使用者指南

AWS Migration Hub 重構空間

AWS Migration Hub 重構空間: 使用者指南

Table of Contents

什麼是 AWS Migration Hub 重構空間？

AWS Migration Hub 重構空間目前為預覽版本，並可能有所變更。

AWS Migration Hub 重構空間是增量應用程式重構至AWS。重構空間有助於減少建築和營運中未分化的繁重工作AWS基礎結構進行增量重構。您可以使用重構空間來協助降低風險，將應用程式演變為微服務，或使用微服務撰寫的新功能擴充現有的應用程式。

重構空間環境藉由協調AWS Transit Gateway、AWS Resource Access Manager和虛擬私有雲端(VPC)。重構空間橋接跨AWS帳戶允許更早和更新的服務進行溝通，同時保持獨立的獨立AWS 帳戶。

重構空間提供了一個應用程序，用於增量重構的 Shangler 無花果模式。重構空間應用程式可協調 Amazon API Gateway、Network Load Balancer 和以資源為基礎的AWS Identity and Access Management(IAM) 政策，以便您可以透明地將新服務新增至外部 HTTP 端點。您也可以遞增地將流量路由傳送至新服務。這使您的應用程序消費者的基礎架構變化保持透明。如需有關 Sigration 無花果模式語法的詳細資訊，請參閱。勒索無花果應用程式。

主題

您是第一次使用重構空間嗎？

如果您是第一次使用重構空間，建議您在開始前先閱讀以下章節：

- 重構空間概念
- 重構空間的運作方式
- 設定
- 開始使用重構空格

Pricing

所有重構空間協調的資源 (例如，Transit Gateway) 都佈建在您的AWS 帳戶。因此，您需要支付重構空間的使用量，以及與佈建資源相關聯的任何成本。如需詳細資訊，請參閱「」AWSMigration Hub 定價。

> **Note**
>
> 重構空間在其預覽期間不收取任何費用。

重構空間概念

本節說明使用 AWS Migration Hub 重構空間時可以建立和管理的主要元件。

主題

- Environment
- Applications
- Services
- Route

Environment

重構 Spaces 環境提供整合的網路、應用程式和服務檢視，跨多個AWS帳戶。

重構空間環境包含重構空間應用程式和服務。這是由橋接虛擬私有雲 (VPC) 組成的多帳戶網路網狀架構，可讓其中的資源透過私有 IP 位址進行互動。此環境提供跨多個AWS 帳戶。

所以此環境擁有者是在中建立重構空間環境的帳戶。無論建立資源的帳戶為何，環境擁有者都可以跨帳戶查看環境中建立的應用程式、服務和路由。

Applications

重構空間應用程式包含服務和路由，並提供單一外部端點，以便將應用程式公開給外部呼叫者。該應用程序提供了一個 Shangler 無花果代理，用於增量應用程序重構。如需的詳細資訊，請參閱。勒索無花果應用程式。

重構空間應用程式模型了扼殺圖模式，並協調 Amazon API Gateway、API 閘道 VPC 連結、Network Load Balancer 和以資源為基礎的AWS Identity and Access Management(IAM) 政策，以便您可以透明地將新服務新增至應用程式的 HTTP 端點。它也會逐步將流量從您現有的應用程式路由傳送到新的服務。這使得基礎架構變更透明的應用程式消費者。

Services

重構 Spaces 服務可提供應用程式的商務功能，並可透過唯一端點存取。服務端點是以下兩種類型的其中一種：HTTP/HTTPS URL，或AWS Lambda函數。

Route

重構空間路由是將要求轉寄至服務的 Proxy 比對規則。每個請求都會針對應用程式中配置的路由集執行。如果規則相符，則會將要求傳送至針對該規則設定的目標服務。如果應用程式不符合任何規則，應用程式有預設路由，可將要求轉寄至預設服務。路由在應用程序的 Amazon API Gateway 代理上配置。

重構空間的運作方式

開始使用 AWS Migration Hub 重構空間時，您可以使用一或多個AWS 帳戶。您可以使用單一帳戶進行測試。不過，一旦您準備好開始著手，建議您從下列三個帳戶開始著手：

- 現有應用程式的一個帳戶。
- 第一個新微服務的帳戶。
- 一個帳戶充當重構環境擁有者，其中重構空間會設定跨帳戶網路並路由流量。

首先，您可以在選擇做為環境擁有者的帳戶中建立重構空間環境。然後，您與其他兩個帳戶共用環境使用AWS Resource Access Manager（重構空間主控台會為您執行此操作）。與另一個帳戶共用環境之後，重構空間會自動與其他帳戶共用它在環境中建立的資源。它通過編排AWS Identity and Access Management(IAM) 資源型政策。

重構環境透過協調AWS Transit Gateway、AWS Resource Access Manager和虛擬私有雲端 (VPC)。重構環境包含您現有的應用程式和新的微服務。建立重構環境後，您可以在環境中建立重構空間應用程式。重構空間應用程式包含服務和路由，並提供單一端點，以便將應用程式公開給外部呼叫者。

應用程式支援路由到容器中執行的服務、無伺服器運算以及具有公有或私有可見性的 Elastic Compute Cloud (Amazon EC2)。應用程式內的服務可以有兩種端點類型之一：VPC 中的 URL (HTTP 和 HTTPS)，或AWS Lambda函數。應用程式包含服務之後，您可以新增預設路由，將所有流量從應用程

式 Proxy 導向至代表現有應用程式的服務。當您在容器或無伺服器計算中發行或新增新功能時，您會新增新的服務和路由，以將流量重新導向至新的服務。

對於 VPC 中具有 URL 端點的服務，重構空間會使用 Transit Gateway 自動橋接環境內的所有服務 VPC。這表示任何AWS資源可以直接與新增至環境的所有其他服務 VPC 通訊。您可以使用 VPC 安全性群組套用其他跨帳戶路由限制。使用 Lambda 端點建立指向服務的路由時，重構空間會協調 Amazon API 閘道的 Lambda 整合，以便在AWS 帳戶。

設定

AWS Migration Hub 重構空間目前為預覽版本，並可能有所變更。

初次使用 AWS Migration Hub 重構空間之前，請先完成以下任務：

註冊 AWS
建立 IAM 使用者

註冊 AWS

在本節中，您會註冊 AWS 帳戶。如果您已有 AWS 帳戶，請跳過這個步驟。

註冊 Amazon Web Services (AWS)，您的AWS帳戶會自動註冊所有AWS服務，包括 AWS Migration Hub 重構空間。您只需針對所使用的服務付費。

如果您還沒有 AWS 帳戶，請完成下列步驟建立新帳戶。

註冊 AWS 帳戶

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

   部分註冊程序需接收來電，並在電話鍵盤輸入驗證碼。

建立 IAM 使用者

建立AWS帳戶時，會取得單一的登入身分，可以完整存取所有AWS帳戶中的服務和資源。這個身分稱為 AWS 帳戶的根使用者。登入AWS Management Console使用您用於建立帳戶的電子郵件地址和密碼後，即可完整存取所有AWS資源。

強烈建議您不要以根使用者處理日常作業，即使是管理作業。相反地，請遵循安全性最佳做法建立個別 IAM 使用者並建立AWS Identity and Access Management(IAM) 管理員使用者。然後，安全地鎖定根使用者登入資料，並只用來執行少數的帳戶與服務管理任務。

除了建立管理使用者外，您還必須建立非管理 IAM 使用者。下列主題說明如何建立這兩種類型的 IAM 使用者。

主題

建立 IAM 管理使用者

管理員帳戶預設繼承AWSMigrationHubRefactorSpacesFullAccess存取 AWS Migration Hub 重構空間所需的受管政策。

建立管理員使用者

- 在您的 AWS 帳戶中建立管理員使用者。如需說明，請參閱「」建立您的第一個 IAM 使用者和管理員群組中的IAM User Guide。

建立 IAM 非管理使用者

本節描述如何授予使用非管理使用者的重構空間所需的許可。

在使用重構空間之前，請使用AWSMigrationHubRefactorSpacesFullAccess管理的原則，然後附加授與使用者使用重構空間所需的額外必要權限的原則。這個額外的必要權限原則在重構空間的額外必要權限。

建立非管理 IAM 使用者時，請遵循安全性最佳實務授予最低權限，並授與使用者最低權限。

若要建立欲搭配重構空間使用的非管理員 IAM 使用者

1. InAWS Management Console中，導覽至 IAM 主控台。
2. 按照使用主控台建立使用者的指示建立非管理員 IAM 使用者，如在您的AWS帳戶中的IAM User Guide。

   雖然遵循IAM User Guide：

   - 在關於選取存取類型的步驟時，請同時選取程式設計存取和AWS管理主控台存取。
   - 當在關於設定許可頁面上，選擇將現有政策直接連接至使用者。然後，選取受管理的 IAM 政策外觀設定因子空間完全存取。
   - 若要檢視使用者的存取金鑰 (存取金鑰 ID 和私密存取金鑰)，請遵循Important (重要)注意事項，瞭解如何將使用者的新存取金鑰 ID 和私密存取金鑰存放在安全處。

3. 建立使用者之後，請依照指示將額外的必要權限原則新增至使用者，以內嵌使用者的內嵌原則新增 IAM 身分識別權限中的IAM User Guide。這個額外的必要權限原則在重構空間的額外必要權限。

開始使用重構空格

AWS Migration Hub 重構空間目前為預覽版本，並可能有所變更。

本節說明如何開始使用 AWS Migration Hub 重構空間

主題

Prerequisites

以下是使用 AWS Migration Hub 重構空間的先決條件。

- 您必須有一或多個AWS 帳戶，以及AWS Identity and Access Management(IAM) 使用者為這些帳戶設定。如需詳細資訊，請參閱 設定。
- 將其中一個 IAM 使用者帳戶指定為「重構空間」環境擁有者帳戶。

下列步驟說明如何在 Migration Hub 主控台中使用 AWS Migration Hub 重構空間。

步驟 1：建立環境

此步驟說明如何建立環境做為「重構空間」的一部分入門精靈。您也可以選擇環境下app 重構在重構空格導覽窗格中。

重構環境可簡化多帳戶使用案例，以加速應用程式重構。當您建立環境時，我們會協調AWS Transit Gateway、虛擬私有雲端 (VPC) 和AWS Resource Access Manager在您帳戶中。

建立環境之後，您可以與其他AWS 帳戶、組織單位 (OU)AWS Organizations，或整個AWS組織。通過與其他人共享環境AWS 帳戶，除非您使用 IAM 限制存取權限，否則這些帳戶中的使用者可以在環境中建立應用程式、服務和路由。

建立環境

1. 使用AWS帳戶，您在設定，登入AWS Management Console，然後在https://console.aws.amazon.com/migrationhub/。
2. 在遷移中樞主控台導覽窗格中，選擇重構空格。
3. 選擇 Getting started (入門)。
4. 選擇建立重構環境，以便開始以增量方式現代化為多個AWS帳戶。
5. 選擇 Start (啟動)。
6. 輸入環境名稱。
7. (選用) 新增環境的描述。
8. 重構空間會使用服務連結角色來連線至AWS 服務會代表您進行這些協調。當您第一次使用重構空間時，會為您建立服務連結角色並具有正確的權限。如需服務連結角色的詳細資訊，請參閱使用服務連結角色。
9. 選擇下一頁以移至建立應用程式(憑證已建立！) 頁面上的名稱有些許差異。

步驟 2：建立應用程式

此步驟說明如何建立應用程式做為「重構空間」的一部分入門精靈。您也可以選擇建立應用程式下快速動作在重構空格導覽窗格中。

應用程式為應用程式中的服務提供多帳戶流量路由。對於每個應用程式，我們都會使用 Amazon API Gateway VPC 連結、Network Load Balancer 和資源政策來協調代理。應用程序是服務和路由的容器。

應用程序的代理需要一個 VPC。代理的 Network Load Balancer 在 VPC 中啟動，並為 VPC 和網絡負載平衡器配置 API 網關 VPC 鏈接。

建立應用程式

1. 在建立應用程式頁面上，輸入您應用程式的名稱。
2. UNEST代理 VPC，選擇代理虛擬私有雲端 (VPC) 或選擇建立 VPC。

應用程序的代理需要一個 VPC。代理的 Network Load Balancer 在 VPC 中啟動，並為 VPC 和網絡負載平衡器配置 API 網關 VPC 鏈接。

3. UNESTProxy 端點類型選取Regional或者私有。

   Proxy 的端點可以是 [區域] 或 [私人]。區域 API Gateway 端點可透過公用網際網路存取，而私有 API Gateway 端點只能透過 VPC 存取。

4. 選擇下一頁以移至共享環境(憑證已建立！) 頁面上的名稱有些許差異。

步驟 3：共享您的環境

此步驟說明如何共用環境作為重構空間的一部分入門精靈。您也可以選擇共享環境下快速動作在重構空格導覽窗格中。

環境會與其他AWS 帳戶運用AWS Resource Access Manager(AWS RAM。環境共用必須接受邀請的帳戶在 12 小時內。否則，必須再次共用環境。如果您是在AWS組織，那麼您就可以啟用自動接受共用。AWS RAM支援與其他AWS 帳戶、組織單位 (OU)AWS Organizations，或整個AWS組織。

由於環境是應用程序，服務，路由和協調AWS資源，共用環境可讓您從受邀帳號存取這些資源。與其他帳戶共用之後，這些帳戶中的使用者可以在環境中建立應用程式、服務和路由，除非您使用 IAM 限制存取。

與另一個AWS 帳戶，重構空間也會共享環境的AWS Transit Gateway使用其他帳戶，方法是協調AWS RAM。

共用環境的步驟

1. 選取下列其中一個主參與者類型以共用您的環境：

   - AWS 帳戶
   - 組織-整個AWS組織
   - 組織單位 (OU)

   AWS RAM支援與其他AWS 帳戶、組織單位 (OU)AWS Organizations，或整個AWS組織。

2. 環境會與其他AWS 帳戶運用AWS Resource Access Manager(AWS RAM。AWS RAM支援與其他AWS 帳戶、組織單位 (OU)AWS Organizations，或整個AWS組織。如果您想要與整個AWS組織或 OU，您必須啟用AWS RAM之前嘗試在重構空間中共享。

3. 輸入AWS 帳戶，然後選擇Add。
4. 選擇下一頁以移至檢閱(憑證已建立！) 頁面上的名稱有些許差異。
5. 檢閱您在之前步驟所輸入的資訊。
6. 如果一切正確，請選擇建立環境。如果您希望進行某些變更，請選擇PREVID。

步驟 4：建立服務

服務提供應用程式的業務功能。您現有的應用程式會由一或多個服務代表。每個服務都有一個端點 (HTTP (TTPS) URL 或AWS Lambda函數)。

建立環境之後，您可以在環境詳細資料頁面 (以環境名稱作為標題的頁面) 上檢視環境的相關資訊。環境詳細資料頁面會顯示您環境的摘要，並列出您環境中的應用程式。

下列程序說明如何從環境詳細資訊頁面開始建立服務。您也可以選擇建立服務下快速動作在重構空格導覽窗格中。

從環境詳細資訊頁面建立服務

1. 從應用程式清單選擇您要新增服務的應用程式名稱。
2. 在應用程式詳細資料頁面 (以應用程式名稱作為標題的頁面) 的服務中，選擇建立服務。
3. 輸入新服務的名稱。
4. (選用) 輸入服務的描述。
5. 選取其中一個服務端點類型。
6. 如果服務是 VPC 中的 URL 端點，請選取 VPC。
    a. 選取要新增至環境網路橋接器的 VPC。
    b. 輸入服務 URL 端點。

        VPC 端點 URL 可以包含可公開解析的 DNS 名稱 (http://www.example.com) 或 IP 位址。服務 URL 不支援私人 DNS 名稱，但您可以使用服務 VPC 中的私人 IP 位址。
    c. (選擇性) 輸入健全狀況檢查端點 URL。
7. a. 如果服務是 Lambda 函數，請選取 Lambda 函數。
    b. 從您帳戶中選擇 Lambda 函數。
8. (選擇性) 在將流量路由到此服務，如果您想要將此服務設定為應用程式的預設路由，請選取對應的核取方塊。

在您建立服務時，您可以選擇性地將應用程式流量路由至該服務。如果建立服務的應用程式沒有任何路由，您可以將服務設為應用程式的預設路由，以便將所有流量路由至服務。如果應用程序有現有的路由，那麼您可以添加路徑指向服務的路由。

步驟 5：建立路由

本節說明如何建立路由。

應用程式是用來遞增地將流量從現有的應用程式重新路由傳送到新的服務。您也可以使用它來啟動新功能，而無需觸及現有的應用程式。

如果選取的應用程式沒有任何路由，則新路由會成為應用程式的預設路由，而所有流量都會路由至選取的服務。如果應用程序有現有的路由，那麼路由的範圍是路徑和動詞組合。

> **Note**
>
> 建立路由後會立即生效，並將流量重新導向離開預設路由或現有的父路由。

建立路由

在應用程式詳細資料頁面 (以應用程式名稱作為標題的頁面) 的路由中，選擇建立路由。

1. 選擇路由的服務。
2. 選擇 Create route (建立路由)。

AWS Migration Hub 的安全性重構空間

AWS Migration Hub 重構空間目前為預覽版本，並可能有所變更。

雲端安全是 AWS 最重視的一環。身為 AWS 客戶的您，將能從資料中心和網路架構的建置中獲益，以滿足組織最為敏感的安全要求。

安全是 AWS 與您共同肩負的責任。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：

- 雲端本身的安全 – AWS 負責保護在 AWS Cloud 中執行 AWS 服務的基礎設施。AWS 也提供您可安全使用的服務。第三方稽核人員會定期測試和驗證我們安全性的有效性，做為 AWS 合規計劃的一部分。若要了解適用於重構空間的合規計劃，請參閱AWS合規計劃範圍內的服務範圍。
- 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、您公司的要求和適用法律和法規。

本文件有助於您了解如何在使用 AWS Migration Hub 重構空間時套用共同責任模型。它會示範如何設定重構空間以符合您的安全性和合規目標。您也將了解如何使用其他AWS服務，協助您監控並保護重構空間資源。

內容

AWS Migration Hub 中的資料保護重構空間

所以此AWS 共同責任模型適用於 AWS Migration Hub 重構空間中的資料保護。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。您必須負責維護在此基礎設施上託管之內容的控制權。此內容包括您所使用 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，建議您使用 AWS 帳戶 (IAM) 保護 AWS Identity and Access Management 憑證，並設定個別使用者帳戶。如此一來，每個使用者都只會獲得授予完成其任務所必須的許可。我們也建議您採用下列方式保護資料：

- 每個帳戶都使用多重要素驗證 (MFA)。
- 使用 SSL/TLS 與 AWS 資源通訊。建議使用 TLS 1.2 或更新版本。
- 使用 AWS CloudTrail 設定 API 和使用者活動記錄。
- 使用 AWS 加密解決方案，以及 AWS 服務內的所有預設安全控制。
- 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 的個人資料。
- 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 端點的詳細資訊，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欄位中，例如名稱欄位。這包括當您使用重構空間或其他AWS服務使用主控台、API、AWS CLI, 或AWS開發套件。您在標籤或自由格式欄位中輸入的任何資料都可能用於計費或診斷記錄。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 中包含登入資料資訊。

靜態加密

重構空間會加密所有靜態資料。

傳輸中加密

重構空間網際網路通訊支援所有元件與用戶端之間的 TLS 1.2 加密。

AWS Migration Hub 的 Identity and Access Management

AWS Identity and Access Management (IAM) 是一種 AWS 服務，讓管理員能夠安全地控制對 AWS 資源的存取。IAM 管理員控制哪些人可以成為認證(已登入) 和授權(具有權限) 來使用重構空間資源。IAM 是一種您可以免費使用的 AWS 服務。

主題

- Audience
- 使用身分來驗證
- 使用政策管理存取權
- AWS Migration Hub 重構空間如何搭配 IAM 使用

- AWSAWS Migration Hub Migration Hub 重構空間的受管政策
- AWS Migration Hub 重構空間的身分型政策範例
- 疑難排解 AWS Migration Hub 重構空間身分識別和存取
- 使用服務連結角色

Audience

您使用的方式AWS Identity and Access Management(IAM) 會不同，取決於您在重構空間中執行的工作。

服務使用者— 若您使用重構 Space 來執行任務，您的管理員可以提供您需要的登入資料和許可。隨著您為了執行作業而使用的重構空間數量變多，您可能會需要額外的許可。了解存取的管理方式可協助您向管理員請求正確的許可。如果您無法存取重構空間中的功能，請參閱疑難排解 AWS Migration Hub 重構空間身分識別和存取。

服務管理員— 如果您負責公司的重構空間資源，您可能具備重構空間的完整存取權限。您的任務是判斷員工應存取的重構 Space 功能及資源。您接著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可搭配重構空間使用 IAM 的方式，請參閱AWS Migration Hub 重構空間如何搭配 IAM 使用。

IAM 管理員— 若您是 IAM 管理員，您可能會想要了解如何撰寫政策來管理重構 Space 存取權的詳細資訊。若要檢視您可以在 IAM 中使用的範例重構空間身分型政策，請參閱AWS Migration Hub 重構空間的身分型政策範例。

使用身分來驗證

身分驗證是使用身分登入資料登入 AWS 的方式。若需使用 AWS Management Console 登入的詳細資訊，請參閱 IAM 使用者指南中的以 IAM 使用者或根使用者身分登入 AWS Management Console。

您必須以 AWS 帳戶 根使用者身分、IAM 使用者身分，或使用 IAM 角色進行驗證 (登入至 AWS)。您也可以使用貴公司的單一登入身分驗證，甚至使用 Google 或 Facebook 進行登入。在上述案例中，您的管理員會使用 IAM 角色預先設定聯合身分。當您使用來自其他公司的身分驗證來存取 AWS 時，您是間接地擔任角色。

若要直接登入 AWS Management Console，請使用您的根使用者電子郵件地址或您的 IAM 使用者名稱密碼。您可以使用您的根使用者或 IAM 使用者存取金鑰，透過程式設計程式的方式存取 AWS。AWS 提供開發套件和命令列工具，以加密的方式使用您的登入資料簽署您的請求。如果您不使用 AWS 工

具，您必須自行簽署請求。請使用 Signature 第 4 版來執行此作業，它是針對傳入 API 請求進行身分驗證的通訊協定。如需驗證請求的詳細資訊，請參閱 AWS 一般參考中的簽章版本 4 簽署程序。

無論您使用何種身分驗證方法，您可能還需要提供額外的安全性資訊。例如，AWS 建議您使用多重要素驗證 (MFA) 來提高帳戶的安全。若要進一步了解，請參閱 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

如果是首次建立 AWS 帳戶，您會先有單一的登入身分，可以完整存取帳戶中所有 AWS 服務與資源。此身分稱為 AWS 帳戶 根使用者，使用建立帳戶時所使用的電子郵件地址和密碼即可登入並存取。強烈建議您不要以根使用者處理日常作業，即使是管理作業。反之，請遵循僅以根使用者建立您第一個 IAM 使用者的最佳實務。接著請妥善鎖定根使用者憑證，只用來執行少數的帳戶與服務管理作業。

IAM 使用者和群組

IAM 使用者是您 AWS 帳戶 中的一種身分，具備單一人員或應用程式的特定許可。IAM 使用者可有長期憑證 (例如，使用者名稱和密碼或一組存取金鑰)。若要了解如何產生存取金鑰，請參閱 IAM 使用者指南中的管理 IAM 使用者的存取金鑰。當您產生 IAM 使用者的存取金鑰時，請確認您已檢視且安全地儲存金鑰對。您在這之後便無法復原私密存取金鑰。屆時您必須改為產生新的存取金鑰對。

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

使用者與角色不同。使用者只會與單一人員或應用程式建立關聯，但角色的目的是在由任何需要它的人員取得。使用者擁有永久的長期憑證，但角色僅提供暫時憑證。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 中的一種身分，具備特定許可。它類似 IAM 使用者，但不與特定的人員相關聯。您可以在 AWS Management Console 中透過切換角色來暫時取得 IAM 角色。您可以透過呼叫 AWS CLI 或 AWS API 操作，或是使用自訂 URL 來取得角色。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。

使用臨時憑證的 IAM 角色在下列情況中非常有用：

- 暫時 IAM 使用者許可 – 使用者可以擔任 IAM 角色來暫時針對特定任務採用不同的許可。

- 聯合身分使用者存取 – 並非建立 IAM 使用者，而是使用來自 AWS Directory Service、您的企業使用者目錄或 Web 身分供應商現有的使用者身分。這些稱為聯合身分使用者。透過身分供應商來請求存取時，AWS 會指派角色給聯合身分使用者。如需聯合身分使用者的詳細資訊，請參閱 IAM 使用者指南中的聯合身分使用者和角色。
- 跨帳戶存取 – 您可以使用 IAM 角色，允許不同帳戶中的某人 (信任的委託人) 存取您帳戶的資源。角色是授予跨帳戶存取的主要方式。但是，針對某些 AWS 服務，您可以將政策直接連接到資源 (而非使用角色做為代理)。若要了解跨帳戶存取角色和資源類型政策間的差異，請參閱 IAM 使用者指南中的 IAM 角色與資源類型政策的差異。
- 跨服務存取 – 有些 AWS 服務會使用其他 AWS 服務中的功能。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存放在 Amazon S3 中。服務可能會使用呼叫委託人的許可、使用服務角色或使用服務連結角色來執行此作業。
  - 委託人許可 – 當您使用 IAM 使用者或角色在 AWS 中執行動作時，您會被視為委託人。政策能將許可授予委託人。當您使用某些服務時，您可能會執行一個動作，然後在不同的服務中觸發另一個動作。在此情況下，您必須具有執行這兩個動作的許可。若要查看某個動作是否需要原則中的其他相依動作，請參閱AWS Migration Hub 的動作、資源和條件金鑰重構空間中的服務授權參考。
  - 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。如需更多詳細資訊，請參閱 IAM 使用者指南中的建立角色以委派許可給 AWS 服務。
  - 服務連結角色 – 服務連結角色是一種連結到 AWS 服務的服務角色類型。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 IAM 帳戶中，並由該服務所擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。
- 在 Amazon EC2 上執行的應用程式 - 針對在 EC2 執行個體上執行並提出 AWS CLI 和 AWS API 請求的應用程式，您可以使用 IAM 角色來管理臨時登入資料。這是在 EC2 執行個體內存放存取金鑰的較好方式。若要指派 AWS 角色給 EC2 執行個體並提供其所有應用程式使用，您可以建立連接到執行個體的執行個體描述檔。執行個體描述檔包含該角色，並且可讓 EC2 執行個體上執行的程式取得臨時憑證。如需更多詳細資訊，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

您可以透過建立政策並將其連接到 IAM 身分或 AWS 資源，在 AWS 中控制存取。政策為 AWS 中的一個物件，當與身分或資源相關聯時，會定義它們的許可。您可以根使用者或 IAM 使用者的身分登入，或者可以擔任 IAM 角色。當您接著提出請求時，AWS 會評估相關以身分或資源為基礎的政策。政策中

的許可，決定是否允許或拒絕請求。大部分政策以 JSON 文件形式存放在 AWS 中。如需 JSON 政策文件結構和內容的詳細資訊，請參閱 IAM 使用者指南中的 JSON 政策概觀。

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個委託人可以對什麼資源以及在什麼條件下執行動作。

每個 IAM 實體 (使用者或角色) 在開始時都沒有許可。換句話說，根據預設，使用者無法執行任何作業，甚至也無法變更他們自己的密碼。若要授予使用者執行動作的許可，管理員必須將許可政策連接到使用者。或者，管理員可以將使用者新增到具備預定許可的群組。管理員將許可給予群組時，該群組中的所有使用者都會獲得那些許可。

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。具備該政策的使用者便可以從 AWS Management Console、AWS CLI 或 AWS API 取得角色資訊。

身分型政策

以身分為基礎的政策是可以附加到身分 (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。

身分類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。受管政策則是獨立的政策，您可以將這些政策連接到 AWS 帳戶 中的多個使用者、群組和角色。受管政策包含 AWS 受管政策和客戶受管政策。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。以資源為基礎的政策的最常見範例是 Amazon S3 儲存貯體政策和 IAM 角色信任政策。在支援以資源為基礎的政策的服務中，服務管理員可以使用它們來控制對特定資源的存取。對於附加政策的資源，政策會定義指定的委託人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委託人。委託人可以包括帳戶、使用者、角色、聯合身分使用者或 AWS 服務。

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

存取控制清單 (ACL)

存取控制清單 (ACL) 可控制哪些委託人 (帳戶成員、使用者或角色) 擁有存取某資源的許可。ACL 類似於以資源為基礎的政策，但它們不使用 JSON 政策文件格式。

Amazon S3、AWS WAF 和 Amazon VPC 是支援 ACL 的服務範例。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 支援其他較少見的政策類型。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類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。如需許可邊界的詳細資訊，請參閱 IAM 使用者指南中的 IAM 實體許可邊界。
- 服務控制政策 (SCP) – SCP 是 JSON 政策，可指定 AWS Organizations 中組織或組織單位 (OU) 的最大許可。AWS Organizations 服務可用來分組和集中管理您企業所擁有的多個 AWS 帳戶。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 會限制成員帳戶中的實體許可，包括每個 AWS 帳戶 的根使用者。如需 Organizations 和 SCP 的詳細資訊，請參閱 AWS Organizations 使用者指南中的 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，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 AWS 在涉及多種政策類型時如何判斷是否允許一項請求，請參閱 IAM 使用者指南中的政策評估邏輯。

AWS Migration Hub 重構空間如何搭配 IAM 使用

在您使用 IAM 管理對重構空間的存取權前，請了解可搭配重構空間使用的 IAM 功能有哪些。

您可以搭配 AWS Migration Hub 重構空間使用的 IAM 功能

IAM 功能	重構空間支援
以身分為基礎的政策	是
以資源為基礎的政策	是

IAM 功能	重構空間支援
政策動作	是
政策資源	是
政策條件金鑰	是
ACL	否
ABAC (政策中的標籤)	部分
暫時性憑證	是
主參與者權限	是
服務角色	否
服務連結角色	是

若要取得重構空間和其他AWS服務可與大多數 IAM 功能搭配使用，請參閱AWS可搭配 IAM 運作的服務中的IAM User Guide。

適用於重構空間的身分型政策

支援以身分為基礎的政策	是

以身分為基礎的政策是可以附加到身分 (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。您無法在以身分為基礎的政策中指定委託人，因為這會套用至連接的使用者或角色。若要了解您在 JSON 政策中使用的所有元素，請參閱《IAM 使用者指南》中的 JSON 政策元素參考。

適用於重構空間的身分型政策範例

若要檢視重構空間身分型政策的範例，請參閱AWS Migration Hub 重構空間的身分型政策範例。

重構空間內的資源型政策

支援以資源基礎的政策	是

資源型政策是連接到資源的 JSON 政策文件。以資源為基礎的政策的最常見範例是 Amazon S3 儲存貯體政策和 IAM 角色信任政策。在支援以資源為基礎的政策的服務中，服務管理員可以使用它們來控制對特定資源的存取。對於附加政策的資源，政策會定義指定的委託人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委託人。委託人可以包括帳戶、使用者、角色、聯合身分使用者或 AWS 服務。

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，做為資源型政策的委託人。新增跨帳戶委託人至資源型政策，只是建立信任關係的一半。當委託人和資源在不同的 AWS 帳戶 中時，受信任帳戶中的 IAM 管理員也必須授與委託人實體 (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予許可。不過，如果資源型政策會為相同帳戶中的委託人授予存取，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 角色與以資源為基礎的政策有何差異。

重構空間的原則動作

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哪些內容。也就是說，哪個委託人可以對什麼資源以及在什麼條件下執行動作。

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。政策動作的名稱通常會和相關聯的 AWS API 操作相同。有一些例外狀況，例如沒有相符的 API 作業的僅限許可動作。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操作的許可。

若要查看重構空間動作的清單，請參閱AWS Migration Hub 定義的動作重構空間中的服務授權參考。

重構空間中的政策動作會在動作之前使用以下字首：

```
refactor-spaces
```

若要在單一陳述式中指定多個動作，請用逗號分隔。

```
"Action": [
      "refactor-spaces:action1",
      "refactor-spaces:action2"
         ]
```

若要檢視重構空間身分型政策的範例，請參閱AWS Migration Hub 重構空間的身分型政策範例。

重構空間的原則資源

支援政策資源	是

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個委託人可以對什麼資源以及在什麼條件下執行動作。

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 資源名稱 (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 (例如列出作業)，請使用萬用字元 (*) 來表示陳述式適用於所有資源。

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

若要查看重構空間資源類型及其 ARN 的清單，請參閱AWS Migration Hub 定義的資源重構空間中的服務授權參考。若要了解您可以使用哪些動作指定每項資源的 ARN，請參閱AWS Migration Hub 定義的動作重構空間。

若要檢視重構空間身分型政策的範例，請參閱AWS Migration Hub 重構空間的身分型政策範例。

重構空間的原則條件索引鍵

支援政策條件金鑰	是

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個委託人可以對什麼資源以及在什麼條件下執行動作。

Condition 元素 (或 Condition「區塊」) 可讓您指定使陳述式生效的條件。Condition 元素是選用的。您可以建立使用條件運算子的條件表達式 (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 元素中指定多個金鑰，AWS 會使用邏輯 AND 操作評估他們。若您為單一條件金鑰指定多個值，AWS 會使用邏輯 OR 操作評估條件。必須符合所有條件，才會授予陳述式的許可。

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 支援全球條件金鑰和服務特定的條件金鑰。若要查看 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。

若要查看重構空格條件金鑰的清單，請參閱AWS Migration Hub 的條件金鑰重構空間中的服務授權參考。若要了解您可以針對何種動作及資源使用條件金鑰，請參閱AWS Migration Hub 定義的動作重構空間。

若要檢視重構空間身分型政策的範例，請參閱AWS Migration Hub 重構空間的身分型政策範例。

重構空間中的存取控制清單 (ACL)

支援 ACL	否

存取控制清單 (ACL) 可控制哪些委託人 (帳戶成員、使用者或角色) 擁有存取某資源的許可。ACL 類似於以資源為基礎的政策，但它們不使用 JSON 政策文件格式。

具備重構空間的屬性類型存取控制 (ABAC)

支援 ABAC (政策中的標籤)	部分

屬性為基礎的存取控制 (ABAC) 是一種授權策略，可根據屬性來定義許可。在 AWS 中，這些屬性稱為標籤。您可以將標籤連接到 IAM 實體 (使用者或角色)，以及許多 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，允許在委託人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。

如需 ABAC 的詳細資訊，請參閱《IAM 使用者指南》中的什麼是 ABAC?。若要查看具設定 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)。

搭配重構空間使用臨時憑證

支援暫時性憑證	是

當您使用暫時性憑證進行登入時，某些 AWS 服務無法運作。如需詳細資訊，包括哪些 AWS 服務搭配暫時性憑證使用，請參閱《IAM 使用者指南》中的可搭配 IAM 運作的 AWS 服務。

如果您使用使用者名稱和密碼之外的任何方法登入 AWS Management Console，則您正在使用暫時性憑證。例如，當您使用公司的單一登入(SSO)連結存取 AWS 時，該程序會自動建立暫時性憑證。當您以使用者身分登入主控台，然後切換角色時，也會自動建立暫時性憑證。如需切換角色的詳細資訊，請參閱《IAM 使用者指南》中的切換到角色 (主控台)。

您可使用 AWS CLI 或 AWS API，手動建立暫時性憑證。接著，您可以使用這些暫時性憑證來存取 AWS。AWS 建議您動態產生暫時性憑證，而非使用長期存取金鑰。如需詳細資訊，請參閱 IAM 中的暫時性安全憑證。

重構空間的跨服務主體權限

支援委託人許可權限	是

當您使用 IAM 使用者或角色在 AWS 中執行動作時，您會被視為委託人。政策能將許可授予委託人。當您使用某些服務時，您可能會執行一個動作，然後在不同的服務中觸發另一個動作。在此情況下，您必須具有執行這兩個動作的許可。若要查看某個動作是否需要原則中的其他相依動作，請參閱AWS Migration Hub 的動作、資源和條件金鑰重構空間中的服務授權參考。

重構空間的服務角色

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。如需更多詳細資訊，請參閱 IAM 使用者指南中的建立角色以委派許可給 AWS 服務。

> **Warning**
>
> 變更服務角色的權限可能會中斷「重構空間」功能。只有在重構空間提供指引時，才能編輯服務角色。

重構空間的服務連結角色

支援服務連結角色	是

服務連結角色是一種連結到 AWS 服務的服務角色類型。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 IAM 帳戶中，並由該服務所擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

如需建立或管理服務連結角色的詳細資訊，請參閱可搭配 IAM 運作的 AWS 服務。在表格中尋找服務，其中包含服務連結角色欄中的 Yes。選擇 Yes (是) 連結，以檢視該服務的服務連結角色文件。

AWSAWS Migration Hub Migration Hub 重構空間的受管政策

若要新增許可給使用者、群組和角色，使用 AWS 受管政策比自己撰寫政策更容易。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 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 受管政策。您無法更改 AWS 受管政策中的許可。服務偶爾會在 AWS 受管政策中新增其他許可以支援新功能。此類型的更新會影響已連接政策的所有身分識別 (使用者、群組和角色)。當新功能啟動或新操作可用時，服務很可能會更新 AWS 受管政策。服務不會從 AWS 受管政策中移除許可，因此政策更新不會破壞您現有的許可。

AWS受管政策：外觀設定因子空間完全存取

您可以將 AWSMigrationHubRefactorSpacesFullAccess 政策連接到 IAM 身分。

所以此AWSMigrationHubRefactorSpacesFullAccess政策授與 AWS Migration Hub 重構空間、重構空間主控台功能以及其他相關AWS服務。

許可詳細資訊

所以此AWSMigrationHubRefactorSpacesFullAccess政策內容如下。

- refactor-spaces— 允許 IAM 使用者帳戶完整存取重構空間。
- ec2— 允許 IAM 使用者帳戶執行重構空間使用的 Amazon Elastic Compute Cloud (Amazon EC2) 操作。
- elasticloadbalancing— 允許 IAM 使用者帳戶執行「重構空間」所使用的「Elastic Load Balancing」作業。
- apigateway— 允許 IAM 使用者帳戶執行重構空間使用的 Amazon API Gateway 操作。
- organizations— 允許 IAM 使用者帳戶AWS Organizations重構空間所使用的作業。
- cloudformation— 允許 IAM 使用者帳戶執行AWS CloudFormation作業，從主控台建立單鍵範例環境。
- iam— 允許為 IAM 使用者帳戶建立服務連結的角色，這是使用「重構空間」的必要條件。

重構空間的額外必要權限

在您可以使用「重構空間」之前，除了AWSMigrationHubRefactorSpacesFullAccess受管政策，必須將下列額外必要許可指派給您帳戶中的 IAM 使用者、群組或角色。

- 授予為建立服務連結角色的許可AWS Transit Gateway。
- 授與將虛擬私有雲 (VPC) 附加至所有資源呼叫帳戶的轉輸閘道的權限。
- 授予修改 VPC 端點服務的許可。
- 授與權限，以傳回所有資源的呼叫帳戶之已標記或先前已標記的資源。
- 授予執行所有AWS Resource Access Manager(AWS RAM) 所有資源上呼叫帳戶的動作。
- 授予執行所有AWS Lambda動作的呼叫帳戶。

您可以將內嵌政策新增至 IAM 使用者、群組或角色，以取得這些額外許可。不過，您可以使用下列政策 JSON 建立 IAM 政策，並將其附加至 IAM 使用者、群組或角色，而不使用內嵌政策。

下列原則會授與能夠使用重構空間所需的額外必要權限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:AWSServiceName": "transitgateway.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTransitGatewayVpcAttachment"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:ModifyVpcEndpointServicePermissions"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "tag:GetResources"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ram:*"
            ],
            "Resource": "*"
        },
        {
```

```
            "Effect": "Allow",
            "Action": [
                "lambda:*"
            ],
            "Resource": "*"
        }
    ]
}
```

如下所示AWSMigrationHubRefactorSpacesFullAccess政策。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "RefactorSpaces",
            "Effect": "Allow",
            "Action": [
                "refactor-spaces:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcEndpointServiceConfigurations",
                "ec2:DescribeVpcs",
                "ec2:DescribeTransitGatewayVpcAttachments",
                "ec2:DescribeTransitGateways",
                "ec2:DescribeTags",
                "ec2:DescribeTransitGateways",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeInternetGateways"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
```

```
                "ec2:CreateTransitGateway",
                "ec2:CreateSecurityGroup",
                "ec2:CreateTransitGatewayVpcAttachment"
            ],
            "Resource": "*",
            "Condition": {
                "Null": {
                    "aws:RequestTag/refactor-spaces:environment-id": "false"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTransitGateway",
                "ec2:CreateSecurityGroup",
                "ec2:CreateTransitGatewayVpcAttachment"
            ],
            "Resource": "*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/refactor-spaces:environment-id": "false"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateVpcEndpointServiceConfiguration"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteTransitGateway",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:DeleteSecurityGroup",
                "ec2:DeleteTransitGatewayVpcAttachment",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:DeleteTags"
            ],
```

```
            "Resource": "*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/refactor-spaces:environment-id": "false"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DeleteVpcEndpointServiceConfigurations",
            "Resource": "*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/refactor-spaces:application-id": "false"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "elasticloadbalancing:CreateLoadBalancer"
            ],
            "Resource": "*",
            "Condition": {
                "Null": {
                    "aws:RequestTag/refactor-spaces:application-id": "false"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "elasticloadbalancing:DescribeLoadBalancers",
                "elasticloadbalancing:DescribeTags",
                "elasticloadbalancing:DescribeTargetHealth",
                "elasticloadbalancing:DescribeTargetGroups",
                "elasticloadbalancing:DescribeListeners"
```

```
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "elasticloadbalancing:RegisterTargets",
                "elasticloadbalancing:CreateLoadBalancerListeners",
                "elasticloadbalancing:CreateListener",
                "elasticloadbalancing:DeleteListener",
                "elasticloadbalancing:DeleteTargetGroup"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/refactor-spaces:route-id": [
                        "*"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "elasticloadbalancing:DeleteLoadBalancer",
            "Resource": "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-
spaces-nlb-*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "elasticloadbalancing:AddTags",
                "elasticloadbalancing:CreateListener"
            ],
            "Resource": "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-
spaces-nlb-*",
            "Condition": {
                "Null": {
                    "aws:RequestTag/refactor-spaces:route-id": "false"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "elasticloadbalancing:DeleteListener",
```

```
            "Resource": "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-
nlb-*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "elasticloadbalancing:DeleteTargetGroup",
                "elasticloadbalancing:RegisterTargets"
            ],
            "Resource": "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-
*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "elasticloadbalancing:AddTags",
                "elasticloadbalancing:CreateTargetGroup"
            ],
            "Resource": "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-
*",
            "Condition": {
                "Null": {
                    "aws:RequestTag/refactor-spaces:route-id": "false"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "apigateway:GET",
                "apigateway:DELETE",
                "apigateway:PATCH",
                "apigateway:POST",
                "apigateway:PUT",
                "apigateway:UpdateRestApiPolicy"
            ],
            "Resource": [
                "arn:aws:apigateway:*::/restapis",
                "arn:aws:apigateway:*::/restapis/*",
                "arn:aws:apigateway:*::/vpclinks",
                "arn:aws:apigateway:*::/vpclinks/*",
                "arn:aws:apigateway:*::/tags",
                "arn:aws:apigateway:*::/tags/*"
            ],
```

```
            "Condition": {
                "Null": {
                    "aws:ResourceTag/refactor-spaces:application-id": "false"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "apigateway:GET",
            "Resource": [
                "arn:aws:apigateway:*::/vpclinks",
                "arn:aws:apigateway:*::/vpclinks/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeOrganization"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudformation:CreateStack"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:AWSServiceName": "refactor-spaces.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
```

```
                    "iam:AWSServiceName": "elasticloadbalancing.amazonaws.com"
                }
            }
        }
    ]
}
```

「重構空間」會更新為AWS受管政策

檢視更新的詳細資訊AWS的受管政策，因為此服務開始追蹤這些變更。如需有關此頁面變更的自動提醒，請訂閱「重構空間文件歷程記錄」頁面上的 RSS 摘要。

變更	描述	日期
外觀設定因子空間完全存取—推出時提供的新政策	所以此AWSMigrationHubRefactorSpacesFullAccess 政策授予對重構空間、重構空間主控台功能及其他相關AWS服務。	2021 年 11 月 29 日
移轉因子空間服務角色原則—推出時提供的新政策	MigrationHubRefactorSpacesServiceRolePolicy 提供對AWS由 AWS Migration Hub 管理或使用的資源重構空間。AWSElastic Figration Figration Figration Figration 因子空間服務連結角色會使用該政策。	2021 年 11 月 29 日
重構空間開始追蹤變更	重構空間開始追蹤其AWS受管政策。	2021 年 11 月 29 日

AWS Migration Hub 重構空間的身分型政策範例

根據預設，IAM 使用者和角色沒有建立或修改重構空間資源的許可。他們也無法使用 AWS Management Console、AWS CLI 或 AWS API 執行任務。IAM 管理員必須建立 IAM 政策，授與使用

者和角色對其所需資源執行動作的許可權限。管理員接著必須將這些政策連接至需要這些許可的 IAM 使用者或群組。

若要了解如何使用這些範例 JSON 政策文件建立 IAM 身分型政策，請參閱 IAM 使用者指南中的在 JSON 標籤上建立政策。

主題

- 政策最佳實務
- 使用重構空間主控台
- 允許使用者檢視他們自己的許可

政策最佳實務

身分型政策相當強大。他們可以判斷您帳戶中的某個人員是否可以建立、存取或刪除重構 Space 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— 若要快速開始使用重構空間，請使用AWS受管政策，為您的員工提供他們需要的許可。這些政策已在您的帳戶中提供，並由 AWS 維護和更新。如需詳細資訊，請參閱 IAM 使用者指南中的開始搭配 AWS 受管政策使用許可。
- 授予最低權限 – 當您建立自訂政策時，請只授予執行任務所需要的許可。以最小一組許可開始，然後依需要授予額外的許可。這比一開始使用太寬鬆的許可，稍後再嘗試將他們限縮更為安全。如需詳細資訊，請參閱 IAM 使用者指南中的授予最低權限。
- 為敏感操作啟用 MFA – 為了增加安全，請要求IAM 使用者使用多重要素驗證 (MFA) 存取敏感資源或 API 操作。如需詳細資訊，請參閱 IAM 使用者指南中的在 AWS 中使用多重要素驗證 (MFA)。
- 使用政策條件以增加安全 – 在切實可行的範圍中，請定義您身分類型政策允許存取資源的條件。例如，您可以撰寫條件，指定請求必須來自一定的允許 IP 地址範圍。您也可以撰寫條件，只在指定的日期或時間範圍內允許請求，或是要求使用 SSL 或 MFA。如需詳細資訊，請參閱「」IAM JSON 政策元素：Condition中的IAM User Guide。

使用重構空間主控台

若要存取 AWS Migration Hub 重構 Spacration Hub 主控台，您必須擁有最基本的一組許可。這些許可必須允許您列出和檢視您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 (IAM 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，您不需要允許其最基本主控台許可。反之，只需允許存取符合您嘗試執行之 API 操作的動作就可以了。

為了確保使用者和角色仍可使用重構空間主控台，請將重構空間連接`ConsoleAccess`或者`ReadOnly` AWS受管政策傳遞給實體。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 使用者檢視連接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上，或是使用 AWS CLI 或 AWS API 透過編寫程式的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": "*"
        }
    ]
}
```

疑難排解 AWS Migration Hub 重構空間身分識別和存取

請使用以下資訊來協助您診斷和修正使用重構空間和 IAM 時可能遇到的常見問題。

主題

我未獲得在重構空間中執行動作

若 AWS Management Console 告知您並未獲得執行動作的授權，您必須聯絡您的管理員以取得協助。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 `refactor-spaces:`*`GetWidget`* 許可時發生。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 refactor-spaces: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 `refactor-spaces:`*`GetWidget`* 資源。

我未獲得執行 iam: PassRole 的授權

若您收到錯誤，告知您並未獲得執行 `iam:PassRole` 動作的授權，您必須聯絡您的管理員以取得協助。您的管理員是提供您使用者名稱和密碼的人員。要求該人員更新您的政策，允許您將角色傳遞給重構空間。

有些 AWS 服務允許您傳遞現有的角色至該服務，而無須建立新的服務角色或服務連結角色。若要執行此作業，您必須擁有將角色傳遞至該服務的許可。

以下範例錯誤會在名為`marymajor`會嘗試使用主控台在重構空間中執行動作。但是，動作要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 會請求管理員更新她的政策，允許她執行 iam:PassRole 動作。

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。若您遺失了秘密金鑰，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。執行此作業，可能會讓他人能夠永久存取您的帳戶。

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重構空間

若要允許其他人存取重構空間，您必須針對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。您接著必須將政策連接到實體，在重構空間中授予正確的許可。

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。

我想要允許我以外的人員AWS 帳戶來訪問我的重構空間資源

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對象取得該角色。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權限。

若要進一步了解，請參閱以下內容：

- 若要了解重構空間是否支援這些功能，請參閱AWS Migration Hub 重構空間如何搭配 IAM 使用。
- 若要了解如何存取您擁有的所有 AWS 帳戶 所提供的資源，請參閱 IAM 使用者指南中的將存取權提供給您所擁有的另一個 AWS 帳戶 中的 IAM 使用者。
- 若要了解如何將資源的存取權提供給第三方 AWS 帳戶，請參閱 IAM 使用者指南中的將存取權提供給第三方擁有的 AWS 帳戶。
- 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。

使用服務連結角色

AWS Migration Hub 重構空間使用AWS Identity and Access Management(IAM)服務連結角色。服務連結角色是直接連結至「重構空間」的一種特殊 IAM 角色類型。服務連結角色由 Researcing 的角色預先定義，並包含服務呼叫其他呼叫所有服務所需要的許可AWS服務。

服務連結角色可讓設定重構空間變得更輕鬆，因為您不必手動新增必要的許可。Resature Spaces 定義其服務連結角色的許可，除非另有定義，否則僅有 Resource Spaces 可以擔任其角色。定義的許可包括信任政策和許可政策，並且該許可政策不能連接到任何其他 IAM 實體。

您必須先刪除服務連結角色的相關資源，才能將其刪除。這樣可保護您的 Resoute Spaces 資源，避免您不小心移除資源的存取許可。

如需關於支援服務連結角色的其他服務的資訊，請參閱可搭配 IAM 運作的 AWS 服務，並尋找 Service-Linked Role (服務連結角色) 欄顯示為 Yes (是) 的服務。選擇具有連結的 Yes (是)，以檢視該服務的服務連結角色文件。

服務連結角色許可

重構空間會使用名為的服務連結角色AWS 服務性質表單中的因子空間並將其與移轉因子空間服務角色原則IAM 政策 — 提供對AWS由 AWS Migration Hub 管理或使用的資源重構空間。

AWSServiceRoleForAWSServiceRoleForAWSServiceRoleForAWSServiceRoleForAWSServiceRoleForAWS Compu

- `refactor-spaces.amazonaws.com`

以下是 AWSServiceRoleForElastic Compute Resource Name (ARN) 的 Amazon Resource Name)。

```
arn:aws:iam::111122223333:role/aws-service-role/refactor-spaces.amazonaws.com/
AWSServiceRoleForMigrationHubRefactorSpaces
```

重構空間使用AWS 服務性質表單中的因子空間執行跨帳戶變更時，服務連結的角色。此角色必須出現在您的帳戶中，才能使用「重構空間」。如果不存在，重構空間會在下列 API 呼叫期間建立它：

- `CreateEnvironment`
- `CreateService`
- `CreateApplication`
- `CreateRoute`

您必須具備 `iam:CreateServiceLinkedRole` 許可才能建立服務連結角色。若服務連結角色不存在於您的帳戶中，且無法建立服務連結角色，`Create`呼叫將失敗。除非您使用的是「重構空間」主控台，否則您必須先在 IAM 主控台中建立服務連結的角色，才能使用「重構空間」。

在目前登入的帳戶中進行變更時，重構 Space 不會使用服務連結角色。例如，建立應用程式時，「重構空間」會更新環境中的所有 VPC，以便它們可以與新增的 VPC 通訊。如果 VPC 位於其他帳戶中，重構空間會使用服務連結的角色，而`ec2:CreateRoute`權限來更新其他帳戶中的路由表。

若要進一步擴充建立應用程式範例，在建立應用程式時，Refactor Spaces 會更新位於`CreateApplication`呼叫。如此一來，VPC 就可以與環境中的其他 VPC 通訊。

呼叫者必須安裝`ec2:CreateRoute`權限，我們用來更新路由表。此權限存在於服務連結的角色中，但重構空間不會使用來電者帳戶中的服務連結的角色來取得此權限。相反，呼叫者必須具有`ec2:CreateRoute`許可。否則，呼叫會失敗。

您不能使用服務連結角色來提升您的許可。您的帳戶必須已經具有服務連結角色的權限，才能在呼叫帳戶中進行變更。所以此`AWSMigrationHubRefactorSpacesFullAccess`受管理的原則，以及授與額外必要權限的原則，會定義建立重構空間資源的所有必要權限。服務連結的角色是這些權限的子集，用於特定跨帳戶呼叫。如需有關 `AWSMigrationHubRefactorSpacesFullAccess` 的詳細資訊，請參閱 AWS受管政策：外觀設定因子空間完全存取。

Tags

當重構空間在您的帳戶中建立資源時，它們會以適當的重構空間資源識別碼加上標記。例 Transit Gateway，從`CreateEnvironment`被標記為`refactor-spaces:environment-id`標記的環境識

別碼作為值。API Gateway APICreateApplication被標記為refactor-spaces:application-id將應用程式識別碼做為值。這些標籤允許重構空間來管理這些資源。如果您編輯或移除標籤，重構空間將無法再更新或刪除資源。

MigrationHubRefactorSpacesServiceRolePolicy

名為的角色許可政策角色許可政策原則允許重構空間在指定資源上完成下列動作：

Amazon API Gateway 動作

- apigateway:PUT
- apigateway:POST
- apigateway:GET
- apigateway:PATCH
- apigateway:DELETE

Amazon Elastic Compute Cloud 操作

- ec2:DescribeNetworkInterfaces
- ec2:DescribeRouteTables
- ec2:DescribeSubnets
- ec2:DescribeSecurityGroups
- ec2:DescribeVpcEndpointServiceConfigurations
- ec2:DescribeTransitGatewayVpcAttachments
- ec2:AuthorizeSecurityGroupIngress
- ec2:RevokeSecurityGroupIngress
- ec2:DeleteSecurityGroup
- ec2:DeleteTransitGatewayVpcAttachment
- ec2:CreateRoute
- ec2:DeleteRoute
- ec2:DeleteTags

ec2:DeleteVpcEndpointServiceConfigurations

AWS Resource Access Manager 動作

ram:GetResourceShareAssociations

ram:DeleteResourceShare

ram:AssociateResourceShare

ram:DisassociateResourceShare

Elastic Load Balancing；動作

elasticloadbalancing:DescribeTargetHealth

elasticloadbalancing:DescribeListener

elasticloadbalancing:DescribeTargetGroups

elasticloadbalancing:RegisterTargets

elasticloadbalancing:CreateLoadBalancerListeners

elasticloadbalancing:CreateListener

elasticloadbalancing:DeleteListener

elasticloadbalancing:DeleteTargetGroup

elasticloadbalancing:DeleteLoadBalancer

elasticloadbalancing:AddTags

elasticloadbalancing:CreateTargetGroup

以下是顯示前述動作套用於哪些資源的完整政策：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
```

```
                "ec2:DescribeSubnets",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeVpcEndpointServiceConfigurations",
                "ec2:DescribeTransitGatewayVpcAttachments",
                "elasticloadbalancing:DescribeTargetHealth",
                "elasticloadbalancing:DescribeListeners",
                "elasticloadbalancing:DescribeTargetGroups",
                "ram:GetResourceShareAssociations"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:DeleteSecurityGroup",
                "ec2:DeleteTransitGatewayVpcAttachment",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:DeleteTags",
                "ram:DeleteResourceShare",
                "ram:AssociateResourceShare",
                "ram:DisassociateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/refactor-spaces:environment-id": "false"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DeleteVpcEndpointServiceConfigurations",
            "Resource": "*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/refactor-spaces:application-id": "false"
                }
            }
        },
        {
            "Effect": "Allow",
```

```
            "Action": [
                "elasticloadbalancing:RegisterTargets",
                "elasticloadbalancing:CreateLoadBalancerListeners",
                "elasticloadbalancing:CreateListener",
                "elasticloadbalancing:DeleteListener",
                "elasticloadbalancing:DeleteTargetGroup"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/refactor-spaces:route-id": [
                        "*"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "apigateway:PUT",
                "apigateway:POST",
                "apigateway:GET",
                "apigateway:PATCH",
                "apigateway:DELETE"
            ],
            "Resource": [
                "arn:aws:apigateway:*::/restapis",
                "arn:aws:apigateway:*::/restapis/*",
                "arn:aws:apigateway:*::/vpclinks/*",
                "arn:aws:apigateway:*::/tags",
                "arn:aws:apigateway:*::/tags/*"
            ],
            "Condition": {
                "Null": {
                    "aws:ResourceTag/refactor-spaces:application-id": "false"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "apigateway:GET",
            "Resource": "arn:aws:apigateway:*::/vpclinks/*"
        },
        {
```

```
            "Effect": "Allow",
            "Action": "elasticloadbalancing:DeleteLoadBalancer",
            "Resource": "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-
spaces-nlb-*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "elasticloadbalancing:AddTags",
                "elasticloadbalancing:CreateListener"
            ],
            "Resource": "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-
spaces-nlb-*",
            "Condition": {
                "Null": {
                    "aws:RequestTag/refactor-spaces:route-id": "false"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "elasticloadbalancing:DeleteListener",
            "Resource": "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-
nlb-*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "elasticloadbalancing:DeleteTargetGroup",
                "elasticloadbalancing:RegisterTargets"
            ],
            "Resource": "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-
*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "elasticloadbalancing:AddTags",
                "elasticloadbalancing:CreateTargetGroup"
            ],
            "Resource": "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-
*",
            "Condition": {
                "Null": {
```

```
                    "aws:RequestTag/refactor-spaces:route-id": "false"
                }
            }
        }
    ]
}
```

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。當您建立重構空間環境、應用程式、服務或路由AWS Management Console，AWS CLI，或AWSAPI，重構空間會為您建立服務連結角色。如需為建立服務連結角色的詳細資訊，請參閱服務連結角色許可。

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。當您建立重構 Spaces 環境、應用程式、服務或路由資源時，重構 Spaces 會再次為您建立服務連結角色。

編輯重構空間的服務連結角色

重構空間不允許您編輯 AWSServiceRoleForAWSServiceRoleForAWSServiceRoleForAWSServiceRoleForAWSServiceRoleForAWS 因為有各種實體可能會參考服務連結角色，所以您無法在建立角色之後變更角色名稱。然而，您可使用 IAM 來編輯角色描述。如需更多資訊，請參閱 IAM 使用者指南中的編輯服務連結角色。

刪除重構空間的服務連結角色

若您不再使用需要服務連結角色的功能或服務，我們建議您刪除該角色。如此一來，您就沒有未主動監控或維護的未使用實體。然而，在手動刪除服務連結角色之前，您必須先清除資源。

> **Note**
>
> 若重構 Spaces 服務在您試圖刪除資源時正在使用該角色，刪除可能會失敗。若此情況發生，請等待數分鐘後並再次嘗試操作。

若要刪除 AwsService 表單表單空間所使用的重構空間資源，請使用「重構空間」主控台刪除資源，或使用資源的刪除 API 作業。如需刪除 API 操作的詳細資訊，請參閱重構空間 API 參考。

使用 IAM 手動刪除服務連結角色

使用 IAM 主控台、AWS CLI，或AWSAPI 來刪除 AWSServiceRoleForAWSServiceRoleForAWSServiceRoleForAWSServiceRoleForAWSServiceRoleForForA 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。

重構 Space 服務連結角色的支援區域

重構 Spaces 支援在所有提供服務的區域中，使用服務連結角色。如需詳細資訊，請參閱 AWS 區域與端點。

AWS Migration Hub Rigration Hub 的合規驗證

在多 AWS Migration Hub 多個AWS合規計劃。這些計劃包括 SOC、PCI、FedRAMP、HIPAA 等等。

如需特定合規計劃範圍內的 AWS 服務清單，請參閱合規計劃範圍內的 AWS 服務。如需一般資訊，請參閱 AWS 合規計劃。

您可使用 AWS Artifact 下載第三方稽核報告。如需詳細資訊，請參閱 AWS Artifact 中的下載報告。

您使用 Reration Space 的合規責任，取決於資料的機密性、您公司的合規目標及適用法律和法規。AWS提供下列資源，以協助合規：

- 安全與合規快速入門指南 – 這些部署指南討論架構考量，並提供在 AWS 上部署以安全及合規為重心之基準環境的步驟。
- HIPAA 安全與合規架構白皮書 – 本白皮書說明公司可如何運用 AWS 來建立 HIPAA 合規的應用程式。
- AWS 合規資源 – 這組手冊和指南可能適用於您的產業和位置。
- AWS Config 開發人員指南中的使用規則評估資源 – AWS Config 可評估資源組態對於內部實務、業界準則和法規的合規狀態。
- AWS Security Hub – 此 AWS 服務可供您檢視 AWS 中的安全狀態，可助您檢查是否符合安全產業標準和最佳實務。

使用其他 服務

AWS Migration Hub 重構空間目前為預覽版本，並可能有所變更。

本節說明其他AWS與重構空間互動的服務。

使用 CloudFormation 建立重構空間資源

AWS Migration Hub 重構空間與AWS CloudFormation，這項服務可協助您建置您的AWS資源，以減少建立和管理資源和基礎架構的時間。您建立範本，描述所有AWS資源 (例如環境、應用程式、服務和路由)，以及AWS CloudFormation會為您佈建及設定這些資源。

當您使用AWS CloudFormation，您可以重複使用您的範本，以便重複且一致地設定您的「重構空間」資源。只需描述一次您的資源，即可在多個 AWS 帳戶與區域內重複佈建相同資源。

重構空間和 CloudFormation 模板

若要佈建和設定重構空間與相關服務的資源，您必須了解AWS CloudFormation模板。範本是以 JSON 或 YAML 格式化的文本檔案。而您亦可以透過這些範本的說明，了解欲在 AWS CloudFormation 堆疊中佈建的資源。如果您不熟悉 JSON 或 YAML，您可以使用 AWS CloudFormation Designer 協助您開始使用 AWS CloudFormation 範本。如需詳細資訊，請參閱 AWS CloudFormation 使用者指南中的什麼是 AWS CloudFormation Designer？。

重構空間支援建立環境、應用程式、服務和AWS CloudFormation。如需詳細資訊 (包括環境、應用程式、服務和路由的 JSON 和 YAML 範本範例)，請參閱AWS Migration Hub 重構空間中的AWS CloudFormation使用者指南。

範本範例

下列範例範本會建立虛擬私有雲端 (VPC) 和重構空間資源。當您選擇部署AWS CloudFormation範本來建立演示重構環境，從入門] 對話方塊中，下列範本會部署由重構空間主控台。

Example YAML 重構空格範本

```
AWSTemplateFormatVersion: '2010-09-09'
Description: This creates resources in one account.
Resources:
  VPC:
```

```
    Type: AWS::EC2::VPC
    Properties:
      CidrBlock: 10.2.0.0/16
      Tags:
        - Key: Name
          Value: VpcForRefactorSpaces
  PrivateSubnet1:
    Type: AWS::EC2::Subnet
    Properties:
      VpcId: !Ref VPC
      AvailabilityZone: !Select [ 0, !GetAZs  '' ]
      CidrBlock: 10.2.1.0/24
      MapPublicIpOnLaunch: false
      Tags:
        - Key: Name
          Value: RefactorSpaces Private Subnet (AZ1)
  PrivateSubnet2:
    Type: AWS::EC2::Subnet
    Properties:
      VpcId: !Ref VPC
      AvailabilityZone: !Select [ 1, !GetAZs  '' ]
      CidrBlock: 10.2.2.0/24
      MapPublicIpOnLaunch: false
      Tags:
        - Key: Name
          Value: RefactorSpaces Private Subnet (AZ2)
  RefactorSpacesTestEnvironment:
    Type: AWS::RefactorSpaces::Environment
    DeletionPolicy: Delete
    Properties:
      Name: EnvWithMultiAccountServices
      NetworkFabricType: TRANSIT_GATEWAY
      Description: "This is a test environment"
  TestApplication:
    Type: AWS::RefactorSpaces::Application
    DeletionPolicy: Delete
    DependsOn:
      - PrivateSubnet1
      - PrivateSubnet2
    Properties:
      Name: proxytest
      EnvironmentIdentifier: !Ref RefactorSpacesTestEnvironment
      VpcId: !Ref VPC
      ProxyType: API_GATEWAY
```

```
      ApiGatewayProxy:
        EndpointType: "REGIONAL"
        StageName: "admintest"
  AdminAccountService:
    Type: AWS::RefactorSpaces::Service
    DeletionPolicy: Delete
    Properties:
      Name: AdminAccountService
      EnvironmentIdentifier: !Ref RefactorSpacesTestEnvironment
      ApplicationIdentifier: !GetAtt TestApplication.ApplicationIdentifier
      EndpointType: URL
      VpcId: !Ref VPC
      UrlEndpoint:
        Url: "http://aws.amazon.com"
  RefactorSpacesDefaultRoute:
    Type: AWS::RefactorSpaces::Route
    Properties:
      RouteType: "DEFAULT"
      EnvironmentIdentifier: !Ref RefactorSpacesTestEnvironment
      ApplicationIdentifier: !GetAtt TestApplication.ApplicationIdentifier
      ServiceIdentifier: !GetAtt AdminAccountService.ServiceIdentifier
  RefactorSpacesURIRoute:
    Type: AWS::RefactorSpaces::Route
    DependsOn: 'RefactorSpacesDefaultRoute'
    Properties:
      RouteType: "URI_PATH"
      EnvironmentIdentifier: !Ref RefactorSpacesTestEnvironment
      ApplicationIdentifier: !GetAtt TestApplication.ApplicationIdentifier
      ServiceIdentifier: !GetAtt AdminAccountService.ServiceIdentifier
      UriPathRoute:
        SourcePath: "/cfn-created-route"
        ActivationState: ACTIVE
        Methods: [ "GET" ]
```

進一步了解 CloudFormation

若要進一步了解 AWS CloudFormation，請參閱下列資源：

- AWS CloudFormation
- 《AWS CloudFormation 使用者指南》
- AWS CloudFormation API 參考
- AWS CloudFormation 命令行介面使用者指南

使用記錄重構空間 API 呼叫AWS CloudTrail

AWS Migration Hub 重構空間與AWS CloudTrail，可提供記錄使用者、角色或AWS服務重構空間。CloudTrail 會將重構空間的所有 API 呼叫擷取為事件。擷取的呼叫包括從重構空間主控台進行的呼叫，以及對重構空間 API 操作的程式碼呼叫。如果您建立追蹤記錄，就可以持續傳送 CloudTrail 事件至 Amazon S3 儲存貯體，包括重構空間的事件。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 REST 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》。

重構 CloudTrail 中的空間資訊

當您建立帳戶時，系統即會在 AWS 帳戶中啟用 CloudTrail。此外，重構空間發生活動時，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 事件歷史記錄檢視事件。

如需您的事件記錄AWS帳戶 (包括重構空間的事件) 建立線索。追蹤能讓 CloudTrail 將日誌檔交付至 Amazon S3 儲存貯體。根據預設，當您在主控台建立追蹤記錄時，追蹤記錄會套用到所有 AWS 區域。該追蹤會記錄來自 AWS 分割區中所有區域的事件，並將日誌檔案交付到您指定的 Amazon S3 儲存貯體。此外，您可以設定其他 AWS 服務，以進一步分析和處理 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
- 從多個區域接收 CloudTrail 日誌檔案
- 從多個帳戶接收 CloudTrail 日誌檔案

CloudTrail 會記錄所有重構空間動作，並記載於中重構空間 API 參考。例如，對 `CreateEnvironment`、`GetEnvironment` 和 `ListEnvironments` 動作發出的呼叫會在 CloudTrail 記錄檔案中產生項目。

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

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

- 該請求是否由另一項 AWS 服務提出。

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

了解重構空間日誌檔案項目

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。

使用共用重構空間環境AWS RAM

AWS Migration Hub 重構空間與AWS Resource Access Manager(AWS RAM) 以啟用資源共用。AWS RAM服務可讓您將某些重構空間資源分享給其他AWS 帳戶或透過AWS Organizations。您可以透過 AWS RAM 建立資源共享，以分享您擁有的資源。資源共享指定要分享的資源，以及共用它們的消費者。消費者可以包括：

- SPCAWS 帳戶組織內外AWS Organizations
- 之組織內的組織單位AWS Organizations
- 中的整個組織AWS Organizations

如需 AWS RAM 的詳細資訊，請參閱《AWS RAM 使用者指南》。

如需共用重構空間環境的詳細資訊，請參閱步驟 3：共享您的環境 。

AWS Migration Hub 的配額

AWS Migration Hub Rotas Space 目前為預覽版本，並可能有所變更。

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。

若要檢視 AWS Migration Hub 重構空間的配額清單，請參閱重構空間服務配額。

您也可以檢視重構空間的配額，方法是開啟Service Quotas 主控台。在導覽窗格中，選擇AWS服務，然後選取AWS Migration Hub 重構空間。

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。

重構空間使用者指南的文件歷史記錄

AWS Migration Hub 重構空間目前為預覽版本，並可能有所變更。

下表說明「重構空間」的文件版本。

update-history-change	update-history-description	update-history-date
初始版本	《重構空間使用者指南》的初始版本	2021 年 11 月 29 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。