雲端。您負責維護在此基礎設施上託管內容的控制權。您也同時負責所使用 AWS 服務 的安全組態和管理任務。如需資料隱私權的詳細資訊，請參閱資料隱私權常見問答集。如需有關歐洲資料保護的相關資訊，請參閱 AWS 安全性部落格上的 AWS 共同的責任模型和 GDPR 部落格文章。

基於資料保護目的，我們建議您保護 AWS 帳戶 登入資料，並使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 設定個別使用者。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 設定 API 和使用者活動記錄 AWS CloudTrail。如需有關使用 CloudTrail 追蹤擷取 AWS 活動的資訊，請參閱AWS CloudTrail 《 使用者指南》中的使用 CloudTrail 追蹤。
- 使用 AWS 加密解決方案，以及其中的所有預設安全控制 AWS 服務。
- 使用進階的受管安全服務 (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 AWS 透過命令列界面或 API 存取 時需要 FIPS 140-3 驗證的密碼編譯模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的更多相關資訊，請參閱聯邦資訊處理標準 (FIPS) 140-3。

我們強烈建議您絕對不要將客戶的電子郵件地址等機密或敏感資訊，放在標籤或自由格式的文字欄位中，例如名稱欄位。這包括當您使用 Strategy Recommendations 或使用 AWS 服務 主控台、API AWS CLI或其他 時 AWS SDKs 。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

存放在 Strategy Recommendations 資料庫中的所有資料都會加密。

傳輸中加密

策略建議 網際網路通訊支援所有元件和用戶端之間的 TLS 1.2 加密。

Migration Hub 策略建議的身分和存取管理

AWS Identity and Access Management (IAM) 是 AWS 服務 ，可協助管理員安全地控制對 AWS 資源的存取。IAM 管理員可控制誰可以進行身分驗證 （ 登入 ） 和授權 （ 具有許可 ），以使用策略建議資源。IAM 是您可以免費使用 AWS 服務 的 。

主題

- 目標對象
- 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 受管政策

- Migration Hub 策略建議的身分型政策範例
- 對 Migration Hub 策略建議身分和存取進行故障診斷
- 針對策略建議使用服務連結角色
- Migration Hub 策略建議和界面 VPC 端點 (AWS PrivateLink)

目標對象

您使用 AWS Identity and Access Management (IAM) 的方式會有所不同，取決於您在策略建議中所做的工作。

服務使用者 – 如果您使用策略建議服務來執行任務，您的管理員會為您提供所需的登入資料和許可。當您使用更多策略建議功能來執行工作時，您可能需要額外的許可。了解存取許可的管理方式可協助您向管理員請求正確的許可。如果您無法存取策略建議中的功能，請參閱 對 Migration Hub 策略建議身分和存取進行故障診斷。

服務管理員 – 如果您在公司負責策略建議資源，您可能擁有策略建議的完整存取權。您的任務是判斷服務使用者應存取的策略建議功能和資源。接著，您必須將請求提交給您的 IAM 管理員，來變更您服務使用者的許可。檢閱此頁面上的資訊，了解 IAM 的基本概念。若要進一步了解貴公司如何使用 IAM 搭配策略建議，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，建議您了解撰寫政策以管理策略建議存取權的詳細資訊。若要檢視您可以在 IAM 中使用的 Strategy Recommendations 身分型政策範例，請參閱 Migration Hub 策略建議的身分型政策範例。

使用身分驗證

身分驗證是您 AWS 使用身分憑證登入 的方式。您必須以 AWS 帳戶根使用者身分、IAM 使用者身分或擔任 IAM 角色來驗證 （登入 AWS)。

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

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

如果您以 AWS 程式設計方式存取 ， AWS 會提供軟體開發套件 (SDK) 和命令列界面 (CLI)，以使用您的 憑證以密碼編譯方式簽署您的請求。如果您不使用 AWS 工具，則必須自行簽署請求。如需

使用建議的方法自行簽署請求的詳細資訊，請參閱《IAM 使用者指南》中的適用於 API 請求的AWS Signature 第 4 版。

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

AWS 帳戶 根使用者

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

聯合身分

最佳實務是， 要求人類使用者，包括需要管理員存取權的使用者，使用臨時 AWS 服務 憑證與身分提供者聯合來存取 。

聯合身分是來自您的企業使用者目錄、Web 身分提供者、 AWS Directory Service、 Identity Center 目錄或任何使用透過身分來源提供的登入資料 AWS 服務 存取的使用者。當聯合身分存取時 AWS 帳戶，它們會擔任 角色，而角色會提供臨時登入資料。

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，也可以連接並同步到您自己的身分來源中的一組使用者 AWS 帳戶 和群組，以便在所有 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 中的身分 AWS 帳戶 ，具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。如需更多資訊，請參閱 IAM 使用者指南中的為需要長期憑證的使用案例定期輪換存取金鑰。

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

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

IAM 角色

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

使用臨時憑證的 IAM 角色在下列情況中非常有用：

- 聯合身分使用者存取 — 如需向聯合身分指派許可，請建立角色，並為角色定義許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並獲授予由角色定義的許可。如需有關聯合角色的相關資訊，請參閱《IAM 使用者指南》中的為第三方身分提供者 (聯合) 建立角色。如果您使用 IAM Identity Center，則需要設定許可集。為控制身分驗證後可以存取的內容，IAM Identity Center 將許可集與 IAM 中的角色相關聯。如需有關許可集的資訊，請參閱 AWS IAM Identity Center 使用者指南中的許可集。
- 暫時 IAM 使用者許可 – IAM 使用者或角色可以擔任 IAM 角色來暫時針對特定任務採用不同的許可。
- 跨帳戶存取權：您可以使用 IAM 角色，允許不同帳戶中的某人 (信任的主體) 存取您帳戶的資源。角色是授予跨帳戶存取權的主要方式。不過，對於某些 AWS 服務，您可以直接將政策連接到資源（而不是使用角色做為代理）。如需了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱《IAM 使用者指南》中的 IAM 中的跨帳戶資源存取。
- 跨服務存取 – 有些 AWS 服務 使用其他 中的功能 AWS 服務。例如，當您在服務中進行呼叫時，該服務通常會在 Amazon EC2 中執行應用程式或將物件儲存在 Amazon Simple Storage Service (Amazon S3) 中。服務可能會使用呼叫主體的許可、使用服務角色或使用服務連結角色來執行此作業。
  - 轉送存取工作階段 (FAS) – 當您使用 IAM 使用者或角色在其中執行動作時 AWS，您會被視為委託人。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 使用呼叫 的委託人許可 AWS 服務，結合 AWS 服務 請求向下游服務提出請求。只有在服務收到需要與其他 AWS 服務 或 資源互動才能完成的請求時，才會提出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出 FAS 請求時的政策詳細資訊，請參閱《轉發存取工作階段》。
  - 服務角色 – 服務角色是服務擔任的 IAM 角色，可代表您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需詳細資訊，請參閱《IAM 使用者指南》中的建立角色以委派許可權給 AWS 服務。

- 服務連結角色 – 服務連結角色是一種連結至 的服務角色。 AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會出現在您的 中 AWS 帳戶 ，並由服務擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。
- 在 Amazon EC2 上執行的應用程式 – 您可以使用 IAM 角色來管理在 EC2 執行個體上執行之應用程式的臨時登入資料，以及提出 AWS CLI 或 AWS API 請求。這是在 EC2 執行個體內儲存存取金鑰的較好方式。若要將 AWS 角色指派給 EC2 執行個體並將其提供給其所有應用程式，您可以建立連接至執行個體的執行個體描述檔。執行個體設定檔包含該角色，並且可讓 EC2 執行個體上執行的程式取得臨時憑證。如需詳細資訊，請參閱《IAM 使用者指南》中的使用 IAM 角色來授予許可權給 Amazon EC2 執行個體上執行的應用程式。

使用政策管理存取權

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

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

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

IAM 政策定義該動作的許可，無論您使用何種方法來執行操作。例如，假設您有一個允許 `iam:GetRole` 動作的政策。具有該政策的使用者可以從 AWS Management Console AWS CLI、 或 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。如需了解如何建立身分型政策，請參閱《IAM 使用者指南》中的透過客戶管理政策定義自訂 IAM 許可。

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

資源型政策

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

資源型政策是位於該服務中的內嵌政策。您無法在資源型政策中使用來自 IAM 的 AWS 受管政策。

存取控制清單 (ACL)

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

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

其他政策類型

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

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

階段政策的交集。許可也可以來自資源型政策。所有這類政策中的明確拒絕都會覆寫該允許。如需詳細資訊，請參閱 IAM 使用者指南中的工作階段政策。

多種政策類型

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

Migration Hub 策略建議如何與 IAM 搭配使用

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

可與 Migration Hub 策略建議搭配使用的 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

若要全面了解策略建議和其他 AWS 服務如何與大多數 IAM 功能搭配使用，請參閱《IAM 使用者指南》中的AWS 與 IAM 搭配使用的 服務。

策略建議的身分型政策

支援身分型政策：是

身分型政策是可以附加到身分 (例如 IAM 使用者、使用者群組或角色) 的 JSON 許可政策文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。如需了解如何建立身分型政策，請參閱《IAM 使用者指南》中的透過客戶管理政策定義自訂 IAM 許可。

使用 IAM 身分型政策，您可以指定允許或拒絕的動作和資源，以及在何種條件下允許或拒絕動作。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。

策略建議的身分型政策範例

若要檢視策略建議身分型政策的範例，請參閱 Migration Hub 策略建議的身分型政策範例。

策略建議中的資源型政策

支援資源型政策：否

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

如需啟用跨帳戶存取權，您可以指定在其他帳戶內的所有帳戶或 IAM 實體，做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。當委託人和資源位於不同位置時 AWS 帳戶，信任帳戶中的 IAM 管理員也必須授予委託人實體 （使用者或角色） 存取資源的許可。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 中的快帳戶資源存取。

策略建議的政策動作

支援政策動作：是

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼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。政策動作通常具有與相關聯 AWS API 操作相同的名稱。有一些例外狀況，例如沒有相符的 API 操作的僅限許可動作。也有一些作業需要政策中的多個動作。這些額外的動作稱為相依動作。

政策會使用動作來授予執行相關聯動作的許可。

若要查看策略建議動作清單，請參閱服務授權參考中的 Migration Hub 策略建議定義的動作。

策略建議中的政策動作在動作之前使用下列字首：

```
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"
         ]
```

若要檢視策略建議身分型政策的範例，請參閱 Migration Hub 策略建議的身分型政策範例。

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 ARNs，請參閱《服務授權參考》中的 Migration Hub 策略建議定義的資源。若要了解您可以使用哪些動作指定每個資源的 ARN，請參閱 Migration Hub Strategy Recommendations 定義的動作。

若要檢視策略建議身分型政策的範例，請參閱 Migration Hub 策略建議的身分型政策範例。

策略建議的政策條件索引鍵

支援服務特定的政策條件索引鍵：否

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Condition 元素 (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， 會使用邏輯OR操作 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。如需更多資訊，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的條件金鑰。若要查看所有 AWS 全域條件索引鍵，請參閱《IAM 使用者指南》中的AWS 全域條件內容索引鍵。

若要查看策略建議條件索引鍵的清單，請參閱《服務授權參考》中的 Migration Hub 策略建議的條件索引鍵。若要了解您可以使用條件金鑰的動作和資源，請參閱 Migration Hub Strategy Recommendations 定義的動作。

若要檢視策略建議身分型政策的範例，請參閱 Migration Hub 策略建議的身分型政策範例。

策略建議中的存取控制清單 (ACLs)

支援 ACL：否

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

具有策略建議的屬性型存取控制 (ABAC)

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。您可以將標籤連接至 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。

如需根據標籤控制存取，請使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 條件索引鍵，在政策的條件元素中，提供標籤資訊。

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

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

搭配策略建議使用暫時登入資料

支援臨時憑證：是

當您使用臨時登入資料登入時，有些 AWS 服務 無法運作。如需詳細資訊，包括哪些 AWS 服務 使用臨時登入資料，請參閱《AWS 服務 IAM 使用者指南》中的使用 IAM 的 。

如果您 AWS Management Console 使用使用者名稱和密碼以外的任何方法登入 ，則會使用臨時登入資料。例如，當您 AWS 使用公司的單一登入 (SSO) 連結存取 時，該程序會自動建立臨時登入資料。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》中的從使用者切換至 IAM 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許可

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，您會被視為委託人。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 使用呼叫 的委託人許可 AWS 服務，結合 AWS 服務 請求向下游服務提出請求。只有當服務收到需要與其他 AWS 服務 或 資源互動才能完成的請求時，才會提出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出 FAS 請求時的政策詳細資訊，請參閱轉發存取工作階段。

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權給 AWS 服務。

> **Warning**
>
> 變更服務角色的許可可能會中斷策略建議功能。只有在策略建議提供指引時，才能編輯服務角色。

策略建議的服務連結角色

支援服務連結角色：是

服務連結角色是連結至 的一種服務角色 AWS 服務。服務可以擔任代表您執行動作的角色。服務連結角色會出現在您的 中 AWS 帳戶 ，並由服務擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

如需建立或管理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 受管政策

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

AWS 服務會維護和更新 AWS 受管政策。您無法變更 AWS 受管政策中的許可。服務偶爾會將其他許可新增至 AWS 受管政策，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)。服務最有可能在新功能啟動或新操作可用時更新 AWS 受管政策。服務不會從 AWS 受管政策中移除許可，因此政策更新不會破壞您現有的許可。

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

AWS 受管政策：AWSMigrationHubStrategyConsoleFullAccess

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

`AWSMigrationHubStrategyConsoleFullAccess` 政策會授予使用者透過 對 Strategy Recommendations 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` – 授予使用者在 Application Discovery Service 中取得探索摘要的存取權。
- `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` – 授予使用者對策略建議的完整存取權。
- `s3` – 允許使用者從策略建議所使用的 S3 儲存貯體建立和讀取。
- `secretsmanager` – 允許使用者在 Secrets Manager 中列出秘密存取。

若要檢視此政策的許可，請參閱 AWS 受管政策參考指南AWSMigrationHubStrategyConsoleFullAccess中的 。

AWS 受管政策：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` – 准許上傳日誌和指標資料以進行應用程式轉換操作，並使用移植相容性評估和建議。
- `execute-api` – 允許使用者存取 Amazon API Gateway 以上傳日誌和指標 AWS。
- `migrationhub-strategy` – 授予使用者註冊訊息、傳送訊息、上傳日誌資料，以及將指標資料上傳至策略建議的權限。

- s3 – 授予使用者列出儲存貯體及其位置的存取權。使用者也會獲得許可，以寫入、擷取物件、新增物件、傳回存取控制清單 (ACL)、建立、存取、設定加密、修改PublicAccessBlock組態、設定版本控制狀態，以及建立或取代 Strategy Recommendations 所使用 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的 Secrets Manager 中的秘密。

若要檢視此政策的許可，請參閱 AWS 受管政策參考指南AWSMigrationHubStrategyCollector中的 。

AWS 受管政策的策略建議更新

檢視自此服務開始追蹤這些變更以來，策略建議 AWS 受管政策更新的詳細資訊。如需此頁面變更的自動提醒，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 – 更新至現有政策	此政策已更新為包含 PutLogData 、GetPortingCompatibilityAssessment 、 StartPortingCompatibilityAssessment StartPortingRecommendationAssessment 和GetPortingRecommendationAssessment 應用程式轉換動作，以允許應用程式轉換服務將日誌和指標傳送至服務。GetBucketLocation 已為 Amazon Simple Storage Service (Amazon S3) 新增 ListBucket 和 ，以支援日誌和指標上傳。PutMetricData 也新增了 PutLogData 和 ，以允許 Strategy	2024 年 4 月 1 日

變更	描述	日期
	Recommendations 收集器將日誌和指標傳送至服務的端點。	
AWSMigrationHubStrategyCollector – 更新至現有政策	此政策會使用 PutMetricData 和 PutLogData 動作更新。這些動作會授予應用程式轉換操作的上傳日誌和指標資料。此更新也會新增條件，以確保 aws:ResourceAccount 等於 aws:PrincipalAccount ，以允許 使用包含的 Amazon Simple Storage Service 和 AWS Secrets Manager 動作。	2024 年 2 月 5 日
AWSMigrationHubStrategyCollector – 更新至現有政策	此政策會使用下列 Amazon S3 APIs 更新：CreateBucket 、PutEncryptionConfiguration 、PutBucketPublicAccessBlock 、PutBucketPolicy 、 PutBucketVersioning 和 PutLifecycleConfiguration 。	2023 年 9 月 15 日
AWSMigrationHubStrategyCollector – 更新至現有政策	此政策更新會授予許可，以允許分析原始程式碼。	2023 年 3 月 8 日

變更	描述	日期
AWSMigrationHubStrategyConsoleFullAccess – 更新至現有政策	此政策更新為三個 AWS Application Discovery Service APIs – `DescribeConfigurations` 、 `DescribeTags` 和 `ListConfigurations` 。	2022 年 11 月 10 日
AWSMigrationHubStrategyCollector – 更新至現有政策	此政策會更新為 `UpdateCollectorConfiguration` 動作。此動作會儲存收集器的組態，以便輕鬆擷取。	2022 年 9 月 7 日
AWSMigrationHubStrategyConsoleFullAccess – 啟動時已提供新政策	`AWSMigrationHubStrategyConsoleFullAccess` 透過 授予使用者對 Strategy Recommendations 服務的完整存取權 AWS Management Console。	2021 年 10 月 25 日
AWSMigrationHubStrategyCollector – 新政策於啟動時提供	`AWSMigrationHubStrategyCollector` 會授予使用者對 Strategy Recommendations 服務的存取權，以及對與服務相關的 S3 儲存貯體的讀取/寫入存取權。它還授予 Amazon API Gateway 將日誌和指標上傳到 的存取權 AWS，以及 AWS Secrets Manager 擷取憑證的存取權。	2021 年 10 月 25 日

變更	描述	日期
AWSMigrationHubStrategyServiceRolePolicy – 新政策於啟動時提供	`AWSMigrationHubStrategyServiceRolePolicy` 服務連結角色政策提供對 AWS Migration Hub 和的存取權 AWS Application Discovery Service。此政策也授予許可，以將報告儲存在 Amazon Simple Storage Service (Amazon S3) 中。	2021 年 10 月 25 日
策略建議開始追蹤變更	策略建議會開始追蹤其 AWS 受管政策的變更。	2021 年 10 月 25 日

Migration Hub 策略建議的身分型政策範例

根據預設，使用者和角色沒有建立或修改策略建議資源的許可。他們也無法使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 或 AWS API 來執行任務。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。

如需了解如何使用這些範例 JSON 政策文件建立 IAM 身分型政策，請參閱《IAM 使用者指南》中的建立 IAM 政策 (主控台)。

如需有關策略建議所定義之動作和資源類型的詳細資訊，包括每種資源類型的 ARNs 格式，請參閱《服務授權參考》中的 Migration Hub 策略建議的動作、資源和條件金鑰。

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

身分型政策會判斷您帳戶中的某個人員是否可以建立、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 受管政策並轉向最低權限許可 – 若要開始將許可授予您的使用者和工作負載，請使用將許可授予許多常見使用案例的 AWS 受管政策。它們可在您的 中使用 AWS 帳戶。我們建議您定義特定於使用案例 AWS 的客戶受管政策，以進一步減少許可。如需更多資訊，請參閱 IAM 使用者指南中的 AWS 受管政策或任務職能的AWS 受管政策。
- 套用最低權限許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的許可。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需使用 IAM 套用許可的更多相關資訊，請參閱 IAM 使用者指南中的 IAM 中的政策和許可。
- 使用 IAM 政策中的條件進一步限制存取權 – 您可以將條件新增至政策，以限制動作和資源的存取。例如，您可以撰寫政策條件，指定必須使用 SSL 傳送所有請求。如果透過特定 例如 使用服務動作 AWS 服務，您也可以使用條件來授予其存取權 AWS CloudFormation。如需詳細資訊，請參閱 IAM 使用者指南中的 IAM JSON 政策元素：條件。
- 使用 IAM Access Analyzer 驗證 IAM 政策，確保許可安全且可正常運作 – IAM Access Analyzer 驗證新政策和現有政策，確保這些政策遵從 IAM 政策語言 (JSON) 和 IAM 最佳實務。IAM Access Analyzer 提供 100 多項政策檢查及切實可行的建議，可協助您撰寫安全且實用的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的使用 IAM Access Analyzer 驗證政策。
- 需要多重要素驗證 (MFA) – 如果您的案例需要 IAM 使用者或 中的根使用者 AWS 帳戶，請開啟 MFA 以提高安全性。如需在呼叫 API 操作時請求 MFA，請將 MFA 條件新增至您的政策。如需詳細資訊，請參閱《IAM 使用者指南》https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_configure-api-require.html中的透過 MFA 的安全 API 存取。

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

使用策略建議主控台

若要存取 Migration Hub 策略建議主控台，您必須擁有一組最低許可。這些許可必須允許您列出和檢視中策略建議資源的詳細資訊 AWS 帳戶。如果您建立比最基本必要許可更嚴格的身分型政策，則對於具有該政策的實體 (使用者或角色) 而言，主控台就無法如預期運作。

對於僅呼叫 AWS CLI 或 AWS API 的使用者，您不需要允許最低主控台許可。反之，只需允許存取符合他們嘗試執行之 API 操作的動作就可以了。

為了確保使用者和角色仍然可以使用策略建議主控台，也請將策略建議`ConsoleAccess`或`ReadOnly` AWS 受管政策連接到實體。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。此政策包含在主控台或使用 或 AWS CLI AWS API 以程式設計方式完成此動作的許可。

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

存取一個 Amazon S3 儲存貯體

在此範例中，您想要授予 IAM 使用者 AWS 帳戶 存取其中一個 Amazon S3 儲存貯體 的權限`amzn-s3-demo-bucket`。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。如需將許可授予使用者並使用主控台進行測試的範例逐步解說，請參閱範例逐步解說：使用使用者政策來控制對儲存貯體的存取。

```
{
   "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:::amzn-s3-demo-bucket"
      },
      {
         "Sid":"ManageBucketContents",
         "Effect":"Allow",
         "Action":[
            "s3:PutObject",
            "s3:PutObjectAcl",
            "s3:GetObject",
            "s3:GetObjectAcl",
            "s3:DeleteObject"
         ],
         "Resource":"arn:aws:s3:::amzn-s3-demo-bucket/*"
      }
   ]
}
```

對 Migration Hub 策略建議身分和存取進行故障診斷

使用以下資訊來協助您診斷和修正使用策略建議和 IAM 時可能遇到的常見問題。

主題

我無權在策略建議中執行動作

如果 AWS Management Console 通知您無權執行 動作，則必須聯絡您的管理員尋求協助。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。

我未獲得執行 iam:PassRole 的授權

如果您收到錯誤，告知您無權執行 `iam:PassRole`動作，您的政策必須更新，以允許您將角色傳遞至策略建議。

有些 AWS 服務 可讓您將現有角色傳遞給該服務，而不是建立新的服務角色或服務連結角色。如需執行此作業，您必須擁有將角色傳遞至該服務的許可。

當名為 的 IAM `marymajor` 使用者嘗試使用主控台在策略建議中執行動作時，會發生下列範例錯誤。但是，動作請求服務具備服務角色授予的許可。Mary 沒有將角色傳遞至該服務的許可。

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

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

如果您需要協助，請聯絡您的 AWS 管理員。您的管理員提供您的登入憑證。

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。透過這樣做，您可以讓某人永久存取您的 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，您必須將許可授予需要存取的人員或應用程式。如果您使用 AWS IAM Identity Center 管理人員和應用程式，您可以將許可集指派給使用者或群組，以定義其存取層級。許可集會自動建立 IAM 政策，並將其指派給與該人員或應用程式相關聯的 IAM 角色。如需詳細資訊，請參閱AWS IAM Identity Center 《 使用者指南》中的許可集。

如果您不是使用 IAM Identity Center，則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 ）。然後，您必須將政策連接到實體，以授予他們策略建議中的正確許可。授予許可後，請將登入資料提供給使用者或應用程式開發人員。他們將使用這些登入資料來存取 AWS。若要進一步了解如何建立 IAM 使用者、群組、政策和許可，請參閱《IAM 使用者指南》中的 IAM 身分和政策和許可。

我想要允許 以外的人員 AWS 帳戶 存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的資源的許可。

如需進一步了解，請參閱以下內容：

- 若要了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 AWS 帳戶 在您擁有的 資源間提供存取權，請參閱《IAM 使用者指南》中的在您擁有 AWS 帳戶 的另一個 IAM 使用者中提供存取權。
- 若要了解如何將資源的存取權提供給第三方 AWS 帳戶，請參閱《IAM 使用者指南》中的將存取權提供給第三方 AWS 帳戶 擁有。
- 如需了解如何透過聯合身分提供存取權，請參閱 IAM 使用者指南中的將存取權提供給在外部進行身分驗證的使用者 (聯合身分)。
- 如需了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱《IAM 使用者指南》中的 IAM 中的跨帳戶資源存取。

針對策略建議使用服務連結角色

Migration Hub Strategy Recommendations 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。服務連結角色是由 Strategy Recommendations 預先定義，並包含服務代表您呼叫其他 AWS 服務所需的所有許可。

服務連結角色可讓您更輕鬆地設定策略建議，因為您不必手動新增必要的許可。Strategy Recommendations 會定義其服務連結角色的許可，除非另有定義，否則只有 Strategy Recommendations 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。

如需支援服務連結角色的其他 服務的資訊，請參閱服務連結角色欄中AWS 與 IAM 搭配使用的服務，並尋找具有是的服務。選擇具有連結的是，以檢視該服務的服務連結角色文件。

Strategy Recommendations 的服務連結角色許可

Strategy Recommendations 使用名為 AWSServiceRoleForMigrationHubStrategy 的服務連結角色，並將其與 AWSMigrationHubStrategyServiceRolePolicy IAM 政策建立關聯 – 提供 AWS Migration Hub 和 的存取權 AWS Application Discovery Service。此政策也授予許可，以將報告儲存在 Amazon Simple Storage Service (Amazon S3) 中。

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

- `migrationhub-strategy.amazonaws.com`

角色許可政策允許 Strategy Recommendations 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
```

若要檢視此政策的許可，請參閱 AWS 受管政策參考指南AWSMigrationHubStrategyServiceRolePolicy中的 。

若要檢視此政策的更新歷史記錄，請參閱 AWS 受管政策的策略建議更新。

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。

為策略建議建立服務連結角色

您不需要手動建立一個服務連結角色。當您同意允許 Migration Hub 在 中的帳戶中建立服務連結角色 (SLR) 時 AWS Management Console，Strategy Recommendations 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 在帳戶中建立服務連結角色 (SLR) 時，Strategy Recommendations 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 編輯角色的描述。

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 AWS CLI、 或 AWS API 來刪除 AWSServiceRoleForMigrationHubStrategy 服務連結角色。如需詳細資訊，請參閱《IAM 使用者指南》中的刪除服務連結角色。

刪除 AWSServiceRoleForMigrationHubStrategy SLR 所使用的策略建議資源時，您無法有任何執行中的評估（產生建議的任務）。也無法執行背景評估。如果評估正在執行，則 IAM 主控台中的 SLR 刪除會失敗。如果 SLR 刪除失敗，您可以在所有背景任務完成後重試刪除。刪除 SLR 之前，您不需要清除任何建立的資源。

Strategy Recommendations 服務連結角色支援的 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 策略建議和界面 VPC 端點 (AWS PrivateLink)

您可以建立界面 VPC 端點，在 VPC 和 Migration Hub 策略建議之間建立私有連線。界面端點是採用 AWS PrivateLink技術。使用 AWS PrivateLink，您可以私下存取 Strategy Recommendations API 操作，無需網際網路閘道、NAT 裝置、VPN 連線或 AWS Direct Connect 連線。VPC 中的執行個體不需要公有 IP 地址，即可與 Strategy Recommendations API 操作通訊。VPC 和策略建議之間的流量會保留在 Amazon 網路中。

每個介面端點都是由您子網路中的一或多個彈性網路介面表示。

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

策略建議 VPC 端點的考量

在設定適用於策略建議的介面 VPC 端點之前，請務必檢閱 Amazon VPC 使用者指南中的介面端點屬性和限制和AWS PrivateLink 配額。

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

為策略建議建立介面 VPC 端點

您可以使用 Amazon VPC 主控台或 AWS Command Line Interface () 為策略建議建立 VPC 端點AWS CLI。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的建立介面端點。

使用下列服務名稱建立策略建議的 VPC 端點：

- `com.amazonaws.region.migrationhub-strategy`

如果您為端點使用私有 DNS，您可以使用區域的預設 DNS 名稱向策略建議提出 API 請求。例如，您可以使用名稱 `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。

為策略建議建立 VPC 端點政策

您可以將端點政策連接至 VPC 端點，以控制對策略建議的存取。此政策會指定下列資訊：

- 可執行動作的主體。
- 可執行的動作。
- 可以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：策略建議動作的 VPC 端點政策

以下是 Strategy Recommendations 的端點政策範例。連接到端點時，此政策會授予所有資源上所有主體所列出的策略建議動作的存取權。

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

```
        }
    ]
}
```

Migration Hub 策略建議的合規驗證

若要了解 是否 AWS 服務 在特定合規計劃的範圍內，請參閱AWS 服務 合規計劃範圍內然後選擇您感興趣的合規計劃。如需一般資訊，請參閱 AWS Compliance Programs。

您可以使用 下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱在 中下載報告 AWS Artifact。

使用 時的合規責任 AWS 服務 取決於資料的敏感度、您公司的合規目標，以及適用的法律和法規。AWS 提供下列資源以協助合規：

- 安全合規與治理 - 這些解決方案實作指南內容討論了架構考量，並提供部署安全與合規功能的步驟。
- HIPAA 合格服務參考 – 列出 HIPAA 合格服務。並非所有 AWS 服務 都符合 HIPAA 資格。
- AWS 合規資源 – 此工作手冊和指南的集合可能適用於您的產業和位置。
- AWS 客戶合規指南 – 透過合規的角度了解共同責任模型。本指南摘要說明保護 的最佳實務， AWS 服務 並將指南映射到跨多個架構的安全控制 （ 包括國家標準和技術研究所 (NIST)、支付卡產業安全標準委員會 (PCI) 和國際標準化組織 (ISO))。
- AWS Config 開發人員指南中的使用規則評估資源 – AWS Config 服務會評估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 可讓您全面檢視其中的安全狀態 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 控制參考」。
- Amazon GuardDuty – 這可透過監控您的環境是否有可疑和惡意活動，來 AWS 服務 偵測對您 AWS 帳戶、工作負載、容器和資料的潛在威脅。GuardDuty 可滿足特定合規架構所規定的入侵偵測需求，以協助您因應 PCI DSS 等各種不同的合規需求。
- AWS Audit Manager – 這 AWS 服務 可協助您持續稽核 AWS 用量，以簡化您管理風險的方式，以及符合法規和產業標準的方式。

使用其他 服務

本節說明與 Migration Hub 策略建議互動的其他 AWS 服務。

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 Strategy Recommendations 已與 整合 AWS CloudTrail，此服務提供使用者、角色或 Strategy Recommendations 中的 AWS 服務所採取動作的記錄。CloudTrail 會將 Strategy Recommendations 的 API 呼叫擷取為事件。擷取的呼叫包括從 Strategy Recommendations 主控台進行的呼叫，以及對 Strategy Recommendations API 操作的程式碼呼叫。

如果您建立線索，您可以啟用 CloudTrail 事件持續交付至 Amazon S3 儲存貯體，包括策略建議的事件。即使您未設定追蹤，依然可以透過 CloudTrail 主控台中的事件歷史記錄檢視最新事件。使用 CloudTrail 收集的資訊，您可以判斷對 Strategy Recommendations 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

建立帳戶 AWS 帳戶 時，您的 上會啟用 CloudTrail。當活動在策略建議中發生時，該活動會記錄於 CloudTrail 事件，以及事件歷史記錄中的其他服務 AWS 事件。您可以檢視、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 事件歷史記錄檢視事件」。

若要持續記錄 中的事件 AWS 帳戶，包括策略建議的事件，請建立追蹤。線索能讓 CloudTrail 將日誌檔案交付至 Amazon S3 儲存貯體。依預設，當您在主控台中建立追蹤時，該追蹤會套用至所有的 AWS 區域。追蹤會記錄 AWS 分割區中所有 區域的事件，並將日誌檔案交付至您指定的 Amazon S3 儲存貯體。此外，您可以設定其他 AWS 服務，以進一步分析和處理 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

策略建議支援將下列動作記錄為 CloudTrail 日誌檔案中的事件：

- GetApplicationComponentStrategies
- GetApplicationComponentDetails
- GetAssesment
- GetImportFileTask
- GetPortfolioPreferences
- GetPortfolioSummary
- GetServerDetails
- GetServerStrategies
- ListApplicationComponents
- ListCollectors
- ListImportFileTask
- ListServers
- PutPortfolioPreferences
- StartAssessment
- StartImportFileTask
- StopAssessment
- UpdateApplicationComponetConfig
- UpdateServerConfig

每一筆事件或日誌專案都會包含產生請求者的資訊。身分資訊可協助您判斷下列事項：

- 請求是使用根或 AWS Identity and Access Management (IAM) 使用者登入資料提出
- 提出該請求時，是否使用了特定角色或聯合身分使用者的臨時安全憑證
- 請求是否由其他 AWS 服務提出

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

了解策略建議日誌檔案項目

追蹤是一種組態，能讓事件以日誌檔案的形式交付到您指定的 Amazon S3 儲存貯體。CloudTrail 日誌檔案包含一或多個日誌專案。一個事件為任何來源提出的單一請求，並包含請求動作、請求的日期和時

間、請求參數等資訊。CloudTrail 日誌檔並非依公有 API 呼叫的堆疊追蹤排序，因此不會以任何特定順序出現。

下列範例顯示示範 GetServerDetails 動作的 CloudTrail 日誌項目。

```
{
    "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 策略建議的配額

AWS 您的帳戶具有每個 AWS 服務的預設配額，先前稱為限制。除非另有說明，否則每個配額都是區域特定規定。您可以請求提高某些配額，而其他配額無法提高。

若要檢視 Migration Hub Strategy Recommendations 的配額清單，請參閱 Strategy Recommendations 服務配額。

您也可以開啟 Service Quotas 主控台來檢視策略建議的配額。在導覽窗格中，選擇 AWS 服務，然後選取 Migration Hub 策略建議。

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

- 收集器 v1.1.47
- 支援 .NET 8 應用程式。

2023 年 10 月 12 日

新功能

- 收集器 v1.1.45

- 支援多資料來源。

2023 年 4 月 17 日

新功能

- 收集器 v1.1.22
- 升級指令碼增強功能。這需要最新版本的 收集器。

2023 年 3 月 17 日

新功能

新增了二進位分析，可提供不含原始碼的反模式和不相容偵測。

2022 年 11 月 7 日

新功能

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

2022 年 9 月 27 日

新功能

- 收集器 v1.1.12
  - SCT 667 版
  - EMPAnalyzer 2.2.0.368
- 已新增伺服器洞見的`diag check`命令。
- 新增對潛在建議的支援。
- 增強型使用者介面，用於檢查組態和評估狀態。

錯誤修正

- 移植助理翻譯程式和其他修正。

2022 年 6 月 30 日

新功能

- 收集器 v1.1.11
  - 新增 VMware API 支援。
  - A2C 請求變更，以在下載二進位檔案時新增使用者標頭。
  - 新增 Linux 主路徑、預設 Shell 和所有 shell 的遠端終止。
- A2C v1.17 公有二進位
  - 新增對 Azure DevOps 的支援做為管道部署目標。

2022 年 4 月 18 日

新功能

- 收集器 1.1.7 版
- 新增了從公有 URL 動態下載 A2C 二進位檔案的功能。

錯誤修正

- A2C 1.1.5 版

2022 年 2 月 25 日

錯誤修正

- SCT 5.6.9 版
- A2C 1.1.2 版
- 收集器 1.1.4 版

2022 年 2 月 10 日

錯誤修正

- SCT 5.6.8 版

- A2C 1.1.1 版
  - 新增 Linux 上tar命令的檢查。
  - 修正在 Amazon ECR 中檢查應用程式映像的問題。
  - 修正需要移除容器以進行預先驗證的問題。
- 收集器 1.1.3 版
  - 已修正遠端 32 位元機器的 4xx 錯誤。
  - 已更新 A2C 錯誤代碼。
  - 驗證 中的 IP 地址，C#以進行遠端機器的原始碼分析。

2022 年 1 月 28 日

新功能

- 收集器 1.1.2 版
- 新增 Azure DevOps Git 儲存庫對原始程式碼分析的支援。

2022 年 1 月 14 日

新功能

- 收集器 1.1.1 版
- 新增了 SQL 資料庫的 Babelfish 建議。

2021 年 12 月 21 日

問題已解決

- 收集器 1.1.0 版
- 已還原資料庫分析。

2021 年 12 月 15 日

已知問題

- 收集器 1.0.4 版
- 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 1.0.0 版
- Migration Hub 策略建議使用者指南的初始版本。

文件和版本歷史記錄

下表說明 Strategy Recommendations 的文件版本。如需詳細資訊，請參閱版本備註。

變更	Description	日期
AWS 受管政策更新 - 更新至 AWSMigrationHubStrategyCollector	已更新 AWSMigrationHubStrategyCollector 政策，以包含新的 `s3`、`application-transformation` 和 `migrationhub-strategy` 動作。	2024 年 4 月 1 日
AWS 受管政策更新 - 更新至 AWSMigrationHubStrategyCollector	更新 AWSMigrationHubStrategyCollector 政策以包含新的`application-transformation` 動作。此更新也會新增條件，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	Strategy Recommendations 應用程式資料收集器用戶端 v1.1.47 支援 .NET 8 應用程式。	2023 年 11 月 17 日
新功能	Strategy Recommendations 應用程式資料收集器用戶端 v1.1.45 支援多個資料來源。	2023 年 10 月 12 日
AWS 受管政策更新 - 更新至 AWSMigrationHubStrategyCollector	更新 AWSMigrationHubStrategyCollector 政策，以包含新的 Amazon S3 APIs。	2023 年 9 月 15 日

AWS 受管政策更新 - 更新至 AWSMigrationHubStrategyCollector	更新 AWSMigrationHubStrategyCollector 政策，以包含原始程式碼的新分析器。	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 受管政策更新 - 更新至現有政策	Migration Hub 策略建議已將三個 AWS Application Discovery Service APIs新增至現有政策。	2022 年 11 月 10 日
安全性更新	建立與介面 VPC 端點的私有連線。	2022 年 3 月 7 日
新功能	新增 Azure DevOps Git 儲存庫對原始程式碼分析的支援。	2022 年 1 月 28 日
新功能	新增了 SQL 資料庫的 Babelfish 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。