使用者指南

AWS Resource Access Manager

AWS Resource Access Manager: 使用者指南

Table of Contents

什麼是 AWS Resource Access Manager？

AWS Resource Access Manager(AWS RAM) 可協助您在組織或組織單位 (OU) 之間AWS 帳戶安全地共用資源，以及支援的資源類型與AWS Identity and Access Management (IAM) 角色和使用者共用資源。如果您有多個資源AWS 帳戶，則可以建立一次資源，然後AWS RAM使用該資源供其他帳號使用。如果您的帳戶由管理AWS Organizations，您可以與組織中的所有其他帳號共用資源，或僅與一或多個指定組織單位 (OU) 所包含的帳號共用資源。您也可以AWS 帳戶透過帳戶 ID 與特定帳戶共用，無論帳戶是否屬於組織。某些支援的資源類型也可讓您與指定的 IAM 角色和使用者共用這些資源類型。

內容

影片概述

下列影片提供如何建立資源共用的簡短介影片。AWS RAM如需詳細資訊，請參閱???。

以下影片示範如何將AWS受管理的權限套用至資AWS源。如需詳細資訊，請參閱???。

此影片示範如何依照最低權限的最佳實務來建立客戶受管權限，並建立客戶受管權限。如需詳細資訊，請參閱 ???。

AWS RAM 的優點

為什麼要使用 AWS RAM？ 它具有以下優點：

- 減少作業額外負荷 — 建立一次資源，然後用AWS RAM來與其他帳號共用該資源。您就不需在每個帳戶中佈建重複的資源，進而降低營運開銷。在擁有資源的帳號內，可AWS RAM簡化授與該帳號中每個角色和使用者的存取權，而不必使用以識別為基礎的權限原則。

- 提供安全性和一致性 — 使用單一原則和權限集，簡化共用資源的安全性管理。如果您要改為在所有個別帳戶中建立重複的資源，則必須執行相同的政策和權限，然後必須在所有這些帳戶之間保持相同的資源。而是由一組策略和權限管理AWS RAM資源共用的所有使用者。 AWS RAM為共享不同類型的AWS資源提供了一致的體驗。
- 提供可見性和可稽核性 — 透過AWS RAM與 Amazon 和的整合，檢視共用資源的使用詳細 CloudWatch 資訊AWS CloudTrail。 AWS RAM提供共用資源和帳戶的全面能見度。

如何使用以資源為基礎的政策進行跨帳戶存取？

您可以將AWS資源型政策附加在您的外部識別AWS Identity and Access Management (IAM) 主體 (IAM 角色和使用者)，以便與其AWS 帳戶他人共用某些類型的資源AWS 帳戶。不過，透過附加政策來共用資源並不會利用AWS RAM提供的額外好處。通過使用，AWS RAM您可以獲得以下功能：

- 您可以與組織或組織單位 (OU) 共用，而不必列舉每個AWS 帳戶 ID。
- 使用者可以直接在原始AWS 服務控制台和 API 操作中查看與他們共用的資源，就好像這些資源直接在使用者的帳戶中一樣。例如，如果您使用與其他帳戶共用 Amazon VPC 子網路，該帳戶中的使用者可以在 Amazon VPC 主控台中看AWS RAM到子網路，以及在該帳戶中執行的 Amazon VPC API 操作結果。透過這種方式連接以資源為基礎的政策共用的資源不可見；相反，您必須透過其 Amazon 資源名稱 (ARN) 探索並明確參考資源。
- 資源的擁有者可以看到哪些主參與者可以存取他們已共用的每個個別資源。
- 如果您與不屬於組織的帳戶共用資源，請AWS RAM啟動邀請程序。收件者必須接受邀請，該委託人才可存取所共用的資源。開啟在組織內共用的功能後，與組織中的帳戶共用不需要邀請。

如果您有透過使用以資源為基礎的權限原則共用的資源，則可以執行下列任一動作，將這些資源升級為完全AWS RAM受控的資源：

- 使用 PromoteResourceShareCreatedFromPolicy API 操作
- 使用 API 作業的等效項目，即AWS Command Line Interface (AWS CLI) promote-resource-share-created-from-policy命令。

資源共用的運作方式

當您與另一個AWS 帳戶使用帳號共用擁有帳號中的資源時，您正在授與共用資源的使用帳號中主參與者的存取權。套用至使用帳號中角色和使用者的任何策略和權限也會套用至共用資源。共用中的資源看起來像是AWS 帳戶您共用資源的原生資源。

您可以共用全球和區域資源。如需詳細資訊，請參閱與全球資源相比，共享區域資源。

分享您的資源

您可以透過 AWS RAM 建立資源共享，以分享您擁有的資源。若要建立資源共用，您可以指定下列項目：

- 您想要建立資源共享。AWS 區域在主控台中，您可以從主控台的右上角的區域下拉式選單進行選擇。在中AWS CLI，您可以使用`--region`參數。
  - 資源共用只能包含與資源共用相AWS 區域同的區域資源。
  - 只有當資源共用位於全球資源的指定本地區域 (美國東部 (維吉尼亞北部) 時，資源共用才能包含全域資源`us-east-1`。
- 資源共享的名稱。
- 您要授與存取權作為此資源共用一部分的資源清單。
- 您可授與資源共用存取權的委託人。主參與者可以是個人AWS 帳戶、組織中的帳戶或組織單位 (OU)AWS Organizations，也可以是個別AWS Identity and Access Management (IAM) 角色或使用者。

  > **Note**
  >
  > 並非所有資源類型都可與 IAM 角色和使用者共用。如需可與這些主參與者共用之資源的相關資訊，請參閱可共用 AWS 的資源。

- 與您包含在資源共用中的每個資源類型相關聯的受管理權限。受管理的權限決定了其他帳號中的主參與者可以對資源共用中的資源執行的動作。

  權限的行為取決於主體的類型：

  - 如果主參與者與擁有資源的帳號不同，則附加至資源共用的權限就是可授與這些帳號中角色和使用者的最大權限。然後，這些帳戶的管理員必須透過 IAM 身分識別政策授與個別角色和使用者存取共用資源。在這些策略中授予的權限不能超過附加到資源共用的權限中定義的權限。

資源擁有帳號會保留其共用資源的完整擁有權。

使用共用資源

當資源的擁有者與您的帳戶共用資源時，您可以存取共用資源的方式，就像您的帳戶擁有共用資源一樣。您可以使用相關服務的主控台、AWS CLI命令和 API 操作來存取資源。您帳戶中的主體可以執行

的 API 作業視資源類型而有所不同，並且由附加至資源共用的AWS RAM權限指定。您帳戶中設定的所有 IAM 政策和服務控制政策也會繼續套用，讓您能夠利用現有在安全和治理控制方面的投資。

當您使用該資源的服務訪問共享資源時，您具有與擁有AWS 帳戶該資源的能力和限制相同。

- 如果資源是「地區」，則您只能從擁有帳戶AWS 區域中存在的資源來存取該資源。
- 如果資源是全域的，則您可以從資源的服務主控台和工具支援的任何AWS 區域資源存取資源。您只能在指定的本地區域美國東部 (維吉尼亞北部) 的AWS RAM主控台和工具中檢視和管理資源共用及其全域資源`us-east-1`。

存取 AWS RAM

您可以透過以下任何方式來使用 AWS RAM：

AWS RAM 主控台

AWS RAM 提供 Web 型使用者界面，亦即 AWS RAM 主控台。若您已註冊AWS 帳戶，您可登入AWS Management Console並從主AWS RAM控台首頁進行選擇AWS RAM來存取主控台。

您也可以在瀏覽器中直接導航到AWS RAM控制台。如果您尚未登入，系統會要求您在主機出現之前登入。

AWS CLI和視窗的工具 PowerShell

AWS CLI並提AWS Tools for PowerShell供對AWS RAM公共 API 操作的直接訪問。 AWS支援Windows、macOS和上的這些工具Linux。如需有關入門的詳細資訊，請參閱AWS Command Line Interface使用者指南或AWS Tools for Windows PowerShell使用者指南。如需命令的詳細資訊AWS RAM，請參閱命AWS CLI令參考或 C AWS Tools for Windows PowerShellmdlet 參考。

AWS SDK

AWS為各種程式語言提供 API 命令。如需有關入門的詳細資訊，請參閱 AWSSDK 和工具參考指南。

查詢 API

如果您不使用其中一種支援的程式設計語言，則AWS RAM HTTPS 查詢 API 可讓您以程式設計方式存取AWS RAM和AWS. 您可以透過AWS RAM API 直接向該服務發出 HTTPS 請求。當您使用 AWS RAM API 時，必須包含使用您的登入資料來數位簽署請求的程式碼。如需詳細資訊，請參閱 AWS RAM API 參考。

AWS RAM 的定價

使用AWS RAM或建立資源共用，以及跨帳號共用資源不會產生額外費用。資源用量會隨資源類型而異。如AWS需有關可共用資源的詳細資訊，請參閱該資源的擁有服務的文件。

符合規於國際標準

PCI DSS

AWS RAM支援處理、儲存、傳輸商家或服務供應商的信用卡資料，並且已驗證符合支付卡產業 (PCI) 資料安全標準 (DSS)。

如需 PCI DSS 的詳細資訊，包括如何索取 AWS PCI 合規套裝服務的副本，請參閱 PCI DSS 第 1 級。

FedRAMP

AWS RAM在下列使用 FedRAMP 中度AWS 區域：美國東部 (維吉尼亞北部)、美國西部 (加利佛尼亞北部)、美國西部 (加利佛尼亞北部) 及美國西部 (奧勒岡)。

AWS RAM在以下地區被授權為 FedRAMP 高點AWS 區域：AWS GovCloud （美國西部）和AWS GovCloud （美國東部）。

聯邦風險與授權管理計劃 (FedRAMP) 是一項美國政府整體計劃，提供標準化的方法，為雲端產品和服務進行安全評估、授權和持續監控。

如需 FedRAMP 合規性的詳細資訊，請參閱 FedRAMP。

晶片和 ISO

AWS RAM可用於受服務組織控制 (SOC) 合規性和國際標準化組織 (ISO)、ISO 27017、ISO 27018 和 ISO 27701 標準所影響的工作負載。金融、醫療保健和其他監管行業的客戶可以深入了解安全流程和控制措施，以保護 SOC 報告中可以找到的客戶數據，以及在中找到的AWS ISO 和 CSA STAR 證書AWS Artifact。

如需 SOC 合規性的詳細資訊，請參閱 SOC。

如需 ISO 相容性的詳細資訊，請參閱 ISO 9001、ISO 27017 和 ISO 27701。

AWS RAM 入門

同AWS Resource Access Manager，您能存取共用的。AWS 帳戶。如果您的帳戶由AWS Organizations，您也可以與組織中的其他帳號共用資源。您還可以使用其他人與您共享的資源AWS 帳戶。

如果您未在其中啟用共用功能AWS Organizations，您無法與組織或組織中的組織單位 (OU) 共用資源。但是，您仍然能存取共用的。AWS 帳戶在您的組織。對於支援的資源類型，您還可以與個人共享資源AWS Identity and Access Management(IAM) 組織中的角色或使用者。在此情況下，這些主參與者會被視為外部帳戶，而非組織的一部分。他們會收到加入資源共享的邀請，並且在接受邀請後便能存取共用的資源共享的邀請，並且在共享的邀請，並且

目錄

的術語和概念 AWS RAM

下列概念有助於說明如何使用 AWS Resource Access Manager (AWS RAM) 來共用資源。

資源共享

您可以透過建立資源共用 AWS RAM 來使用 共用資源。資源共享有下列三個元素：

- 要共用的一或多個 AWS 資源清單。
- 授予資源存取權的一或多個主體清單。
- 您在共用中包含的每種資源類型的受管許可。每個受管許可都適用於該資源共享中該類型的所有資源。

使用 AWS RAM 建立資源共用後，資源共用中指定的主體可以獲得共用資源的存取權。

- 如果您開啟與 AWS RAM 共用 AWS Organizations，且與 共用的委託人位於共用帳戶相同的組織中，只要這些委託人的帳戶管理員授予他們使用 資源的許可，就可以立即取得存取權 AWS Identity and Access Management IAM。

- 如果您未開啟與 Organizations AWS RAM 共享，您仍然可以與組織中 AWS 帳戶 的個人共享資源。耗用帳戶中的管理員會收到加入資源共享的邀請，而且他們必須先接受邀請，資源共享中指定的主體才能存取共用資源。
- 如果資源類型支援，您也可以與組織外部的帳戶共用。耗用帳戶中的管理員會收到加入資源共享的邀請，而且他們必須先接受邀請，資源共享中指定的主體才能存取共用資源。如需有關哪些資源類型支援這種共用類型的資訊，請參閱 可共用 AWS 的資源和檢視 可以與其組織欄外的帳戶共用。

共用帳戶

共用帳戶包含共用的資源，管理員可在其中使用 AWS RAM 建立 AWS 資源共用 AWS RAM。

AWS RAM 管理員是有權在 中建立和設定資源共用的IAM委託人 AWS 帳戶。由於 AWS RAM 的運作方式是將資源型政策連接至資源共用中的資源， AWS RAM 管理員也必須具有許可，才能 AWS 服務針對資源共用中包含的每個資源類型呼叫 中的 `PutResourcePolicy` 操作。

取用主體

耗用帳戶是共用資源 AWS 帳戶 的 。資源共享可以將整個帳戶指定為主體，或針對某些資源類型，指定帳戶中的個別角色或使用者。如需哪些資源類型支援這種共用類型的資訊，請參閱 可共用 AWS 的資源和檢視可與IAM角色和使用者共用欄。

AWS RAM 也支援服務主體做為資源共用的取用者。如需哪些資源類型支援這種共用類型的資訊，請參閱 可共用 AWS 的資源和檢視與服務主體共用欄。

耗用帳戶中的主體只能執行下列兩個許可允許的這些動作：

- 連接到資源共用的受管許可。這些指定可授予取用帳戶中主體的最大許可。
- 取用帳戶中的IAM管理員連接到個別角色或使用者的IAM身分型政策。這些政策必須授予共用帳戶中資源的指定動作和 Amazon Resource Name (ARN) 的`Allow`存取權。

AWS RAM 支援下列IAM主體類型作為資源共用的取用者：

- 另一個 AWS 帳戶 – 資源共用可讓共用帳戶中包含的資源可供取用帳戶使用。
- 另一個帳戶中的個別IAM角色或使用者 – 有些資源類型支援直接與個別IAM角色或使用者共用。依其指定此委託人類型ARN。
  - IAM 角色 – `arn:aws:iam::123456789012:role/rolename`
  - IAM 使用者 – `arn:aws:iam::123456789012:user/username`

- 服務主體 – 與 AWS 服務共用資源，以授予服務對資源共用的存取權。服務主體共享可讓 AWS 服務代表您採取動作，以減輕營運負擔。

  若要與服務委託人共用，請選擇允許與任何人共用，然後在選取委託人類型下，從下拉式清單中選擇服務委託人。以下列格式指定服務主體的名稱：

  - *service-id*.amazonaws.com

  為了降低混淆代理人的風險，資源政策會在aws:SourceAccount條件索引鍵中顯示資源擁有者的帳戶 ID。

- 組織中的帳戶 – 如果共用帳戶是由 管理 AWS Organizations，則資源共用可以指定要與組織中所有帳戶共用的組織 ID。資源共享可以或者指定組織單位 (OU) ID 來與該 OU 中的所有帳戶共享。共用帳戶只能與自己的組織或自己的組織中IDs的 OU 共用。依組織的 或 OU 在ARN組織中指定帳戶。

  - 組織中的所有帳戶 – 以下是 中組織ARN的範例 AWS Organizations：

    ```
    arn:aws:organizations::123456789012:organization/o-<orgid>
    ```

  - 組織單位中的所有帳戶 – 以下是 OU ID ARN的範例：

    ```
    arn:aws:organizations::123456789012:organization/o-<orgid>/ou-<rootid>-<ouid>
    ```

> **Important**
>
> 當您與組織或 OU 共用，且該範圍包含擁有資源共用的帳戶時，共用帳戶中的所有主體會自動存取共用中的資源。授予的存取是由與共用相關聯的受管許可所定義。這是因為 AWS RAM 連接到共用中每個資源的資源型政策使用 "Principal": "*"。如需詳細資訊，請參閱使用 的含意 "Principal": "*" 在資源型政策中。
> 其他耗用帳戶中的委託人不會立即存取共用的資源。其他帳戶的管理員必須先將身分型許可政策連接至適當的主體。這些政策必須授予 資源共用中個別資源ARNs的 Allow 存取權。這些政策中的許可不能超過與資源共用相關聯的受管許可中指定的許可。

以資源為基礎政策

資源型政策是實作IAM政策語言JSON的文字文件。與您連接到主體的身分型政策不同，例如IAM角色或使用者，您可以將資源型政策連接到 資源。 會根據您為資源共享提供的資訊，代表您 AWS RAM 撰寫資源型政策。您必須指定Principal政策元素，以決定誰可以存取資源。如需詳細資訊，請參閱IAM《 使用者指南》中的身分型政策和資源型政策。

產生的資源型政策 AWS RAM 會與所有其他IAM政策類型一起評估。這包括連接到嘗試存取資源之主體的任何身分IAM型政策，以及可能適用於 AWS Organizations 的服務控制政策 (SCPs) AWS 帳戶。產生的資源型政策會 AWS RAM 參與與所有其他IAM政策相同的政策評估邏輯。如需政策評估的完整詳細資訊，以及如何判斷產生的許可，請參閱IAM《 使用者指南》中的政策評估邏輯。

AWS RAM easy-to-use 透過提供抽象資源型政策，提供簡單且安全的資源共享體驗。

對於支援資源型政策的資源類型， AWS RAM 會自動為您建構和管理資源型政策。對於指定的資源， AWS RAM 會結合來自包含該資源之所有資源共用的資訊，以建置資源型政策。例如，考慮您使用 共用的 Amazon SageMaker AI 管道， AWS RAM 並包含在兩個不同的資源共用中。您可以使用一個資源共用來提供整個組織的唯讀存取權。然後，您可以使用其他資源共享，將 SageMaker AI 執行許可僅授予單一帳戶。 AWS RAM 會自動將這兩組不同的許可組合為具有多個陳述式的單一資源政策。然後，它會將合併的資源型政策連接到管道資源。您可以呼叫 來檢視此基礎資源政策 GetResourcePolicy operation. AWS 服務 然後，使用該資源型政策來授權任何嘗試對共用資源執行動作的委託人。

雖然您可以手動建立以資源為基礎的政策，並呼叫 將其連接至您的資源`PutResourcePolicy`，但我們建議您使用 AWS RAM ，因為它提供下列優點：

- 共用消費者的可探索性 – 如果您使用 共用資源 AWS RAM，使用者可以在擁有服務主控台和API操作的資源中直接看到與他們共用的所有資源，就像這些資源直接位於使用者帳戶中一樣。例如，如果您與其他帳戶共用 AWS CodeBuild 專案，耗用帳戶中的使用者可以在 CodeBuild 主控台和執行的操作 CodeBuild API結果中查看專案。直接連接以資源為基礎的政策所共用的資源不會以這種方式顯示。反之，您必須透過資源的 來探索並明確參考資源ARN。
- 共用擁有者的可管理性 – 如果您使用 共用資源 AWS RAM，共用帳戶中的資源擁有者可以集中查看哪些其他帳戶可以存取其資源。如果您使用以資源為基礎的政策共用資源，則只有在相關服務主控台或 中檢查個別資源的政策，才能查看耗用帳戶API。
- 效率 – 如果您使用 共用資源 AWS RAM，則可以共用多個資源，並將其作為一個單位進行管理。僅使用以資源為基礎的政策來共用的資源，需要將個別政策連接到您共用的每個資源。
- 簡單 – 使用 時 AWS RAM，您不需要了解 JSON型IAM政策語言。 AWS RAM 提供 ready-to-use AWS 受管許可，您可以從中選擇要連接至資源共享。

透過使用 AWS RAM，您甚至可以共用一些尚不支援資源型政策的資源類型。對於這類資源類型， AWS RAM 會自動產生以資源為基礎的政策，以表示實際的許可。使用者可以呼叫 來檢視此表示 GetResourcePolicy。 這包括下列資源類型：

- Amazon Aurora – 資料庫叢集

- Amazon EC2 – 容量保留和專用主機
- AWS License Manager – 授權組態
- AWS Outposts – 本機閘道路由表、前哨站和網站
- Amazon Route 53 – 轉送規則
- Amazon Virtual Private Cloud – 客戶擁有IPv4的地址、字首清單、子網路、流量鏡射目標、傳輸閘道和傳輸閘道多點傳送網域

AWS RAM 產生的資源型政策範例

如果您與個別帳戶共用EC2映像建置器映像資源， AWS RAM 會產生如下所示的政策，並將其連接到資源共用中包含的任何映像資源。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {"AWS": "arn:aws:iam::123456789012:root"},
            "Action": [
                "imagebuilder:GetImage",
                "imagebuilder:ListImages",
            ],
            "Resource": "arn:aws:imagebuilder:us-east-1:123456789012:image/
testimage/1.0.0/44"
        }
    ]
}
```

如果您與不同 中IAM的角色或使用者共用EC2映像建置器映像資源 AWS 帳戶， AWS RAM 會產生如下所示的政策，並將其連接至資源共用中包含的任何映像資源。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:role/MySampleRole"
      },
```

```
      "Action": [
          "imagebuilder:GetImage",
          "imagebuilder:ListImages",
      ],
      "Resource": "arn:aws:imagebuilder:us-east-1:123456789012:image/
testimage/1.0.0/44"
    }
  ]
}
```

如果您與組織中的所有帳戶或 OU 帳戶共用EC2映像建置器映像資源， AWS RAM 會產生如下所示的政策，並將其連接到資源共用中包含的任何映像資源。

> **Note**
>
> 此政策會使用 "Principal": "*" ，然後使用 "Condition"元素來限制許可給符合指定 的身分PrincipalOrgID。如需詳細資訊，請參閱使用 的含意 "Principal": "*" 在資源型政策中。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": [
                "imagebuilder:GetImage",
                "imagebuilder:ListImages",
            ],
            "Resource": "arn:aws:imagebuilder:us-east-1:123456789012:image/
testimage/1.0.0/44"
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "o-123456789"
                }
            }
        }
    ]
}
```

使用 的含意 "Principal": "*" 在資源型政策中

當您將 包含在以資源為基礎的政策"Principal": "*"中時，政策會授予 帳戶中包含資源的所有IAM主體存取權，如果存在，則受Condition元素施加的任何限制所約束。適用於呼叫主體的任何政策中的明確Deny陳述式會覆寫此政策授予的許可。不過，任何適用的身分政策、許可界限政策或工作階段政策中的隱含 Deny (表示缺少明確的 Allow) 不會導致 Deny授予這類資源型政策對 動作之存取權的委託人。

如果此行為不適合您的案例，則您可以將明確Deny陳述式新增至會影響相關角色和使用者的身分政策、許可界限或工作階段政策，以限制此行為。

受管許可

受管許可定義主體可以在資源共享中支援的資源類型上執行的動作。當您建立資源共用時，您必須指定要針對資源共用中包含的每個資源類型使用哪些受管許可。受管許可會列出主體可以使用 共用資源執行的一組 actions和 條件 AWS RAM。

您只能為資源共用中的每個資源類型連接一個受管許可。您無法建立資源共用，其中某些特定類型的資源使用一個受管許可，而其他相同類型的資源使用不同的受管許可。若要這樣做，您需要建立兩個不同的資源共用，並在其中分割資源，為每個集提供不同的受管許可。受管許可有兩種類型：

AWS 受管許可

AWS 受管許可是由 建立和維護 AWS ，並授予常見客戶案例的許可。 會為每個支援的資源類型 AWS RAM 定義至少一個 AWS 受管許可。有些資源類型支援多個 AWS 受管許可，其中有一個受管許可指定為 AWS 預設值。除非您另有指定，否則預設 AWS 受管許可會相關聯。

客戶受管許可

客戶受管許可是您編寫和維護的受管許可，可精確指定哪些動作可在使用 共用資源的條件下執行 AWS RAM。例如，您想要限制 Amazon VPC IP Address Manager (IPAM) 集區的讀取存取權，這可協助您大規模管理您的 IP 地址。您可以建立客戶受管許可，讓開發人員指派 IP 地址，但無法檢視其他開發人員帳戶指派的 IP 地址範圍。您可以遵循最低權限的最佳實務，只授予對共用資源執行任務所需的許可。

您可以在資源共享中定義資源類型的許可，並可選擇新增條件，例如全域內容金鑰和服務特定金鑰，以指定主體可以存取資源的條件。這些許可可用於一或多個 AWS RAM 共用。客戶受管許可是區域特定的。

AWS RAM 接受 受管許可做為輸入，為您共用的資源撰寫以資源為基礎的政策。

受管許可版本

受管許可的任何變更都會顯示為該受管許可的新版本。新版本是所有新資源共用的預設值。每個受管許可一律有一個指定為預設版本的版本。當您或 AWS 建立新的受管許可版本時，您必須明確更新每個現有資源共享的受管許可。您可以在此步驟中將變更套用至資源共享之前進行評估。所有新的資源共用都會自動使用對應資源類型的受管許可新版本。

AWS 受管許可版本

AWS 會處理受 AWS 管許可的所有變更。這類變更可解決新功能或移除發現的缺點。您只能將預設受管許可版本套用至資源共用。

客戶受管許可版本

您可以處理客戶受管許可的所有變更。您可以建立新的預設版本、將較舊版本設定為預設版本，或刪除不再與任何資源共用相關聯的版本。每個客戶受管許可最多可以有五個版本。

當您建立或更新資源共享時，您只能連接指定受管許可的預設版本。如需詳細資訊，請參閱將AWS受管理的權限更新至較新版本。

共用您的 AWS 資源

若要使用 共用您擁有的資源 AWS RAM，請執行下列動作：

- 在 中啟用資源共用 AWS Organizations (選用)
- 建立資源共用

> **備註**
>
> - 與 AWS 帳戶 擁有資源之 外部的主體共用資源，不會變更套用至建立資源之帳戶內資源的許可或配額。
> - AWS RAM 是區域性服務。您共用的主體只能存取建立資源共用 AWS 區域 的 。
> - 有些資源有特殊考量和共用的先決條件。如需詳細資訊，請參閱可共用 AWS 的資源。

在 中啟用資源共用 AWS Organizations

當您的帳戶由 管理時 AWS Organizations，您可以利用它來更輕鬆地共用資源。無論是否有 Organizations，使用者可以與個別帳戶共用。不過，如果您的帳戶位於組織中，則您可以與個別帳戶或組織或 OU 中的所有帳戶共用，而不必列舉每個帳戶。

若要在組織內共用資源，您必須先使用 AWS RAM 主控台或 AWS Command Line Interface (AWS CLI) 來啟用共用 AWS Organizations。當您在組織中共用資源時， AWS RAM 不會傳送邀請給委託人。組織中的主體可以存取共用資源，而無需交換邀請。

當您在組織中啟用資源共享時， 會 AWS RAM 建立稱為 的服務連結角色**AWSServiceRoleForResourceAccessManager**。此角色只能由 AWS RAM 服務擔任，並授予 AWS RAM 許可，以使用 AWS 受管政策 來擷取其所屬組織的相關資訊`AWSResourceAccessManagerServiceRolePolicy`。

如果您不再需要與整個組織或 共用資源OUs，您可以停用資源共用。如需詳細資訊，請參閱停用資源共用 AWS Organizations。

最低許可

若要執行下列程序，您必須以擁有下列許可的組織管理帳戶中的委託人身分登入：

- `ram:EnableSharingWithAwsOrganization`
- `iam:CreateServiceLinkedRole`
- `organizations:enableAWSServiceAccess`
- `organizations:DescribeOrganization`

要求

- 只有在以組織的管理帳戶中的委託人身分登入時，才能執行這些步驟。
- 組織必須啟用所有功能。如需詳細資訊，請參閱AWS Organizations 《 使用者指南》中的啟用組織中的所有功能。

> **Important**
>
> 您必須使用 AWS RAM 主控台或 enable-sharing-with-aws-organization AWS CLI 命令 AWS Organizations 來啟用與 的共用。此可確保建立了

AWSServiceRoleForResourceAccessManager 服務連結角色。如果您使用 AWS Organizations 主控台或 enable-aws-service-access AWS CLI 命令 AWS Organizations 啟用的信任存取，則不會建立AWSServiceRoleForResourceAccessManager服務連結角色，而且您無法在組織內共用資源。

Console

在您的組織中啟用資源共用

1. 在 AWS RAM 主控台中開啟設定頁面。
2. 選擇啟用與 共用 AWS Organizations，然後選擇儲存設定。

AWS CLI

在您的組織中啟用資源共用

使用 enable-sharing-with-aws-organization 命令。

此命令可用於任何 AWS 區域，並可在 AWS RAM 支援 AWS Organizations 的所有區域中與 共用。

```
$ aws ram enable-sharing-with-aws-organization
{
    "returnValue": true
}
```

建立資源共用

若要共用您擁有的資源，請建立資源共用。下列為此程序的概觀：

1. 新增您要共用的資源。
2. 針對您在共用中包含的每個資源類型，指定用於該資源類型的受管許可。
   - 您可以選擇其中一個可用的 AWS 受管許可、現有的客戶受管許可，或建立新的客戶受管許可。
   - AWS 建立受管許可 AWS ，以涵蓋標準使用案例。
   - 客戶受管許可可讓您自訂自己的受管許可，以符合您的安全和業務需求。

> **Note**
>
> 如果選取的受管許可有多個版本，則 AWS RAM 會自動連接預設版本。您只能連接指定為預設值的版本。

3. 指定您要存取資源的主體。

考量事項

- 如果您稍後需要刪除包含在共用中的 AWS 資源，建議您先從任何包含該資源共用中移除資源，或刪除資源共用。
- 您可以在資源共享中包含的資源類型列於 可共用 AWS 的資源。
- 只有在您擁有資源時，才能共用資源。您無法共用與您共用的資源。
- AWS RAM 是區域性服務。當您與其他 中的主體共用資源時 AWS 帳戶，這些主體必須從建立資源 AWS 區域 的相同位置存取每個資源。對於支援的全域資源，您可以從該資源的服務主控台和工具支援的任何 AWS 區域 存取這些資源。您只能在 AWS RAM 指定的主區域美國東部 （維吉尼亞北部） 中檢視這類資源共享及其全域資源`us-east-1`和工具。如需 AWS RAM 和 全域資源的詳細資訊，請參閱 與全球資源相比，共享區域資源。
- 如果您共用的 帳戶是 中組織的一部分， AWS Organizations 且在您的組織中共用已啟用，則您共用的組織中的任何主體都會自動獲得資源共用的存取權，而無需使用邀請。您在組織內容外與其共用的帳戶中的委託人會收到加入資源共用的邀請，並且只有在他們接受邀請之後，才會獲得共用資源的存取權。
- 如果您與服務委託人共用，則無法將任何其他委託人與資源共用建立關聯。
- 如果共用是在屬於組織一部分的帳戶或主體之間，則組織成員資格的任何變更都會動態影響對資源共用的存取。
  - 如果您將 AWS 帳戶 新增至組織或可存取資源共享的 OU，則該新成員帳戶會自動存取資源共享。您共用的帳戶管理員接著可以將該共用中資源的存取權授予該帳戶中的個別主體。
  - 如果您從組織或可存取資源共享的 OU 中移除帳戶，則該帳戶中的任何主體會自動失去透過該資源共享存取的資源存取權。
  - 如果您直接與成員帳戶或成員帳戶中IAM的角色或使用者共用，然後從組織中移除該帳戶，則該帳戶中的任何主體都會失去透過該資源共用存取的資源存取權。

> **Important**
>
> 當您與組織或 OU 共用，且該範圍包含擁有資源共用的帳戶時，共用帳戶中的所有主體會自動存取共用中的資源。授予的存取權是由與共用相關聯的受管許可所定義。這是因為 AWS RAM 連接到共用中每個資源的資源型政策使用 `"Principal": "*"`。如需詳細資訊，請參閱使用 的含意 "Principal": "*" 在資源型政策中。
> 其他耗用帳戶中的委託人不會立即存取共用的資源。其他帳戶的管理員必須先將身分型許可政策連接至適當的主體。這些政策必須授予 資源共用中個別資源ARNs的 `Allow` 存取權。這些政策中的許可不能超過與資源共用相關聯的受管許可中指定的許可。

- 您只能將帳戶所屬的組織，以及OUs從該組織新增至資源共享。您無法將來自自己組織外部的 OUs 或 組織以主體身分新增至資源共享。不過，您可以新增個人或 AWS 帳戶 支援的服務、IAM角色和來自組織外部的使用者，做為資源共用的主體。

> **Note**
>
> 並非所有資源類型都可以與IAM角色和使用者共用。如需您可以與這些委託人共用之資源的相關資訊，請參閱 可共用 AWS 的資源。

- 對於下列資源類型，您有七天的時間接受邀請，以加入下列資源類型的共用。如果您在邀請過期之前不接受邀請，則會自動拒絕邀請。

> **Important**
>
> 對於不在下列清單中的共用資源類型，您有 12 小時的時間接受加入資源共用的邀請。12 小時後，邀請會過期，且資源共享中的最終使用者主體會取消關聯。最終使用者無法再接受邀請。

  - Amazon Aurora – 資料庫叢集
  - Amazon EC2 – 容量保留和專用主機
  - AWS License Manager – 授權組態
  - AWS Outposts – 本機閘道路由表、前哨站和網站
  - Amazon Route 53 – 轉送規則
  - Amazon VPC – 客戶擁有IPv4的地址、字首清單、子網路、流量鏡射目標、傳輸閘道、傳輸閘道多點傳送網域

Console

建立資源共用

1. 開啟 AWS RAM 主控台。
2. 由於 AWS RAM 資源共用存在於特定 中 AWS 區域， AWS 區域 請從主控台右上角的下拉式清單中選擇適當的 。若要查看包含全域資源的資源共用，您必須 AWS 區域 將 設定為美國東部（維吉尼亞北部）、(us-east-1)。如需共用全域資源的詳細資訊，請參閱 與全球資源相比，共享區域資源。如果您想要在資源共享中包含全域資源，則必須選擇指定的主區域，美國東部（維吉尼亞北部），us-east-1。
3. 如果您是新手 AWS RAM，請從首頁選擇建立資源共享。否則，請從我共用：資源共用頁面中選擇建立資源共用。 https://console.aws.amazon.com/ram/home#OwnedResourceShares:
4. 在步驟 1：指定資源共用詳細資訊中，執行下列動作：

   a. 針對名稱，輸入資源共用的描述性名稱。

   b. 在資源下，選擇要新增至資源共用的資源，如下所示：

      - 對於選取資源類型，選擇要共用的資源類型。這會將可共用資源清單篩選為僅所選類型的資源。
      - 在產生的資源清單中，選取您要共用的個別資源旁的核取方塊。選取的資源會在選取的資源下移動。

        如果您要共用與特定可用區域相關聯的資源，則使用可用區域 ID (AZ ID) 可協助您判斷這些資源在帳戶之間的相對位置。如需詳細資訊，請參閱AWS資源的可用區域 ID。

   c. （選用）若要將標籤連接至資源共用，請在標籤下輸入標籤索引鍵和值。選擇新增標籤來新增其他標籤。視需要重複此步驟。這些標籤僅適用於資源共用本身，不適用於資源共用中的資源。
5. 選擇 Next (下一步)。
6. 在步驟 2：將受管許可與每個資源類型建立關聯，您可以選擇將 建立的受管許可 AWS 與資源類型建立關聯、選擇現有的客戶受管許可，或者您可以為支援的資源類型建立自己的客戶受管許可。如需詳細資訊，請參閱受管理的權限類型。

   選擇建立客戶受管許可，以建構符合共用使用案例需求的客戶受管許可。如需詳細資訊，請參閱 建立客戶受管許可。完成程序後，請選擇 ，  然後從受管許可下拉式清單中選擇您的新客戶受管許可。

> **Note**
>
> 如果選取的受管許可具有多個版本，則 AWS RAM 會自動連接預設版本。您只能連接指定為預設值的版本。

若要顯示受管許可允許的動作，請展開檢視此受管許可的政策範本。

7. 選擇 Next (下一步)。
8. 在步驟 3：授予主體存取權，執行下列動作：

   a. 根據預設，會選取允許與任何人共用，這表示對於支援該資源的那些資源類型，您可以與組織 AWS 帳戶 外部的資源共用資源。這不會影響只能在組織內共用的資源類型，例如 Amazon VPC子網路。您也可以與IAM角色和使用者共用一些支援的資源類型。

      若要將資源共用限制為組織中的 帳戶和主體，請選擇僅允許在您的組織中共用。

   b. 對於委託人，請執行下列動作：

      - 若要新增組織、組織單位 (OU) 或屬於組織的 AWS 帳戶 ，請開啟顯示組織結構。這會顯示組織的樹狀檢視。然後，選取您要新增的每個主體旁邊的核取方塊。

        > **Important**
        >
        > 當您與組織或 OU 共用，且該範圍包含擁有資源共用的帳戶時，共用帳戶中的所有主體會自動存取共用中的資源。授予的存取是由與共用相關聯的受管許可所定義。這是因為 AWS RAM 連接到共用中每個資源的資源型政策使用 `"Principal": "*"`。如需詳細資訊，請參閱使用 的含意 "Principal": "*" 在資源型政策中。
        > 其他耗用帳戶中的委託人不會立即存取共用的資源。其他帳戶的管理員必須先將身分型許可政策連接至適當的主體。這些政策必須授予資源共享中個別資源 ARNs的 `Allow` 存取權。這些政策中的許可不能超過與資源共用相關聯的受管許可中指定的許可。

      - 如果您選取組織 (ID 以 開頭o-)，則組織中所有 AWS 帳戶 中的主體都可以存取資源共用。

- 如果您選取 OU (ID 以 開頭ou-)，則該 OU 及其子系 AWS 帳戶 中所有 中的主體 OUs都可以存取資源共用。
- 如果您選取個人 AWS 帳戶，則只有該帳戶中的主體可以存取資源共用。

> **Note**
>
> 顯示組織結構切換只有在 AWS Organizations 已啟用與 共用，且您已登入組織的管理帳戶時才會顯示。
> 您無法使用此方法指定組織 AWS 帳戶 外部的 ，或是IAM角色或使用者。反之，您必須關閉顯示組織結構，並使用下拉式清單和文字方塊來輸入 ID 或 ARN。

- 若要依 ID 或 指定委託人ARN，包括組織外部的委託人，請針對每個委託人選取委託人類型。接著，輸入 ID （適用於 AWS 帳戶、組織或 OU) 或 ARN (適用於IAM角色或使用者），然後選擇新增。可用的委託人類型、ID 和ARN格式如下所示：
  - AWS 帳戶 – 若要新增 AWS 帳戶，請輸入 12 位數的帳戶 ID。例如：

    ```
    123456789012
    ```

  - 組織 – 若要新增 AWS 帳戶 組織中的所有 ，請輸入組織的 ID。例如：

    ```
    o-abcd1234
    ```

  - 組織單位 (OU) – 若要新增 OU，請輸入 OU 的 ID。例如：

    ```
    ou-abcd-1234efgh
    ```

  - IAM 角色 – 若要新增IAM角色，請輸入角色ARN的 。使用下列語法：

    ```
    arn:partition:iam::account:role/role-name
    ```

    例如：

    ```
    arn:aws:iam::123456789012:role/MyS3AccessRole
    ```

    > **Note**
    >
    > 若要取得IAM角色ARN的唯一 ，請在 IAM主控台中檢視角色清單、使用 get-role AWS CLI 命令或 GetRoleAPI動作。

  - IAM user – 若要新增IAM使用者，請輸入使用者的 ARN 。使用下列語法：

```
arn:partition:iam::account:user/user-name
```

例如：

```
arn:aws:iam::123456789012:user/bob
```

> **Note**
>
> 若要ARN取得IAM使用者的唯一 ，請在 IAM主控台中檢視使用者清單，請使用 get-user AWS CLI 命令，或 GetUser API 動作。

- 服務委託人 – 若要新增服務委託人，請從選取委託人類型下拉式清單中選擇服務委託人。 輸入 AWS 服務主體的名稱。使用下列語法：
  - *service-id*.amazonaws.com

    例如：

    ```
    pca-connector-ad.amazonaws.com
    ```

c. 對於選取的委託人，請確認您指定的委託人出現在清單中。

9. 選擇 Next (下一步)。
10. 在步驟 4：檢閱和建立中，檢閱資源共享的組態詳細資訊。若要變更任何步驟的組態，請選擇與您要返回的步驟對應的連結，並進行必要的變更。
11. 檢閱完資源共用後，請選擇建立資源共用。

    資源和委託人可能需要幾分鐘的時間才能完成關聯。在您嘗試使用資源共用之前，請先完成此程序。
12. 您可以隨時新增和移除資源和主體，或將自訂標籤套用至資源共用。您可以變更資源共用中包含的資源類型的受管許可，適用於支援超過預設受管許可的那些類型。當您不想再共用資源時，可以刪除資源共用。如需詳細資訊，請參閱分享您擁有的AWS資源。

AWS CLI

建立資源共用

使用 create-resource-share 命令。下列命令會建立與 AWS 帳戶 組織中所有 共用的資源共用。共用包含 AWS License Manager 授權組態，並授予該資源類型的預設受管許可。

> **Note**
>
> 如果您想要使用此資源共享中具有資源類型的客戶受管許可，您可以使用現有的客戶受管許可或建立新的客戶受管許可。記下客戶受管許可ARN的 ，然後建立資源共享。如需詳細資訊，請參閱建立客戶受管許可。

```
$ aws ram create-resource-share \
    --region us-east-1 \
    --name MyLicenseConfigShare \
    --permission-arns arn:aws:ram::aws:permission/
AWSRAMDefaultPermissionLicenseConfiguration \
    --resource-arns arn:aws:license-manager:us-east-1:123456789012:license-
configuration:lic-abc123 \
    --principals arn:aws:organizations::123456789012:organization/o-1234abcd
{
    "resourceShare": {
        "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/12345678-abcd-09876543",
        "name": "MyLicenseConfigShare",
        "owningAccountId": "123456789012",
        "allowExternalPrincipals": true,
        "status": "ACTIVE",
        "creationTime": "2021-09-14T20:42:40.266000-07:00",
        "lastUpdatedTime": "2021-09-14T20:42:40.266000-07:00"
    }
}
```

使用共用AWS資源

若要開始使用與您帳戶共用的資源AWS Resource Access Manager，請完成下列工作。

任務

- 回應資源共享邀請
- 使用與您共享的資源

回應資源共享邀請

如果您收到加入資源共用的邀請，您必須接受加入資源共用的邀請，您必須接受加入該資源共用的邀請，您

在下列情況況況況況況況況況況況況況況

- 如果您是中組織的一分子，AWS Organizations並已啟用與您所屬組織共用的功能，則組織中的主體便能自動存取所共用的資源。
- 如果您與擁有資源的共用，則AWS 帳戶該帳號中的主參與者會自動取得共用資源的存取權，而無需邀請。

Console

回應邀請

1. 在主控台中開啟 [與我共用：資源共用] 頁AWS RAM面。

   > **Note**
   >
   > 資源共用僅在建立資源共用的AWS 區域位置中可見。如果主控台中未顯示預期的資源共用，您可能需要AWS 區域使用右上角的下拉式控制項切換至其他資源共用。

2. 複查您已被授與存取權的資源共用清單。

   「狀態」(Status) 欄會指出您目前資源共用的參與狀態。狀Pending態表示您已新增至資源共用，但您尚未接受或拒絕邀請。

3. 若要回應資源共用邀請，請選取資源共用 ID，然後選擇 [接受資源共用] 以接受邀請，或選擇 [拒絕資源共用] 以拒絕邀請。如果您拒絕邀請，則無法存取這些資源。如果您接受邀請，就可以存取資源。

AWS CLI

若要開始，請取得可供您使用的資源共用邀請清單。下面的示例命令是在us-west-2區域中運行，並顯示一個資源共享在PENDING狀態中可用。

```
$ aws ram get-resource-share-invitations
{
    "resourceShareInvitations": [
```

```
        {
            "resourceShareInvitationArn": "arn:aws:ram:us-
west-2:111122223333:resource-share-invitation/1234abcd-ef12-9876-5432-aaaaaa111111",
            "resourceShareName": "MyNewResourceShare",
            "resourceShareArn": "arn:aws:ram:us-west-2:111122223333:resource-
share/1234abcd-ef12-9876-5432-bbbbbb222222",
            "senderAccountId": "111122223333",
            "receiverAccountId": "444455556666",
            "invitationTimestamp": "2021-09-15T15:00:32.568000-07:00",
            "status": "PENDING"
        }
    ]
}
```

您可以在下一個命令中使用邀請的 Amazon 資源名稱 (ARN) 作為下一個命令中的參數來接受該邀請。

```
$ aws ram accept-resource-share-invitation \
    --resource-share-invitation-arn arn:aws:ram:us-west-2:111122223333:resource-
share-invitation/1234abcd-ef12-9876-5432-aaaaaa111111
{
    "resourceShareInvitation": {
        "resourceShareInvitationArn": "arn:aws:ram:us-west-2:111122223333:resource-
share-invitation/1234abcd-ef12-9876-5432-aaaaaa111111",
        "resourceShareName": "MyNewResourceShare",
        "resourceShareArn": "arn:aws:ram:us-west-2:111122223333:resource-
share/1234abcd-ef12-9876-5432-bbbbbb222222",
        "senderAccountId": "111122223333",
        "receiverAccountId": "444455556666",
        "invitationTimestamp": "2021-09-15T15:14:12.580000-07:00",
        "status": "ACCEPTED"
    }
}
```

輸出顯示status已變更為ACCEPTED。包含在該資源共用中的資源現在可供接受帳號中的主參與者使用。

使用與您共享的資源

接受加入資源共用的邀請後，您可以對共用資源執行特定動作。這些動作會隨資源類型而異。如需詳細資訊，請參閱可共用 AWS 的資源。資源可直接在每個資源的服務主控台和 API/CLI 作業中使用。

如果資源是地區性的，則必須AWS 區域在服務主控台或 API/CLI 命令中使用正確的資源。如果資源是全域的，則您必須使用指定的主區域美國東部 (維吉尼亞北部)，`us-east-1`若要檢視中的資源AWS RAM，您必須開啟建立資源共用的AWS RAM主控台。AWS 區域

使用共用AWS資源

您可以使用AWS Resource Access Manager (AWS RAM) 來共用您擁有的AWS資AWS源，以及存取與您共用的資源。

內容

與全球資源相比，共享區域資源

本主題討論 AWS Resource Access Manager (AWS RAM) 如何使用區域和全球資源的差異。

資源是區域或全球性的。您可以使用 Amazon 資源名稱 (ARN) 中的第四個欄位來識別資源是區域資源還是全域資源。區域資源顯示AWS 區域. 如果它是空白的，那麼資源是全局的。

區域和全球資源有什麼區別？

區域資源

您可以共享的大多數資源AWS RAM都是區域。您在指定的中創建它們AWS 區域，然後它們存在於該區域中。若要查看這些資源或與這些資源互動，您必須將作業導向至該區域。例如，若要使用建立 Amazon 彈性運算雲端 (Amazon EC2) 執行個體AWS Management Console，請選擇要在其中 AWS 區域建立執行個體的執行個體。如果使用 AWS Command Line Interface (AWS CLI) 建立例證，則包括`--region`參數。每個 AWS SDK 都有自己的等效機制來指定操作使用的區域。

使用區域資源的原因有幾個。一個很好的理由是要確保資源以及您用來存取這些資源的服務端點盡可能接近客戶。這可將延遲降至最低，藉此改善效 另一個原因是提供隔離邊界。這可讓您在多個區域建立獨立的資源副本，以分配負載並改善延展性。同時，它會將資源彼此隔離，以提高可用性。

如果您在控制台或AWS CLI命令AWS 區域中指定了不同的資源，則您將無法再查看上一個「區域」中可以看到的資源或與之互動。

當您查看區域資源的 Amazon 資源名稱 (ARN) 時，會將包含資源的區域指定為 ARN 中的第四個欄位。例如，Amazon EC2 執行個體就是區域資源。此類資源的 ARN 看起來類似於區域中存在的 VPC 的下列範例。`us-east-1`

```
arn:aws:ec2:us-east-1:123456789012:instance/i-0a6f30921424d3eee
```

全球資源

某些AWS服務支持您可以在全球訪問的資源，這意味著您可以從任何地方使用資源。您不會AWS區域在全域服務的主控台中指定。若要存取全域資源，請勿在使用服務AWS CLI和 AWS SDK 作業時指定`--region`參數。

全域資源支援一次只能存在一個特定資源的一個執行個體至關重要的案例。在這種情況下，不同區域中的副本之間的複寫或同步處理不足。必須存取單一全域端點，但延遲可能會增加，因此可以接受，以確保資源的消費者可立即看到任何變更。例如，當您將 AWS Cloud WAN 核心網路建立為全域資源時，該網路對所有使用者都是一致的。它顯示為跨所有區域的單一、連續的全球網路。

全域資源的 Amazon 資源名稱 (ARN) 不包含區域。這種 ARN 的第四個字段是空的，例如下面的示例 ARN 用於雲 WAN 核心網絡。

```
arn:aws:networkmanager::123456789012:core-network/core-network-0514d38fa6f796cea
```

資源分享及其區域

AWS RAM是區域服務，資源共享是區域。因此，資源共用可以包含與資源共用相AWS 區域同的資源，以及任何受支援的全域資源。您在其中建立資源共用的區域是資源共用的本地區域。

> **Important**
>
> 目前，您只能在指定的本地區域美國東部 (維吉尼亞北部) 區域建立具有全域資源的資源共用us-east-1。雖然您只能在該單一主區域中建立資源共用，但在該服務的主控台或 CLI 和 SDK 作業中檢視時，任何共用全域資源都會顯示為標準全域資源。對本地區域的限制僅適用於資源共用，而不適用於其包含的資源。

若要共用您在區域中建立的us-west-2區域資源，您必須將AWS RAM主控台設定為使用us-west-2並在其中建立資源共用。您無法建立包含不同地區資源的資源共用AWS 區域。這表示若要共用us-west-2和的資源eu-north-1，您必須建立兩個不同的資源共用。您無法將來自兩個不同區域的資源合併為單一資源共用。

若要在AWS RAM主控台中共用全域資源，您必須將AWS RAM主控台設定為使用指定的本地區域美國東部 (維吉尼亞北部) us-east-1。然後，在指定的主區域中建立資源共用。您只能將資源共用中的全域資源與us-east-1區域的資源混合使用。

即使只能在指定的本地區域的AWS RAM資源共用中檢視全域資源，但在您共用之後，它仍然是全域資源。您可以AWS 帳戶從任何可以訪問原始區域的共享中訪問它AWS 帳戶。

考量事項

- 若要在AWS RAM主控台中建立資源共用，您必須使用包含您要共用之資源的 [區域]。如果您想要包含全域資源，則必須使用指定的主區域來建立共用。例如，若要共用 AWS Cloud WAN 核心網路，您必須在us-east-1區域中建立資源共用。
- 若要在AWS RAM主控台中檢視或修改資源共用，您必須使用包含資源共用的 [區域]。同樣地，AWS RAMAWS CLI和 SDK 作業可讓您只與您在作業中指定之「區域」中的資源共用互動。若要檢視或修改包含全域資源的資源共用率，您必須使用指定的本地區域美國東部 (維吉尼亞北部) us-east-1。
- 若要在AWS RAM主控台中檢視區域資源以將其包含在資源共用中，您必須使用包含區域資源的 [區域]。
- 若要在AWS RAM主控台中檢視全域資源以將其納入資源共用中，您必須使用指定的本地區域美國東部 (維吉尼亞北部) us-east-1。

- 您只能在指定的本地區域美國東部 (維吉尼亞北部) 建立包含區域和全球資源的資源共用***us-east-1***。

分享您擁有的AWS資源

您可以使用AWS Resource Access Manager (AWS RAM) 與您指定的主參與者共用您指定的資源。本節說明如何建立新的資源共用、修改現有的資源共用率，以及刪除不再需要的資源共用率。

主題

檢視您在其中建立的資源共用AWS RAM

您可以檢視已建立的資源共用清單。您可以查看共用的資源以及與之共用的主參與者。

Console

若要檢視您的資源共用率

1. 在主控台中開啟 [由我共用：資源共用] 頁AWS RAM面。
2. 由於AWS RAM資源共用存在於特定AWS 區域，因此請AWS 區域從主控台的右上角的下拉式清單中選擇適當的共用。若要查看包含全域資源的資源共用，您必須將設定AWS 區域為美國東部 (維吉尼亞北部), (us-east-1)。如需共享全域資源的詳細資訊，請參閱「與全球資源相比，共享區域資源」。
3. 如果結果中資源共用的任何受管理權限具有指定為預設值的新版受管理權限，則頁面會顯示標題以警示您。您可以選擇頁面頂端的 [檢閱並全部更新]，選擇一次更新所有受管理的權限版本。

   或者，對於具有一或多個新版本 Managed 權限的個別資源共用，[狀態] 欄會顯示 [可用的更新]。選擇該連結會開始檢閱更新的受管理權限版本的程序，並讓您將它們指派為該資源共用中相關資源類型的版本。

4. (選擇性) 套用篩選器以尋找特定資源共用率。您可以套用多個篩選條件，藉此縮小搜尋範圍。您可以輸入關鍵字 (例如資源共用名稱的一部分)，以僅列出名稱中包含該文字的資源共用。選擇文字方塊以查看建議屬性欄位的下拉式清單。選擇一個之後，您可以從該字段的可用值列表中進行選擇。您可以新增其他屬性或關鍵字，直到找到所需的資源為止。
5. 選擇要檢閱的資源共用的名稱。主控台會顯示下列有關資源共用的資訊：

   - 摘要 — 列出資源共用名稱、ID、擁有者、Amazon 資源名稱 (ARN)、建立日期、是否允許與外部帳戶共用及其目前狀態。
   - 受管理的權限 — 列出附加至此資源共用的受管理權限。資源共享中包含的每個資源類型最多可以有一個 Managed 許可。每個受管理的權限都會顯示與資源共用關聯的受管理權限版本。如果不是預設版本，則主控台會顯示 [更新為預設版本] 連結。如果您選擇該連結，則會提供您更新資源共用以使用預設版本的機會。
   - 共用資源 — 列出資源共用中包含的個別資源。選擇資源的 ID 以開啟新的瀏覽器索引標籤，以便在其原生服務的主控台中檢視資源。
   - 共用主參與者 — 列出與其共用資源的主參與者。
   - 標籤 — 列出附加至資源共用本身的標籤鍵值配對；這些不是附加至資源共用中包含之個別資源的標籤。

AWS CLI

若要檢視您的資源共用率

您可以在將參數`--resource-owner`設定為的情況下使用get-resource-shares指令，`SELF`以顯示在中建立的資源共用率的詳細資訊AWS 帳戶。

下列範例顯示在 currentAWS 區域 (`us-east-1`) 中為呼叫共用的資源共用率AWS 帳戶。若要取得在不同區域中建立的資源共用，請使用`--region` *<region-code>*參數。若要包含包含全域資源的資源共用率，您必須指定區域美國東部 (維吉尼亞北部)、`us-east-1`。

```
$  aws ram get-resource-shares \
    --resource-owner SELF
{
    "resourceShares": [
        {
            "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/2ebe77d7-4156-4a93-87a4-228568d04425",
            "name": "MySubnetShare",
            "owningAccountId": "123456789012",
```

```
            "allowExternalPrincipals": true,
            "status": "ACTIVE",
            "creationTime": "2021-09-10T15:38:54.449000-07:00",
            "lastUpdatedTime": "2021-09-10T15:38:54.449000-07:00",
            "featureSet": "STANDARD"
        },
        {
            "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/818d71dd-7512-4f71-99c6-2ae57aa010bc",
            "name": "MyLicenseConfigShare",
            "owningAccountId": "123456789012",
            "allowExternalPrincipals": true,
            "status": "ACTIVE",
            "creationTime": "2021-09-14T20:42:40.266000-07:00",
            "lastUpdatedTime": "2021-09-14T20:42:40.266000-07:00",
            "featureSet": "STANDARD"
        }
    ]
}
```


在 中建立資源共享 AWS RAM

若要共用您擁有的資源，請建立資源共用。下列為此程序的概觀：

1. 新增您要共用的資源。
2. 針對您在共用中包含的每個資源類型，指定用於該資源類型的受管許可。
   - 您可以選擇其中一個可用的 AWS 受管許可、現有的客戶受管許可，或建立新的客戶受管許可。
   - AWS 建立受管許可 AWS ，以涵蓋標準使用案例。
   - 客戶受管許可可讓您自訂自己的受管許可，以符合您的安全和業務需求。

> **Note**
>
> 如果選取的受管許可有多個版本，則 AWS RAM 會自動連接預設版本。您只能連接指定為預設值的版本。

3. 指定您要存取資源的主體。

考量事項

- 如果您稍後需要刪除包含在共用中的 AWS 資源，建議您先從任何包含該資源共用中移除資源，或刪除資源共用。
- 您可以在資源共享中包含的資源類型列於 可共用 AWS 的資源。
- 只有在您擁有資源時，才能共用資源。您無法共用與您共用的資源。
- AWS RAM 是區域性服務。當您與其他 中的主體共用資源時 AWS 帳戶，這些主體必須從建立資源 AWS 區域 的相同位置存取每個資源。對於支援的全域資源，您可以從該資源的服務主控台和工具支援的任何 AWS 區域 存取這些資源。您只能在 AWS RAM 指定的主區域美國東部 （維吉尼亞北部） 中檢視這類資源共享及其全域資源`us-east-1`和工具。如需 AWS RAM 和 全域資源的詳細資訊，請參閱 與全球資源相比，共享區域資源。
- 如果您共用的 帳戶是 中組織的一部分， AWS Organizations 且在您的組織中共用已啟用，則您共用的組織中的任何主體都會自動獲得資源共用的存取權，而無需使用邀請。您在組織內容外與其共用的帳戶中的委託人會收到加入資源共用的邀請，並且只有在他們接受邀請之後，才會獲得共用資源的存取權。
- 如果您與服務委託人共用，則無法將任何其他委託人與資源共用建立關聯。
- 如果共用是在屬於組織一部分的帳戶或主體之間，則組織成員資格的任何變更都會動態影響對資源共用的存取。
  - 如果您將 AWS 帳戶 新增至組織或可存取資源共享的 OU，則該新成員帳戶會自動存取資源共享。您共用的帳戶管理員接著可以將該共用中資源的存取權授予該帳戶中的個別主體。
  - 如果您從組織或可存取資源共享的 OU 中移除帳戶，則該帳戶中的任何主體會自動失去透過該資源共享存取的資源存取權。
  - 如果您直接與成員帳戶或成員帳戶中IAM的角色或使用者共用，然後從組織中移除該帳戶，則該帳戶中的任何主體都會失去透過該資源共用存取的資源存取權。

> **Important**
>
> 當您與組織或 OU 共用，且該範圍包含擁有資源共用的帳戶時，共用帳戶中的所有主體會自動存取共用中的資源。授予的存取權是由與共用相關聯的受管許可所定義。這是因為 AWS RAM 連接到共用中每個資源的資源型政策使用 `"Principal": "*"`。如需詳細資訊，請參閱使用 的含意 "Principal": "*" 在資源型政策中。
>
> 其他耗用帳戶中的委託人不會立即存取共用的資源。其他帳戶的管理員必須先將身分型許可政策連接至適當的主體。這些政策必須授予 資源共用中個別資源ARNs的 `Allow` 存取權。這些政策中的許可不能超過與資源共用相關聯的受管許可中指定的許可。

- 您只能將帳戶所屬的組織，以及OUs從該組織新增至資源共享。您無法將來自自己組織外部的 OUs 或 組織以主體身分新增至資源共享。不過，您可以新增個人或 AWS 帳戶 支援的服務、IAM角色和來自組織外部的使用者，做為資源共用的主體。

> **Note**
>
> 並非所有資源類型都可以與IAM角色和使用者共用。如需您可以與這些委託人共用之資源的相關資訊，請參閱 可共用 AWS 的資源。

- 對於下列資源類型，您有七天的時間接受邀請，以加入下列資源類型的共用。如果您在邀請過期之前不接受邀請，則會自動拒絕邀請。

> **Important**
>
> 對於不在下列清單中的共用資源類型，您有 12 小時的時間接受加入資源共用的邀請。12 小時後，邀請會過期，且資源共享中的最終使用者主體會取消關聯。最終使用者無法再接受邀請。

  - Amazon Aurora – 資料庫叢集
  - Amazon EC2 – 容量保留和專用主機
  - AWS License Manager – 授權組態
  - AWS Outposts – 本機閘道路由表、前哨站和網站
  - Amazon Route 53 – 轉送規則
  - Amazon VPC – 客戶擁有IPv4的地址、字首清單、子網路、流量鏡射目標、傳輸閘道、傳輸閘道多點傳送網域

Console

建立資源共用

1. 開啟 AWS RAM 主控台。
2. 由於 AWS RAM 資源共用存在於特定 中 AWS 區域， AWS 區域 請從主控台右上角的下拉式清單中選擇適當的 。若要查看包含全域資源的資源共用，您必須 AWS 區域 將 設定為美國東部 （維吉尼亞北部）、(us-east-1)。如需共用全域資源的詳細資訊，請參閱 與全球資源相

比，共享區域資源。如果您想要在資源共享中包含全域資源，則必須選擇指定的主區域，美國東部（維吉尼亞北部），us-east-1。

3. 如果您是新手 AWS RAM，請從首頁選擇建立資源共享。否則，請從我共用：資源共用頁面中選擇建立資源共用。 https://console.aws.amazon.com/ram/home#OwnedResourceShares:

4. 在步驟 1：指定資源共用詳細資訊中，執行下列動作：

   a. 針對名稱，輸入資源共用的描述性名稱。

   b. 在資源下，選擇要新增至資源共用的資源，如下所示：

      - 針對選取資源類型，選擇要共用的資源類型。這會將可共用資源清單篩選為僅所選類型的資源。
      - 在產生的資源清單中，選取您要共用的個別資源旁的核取方塊。選取的資源會在選取的資源下移動。

        如果您要共用與特定可用區域相關聯的資源，則使用可用區域 ID (AZ ID) 可協助您判斷這些資源在帳戶之間的相對位置。如需詳細資訊，請參閱AWS資源的可用區域 ID。

   c. （選用）若要將標籤連接至資源共享，請在標籤下輸入標籤索引鍵和值。選擇新增標籤來新增其他標籤。視需要重複此步驟。這些標籤僅適用於資源共用本身，不適用於資源共用中的資源。

5. 選擇 Next (下一步)。

6. 在步驟 2：將受管許可與每個資源類型建立關聯，您可以選擇將 建立的受管許可 AWS 與資源類型建立關聯、選擇現有的客戶受管許可，或者您可以為支援的資源類型建立自己的客戶受管許可。如需詳細資訊，請參閱受管理的權限類型。

   選擇建立客戶受管許可，以建構符合共用使用案例需求的客戶受管許可。如需詳細資訊，請參閱 建立客戶受管許可。完成此程序後，請選擇  ，然後從受管許可下拉式清單中選擇您的新客戶受管許可。

   > **Note**
   >
   > 如果選取的受管許可有多個版本，則 AWS RAM 會自動連接預設版本。您只能連接指定為預設值的版本。

   若要顯示受管許可允許的動作，請展開檢視此受管許可的政策範本。

7. 選擇 Next (下一步)。
8. 在步驟 3：授予主體存取權，執行下列動作：

   a. 根據預設，會選取允許與任何人共用，這表示對於支援該資源的那些資源類型，您可以與組織 AWS 帳戶 外部的資源共用資源。這不會影響只能在組織內共用的資源類型，例如 Amazon VPC子網路。您也可以與IAM角色和使用者共用一些支援的資源類型。

      若要將資源共用限制為組織中的 帳戶和主體，請選擇僅允許在組織中共用。

   b. 對於委託人，請執行下列動作：

      - 若要新增組織、組織單位 AWS 帳戶 (OU) 或屬於組織的 ，請開啟顯示組織結構。這會顯示組織的樹狀檢視。然後，選取您要新增的每個主體旁邊的核取方塊。

        > **Important**
        >
        > 當您與組織或 OU 共用，且該範圍包含擁有資源共用的帳戶時，共用帳戶中的所有主體會自動存取共用中的資源。授予的存取權是由與共用相關聯的受管許可所定義。這是因為 AWS RAM 連接到共用中每個資源的資源型政策使用 `"Principal": "*"`。如需詳細資訊，請參閱使用 的含意 "Principal": "*" 在資源型政策中。
        > 其他耗用帳戶中的委託人不會立即存取共用的資源。其他帳戶的管理員必須先將身分型許可政策連接至適當的主體。這些政策必須授予 資源共用中個別資源 ARNs的 `Allow` 存取權。這些政策中的許可不能超過與資源共用相關聯的受管許可中指定的許可。

      - 如果您選取組織 (ID 以 開頭o-)，則組織中所有 AWS 帳戶 中的主體都可以存取資源共用。
      - 如果您選取 OU (ID 以 開頭ou-)，則該 OU AWS 帳戶 中所有 的主體及其子項OUs都可以存取資源共用。
      - 如果您選取個人 AWS 帳戶，則只有該帳戶中的主體可以存取資源共用。

        > **Note**
        >
        > 顯示組織結構切換只有在 AWS Organizations 已啟用與 共用，且您已登入組織的管理帳戶時才會顯示。

您無法使用此方法指定組織 AWS 帳戶 外部的 ，或是IAM角色或使用者。反之，您必須關閉顯示組織結構，並使用下拉式清單和文字方塊來輸入 ID 或 ARN。

- 若要依 ID 或 指定委託人ARN，包括組織外部的委託人，請針對每個委託人選取委託人類型。接著，輸入 ID （適用於 AWS 帳戶、組織或 OU) 或 ARN（適用於IAM角色或使用者），然後選擇新增。可用的委託人類型、ID 和ARN格式如下所示：
  - AWS 帳戶 – 若要新增 AWS 帳戶，請輸入 12 位數的帳戶 ID。例如：

    ```
    123456789012
    ```

  - 組織 – 若要新增 AWS 帳戶 組織中的所有 ，請輸入組織的 ID。例如：

    ```
    o-abcd1234
    ```

  - 組織單位 (OU) – 若要新增 OU，請輸入 OU 的 ID。例如：

    ```
    ou-abcd-1234efgh
    ```

  - IAM 角色 – 若要新增IAM角色，請輸入角色ARN的 。使用下列語法：

    ```
    arn:partition:iam::account:role/role-name
    ```

    例如：

    ```
    arn:aws:iam::123456789012:role/MyS3AccessRole
    ```

    > **Note**
    >
    > 若要取得IAM角色ARN的唯一 ，請在 IAM主控台中檢視角色清單、使用 get-role AWS CLI 命令或 GetRoleAPI動作。

  - IAM user – 若要新增IAM使用者，請輸入使用者的 ARN 。使用下列語法：

    ```
    arn:partition:iam::account:user/user-name
    ```

    例如：

    ```
    arn:aws:iam::123456789012:user/bob
    ```

> **Note**
>
> 若要取得ARNIAM使用者的唯一 ，請在 IAM主控台中檢視使用者清單，請使用 get-user AWS CLI 命令，或 GetUser API 動作。

- 服務委託人 – 若要新增服務委託人，請從選取委託人類型下拉式清單中選擇服務委託人。 輸入 AWS 服務主體的名稱。使用下列語法：
  - *service-id*.amazonaws.com

    例如：

    pca-connector-ad.amazonaws.com

c. 對於選取的委託人，請確認您指定的委託人出現在清單中。

9. 選擇 Next (下一步)。
10. 在步驟 4：檢閱和建立中，檢閱資源共享的組態詳細資訊。若要變更任何步驟的組態，請選擇與您要返回的步驟對應的連結，並進行必要的變更。
11. 檢閱完資源共用後，請選擇建立資源共用。

    資源和委託人可能需要幾分鐘的時間才能完成關聯。在您嘗試使用資源共用之前，請先允許此程序完成。
12. 您可以隨時新增和移除資源和主體，或將自訂標籤套用至資源共用。您可以變更資源共享中包含的資源類型的受管許可，適用於支援超過預設受管許可的那些類型。當您不想再共用資源時，可以刪除資源共用。如需詳細資訊，請參閱分享您擁有的AWS資源。

AWS CLI

建立資源共用

使用 create-resource-share 命令。下列命令會建立與 AWS 帳戶 組織中所有 共用的資源共用。共用包含 AWS License Manager 授權組態，並授予該資源類型的預設受管許可。

> **Note**
>
> 如果您想要使用此資源共享中具有資源類型的客戶受管許可，您可以使用現有的客戶受管許可或建立新的客戶受管許可。記下客戶受管許可ARN的 ，然後建立資源共享。如需詳細資訊，請參閱建立客戶受管許可。

```
$ aws ram create-resource-share \
    --region us-east-1 \
    --name MyLicenseConfigShare \
    --permission-arns arn:aws:ram::aws:permission/
AWSRAMDefaultPermissionLicenseConfiguration \
    --resource-arns arn:aws:license-manager:us-east-1:123456789012:license-
configuration:lic-abc123 \
    --principals arn:aws:organizations::123456789012:organization/o-1234abcd
{
    "resourceShare": {
        "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/12345678-abcd-09876543",
        "name": "MyLicenseConfigShare",
        "owningAccountId": "123456789012",
        "allowExternalPrincipals": true,
        "status": "ACTIVE",
        "creationTime": "2021-09-14T20:42:40.266000-07:00",
        "lastUpdatedTime": "2021-09-14T20:42:40.266000-07:00"
    }
}
```

在 中更新資源共用 AWS RAM

您可以隨時 AWS RAM 以下列方式更新 中的資源共用：

- 您可以將主體、資源或標籤新增至您建立的資源共用。
- 對於支援超過預設 AWS 受管許可的資源類型，您可以選擇哪些受管許可適用於每種類型的資源。
- 當連接至資源共享的受管許可具有新的預設版本時，您可以更新受管許可以使用新版本。
- 您可以透過從資源共用中移除主體或資源，撤銷對共用資源的存取。如果您撤銷存取權，主體將無法再存取共用資源。

> **Note**
>
> 如果共用是空的，或僅包含支援離開資源共用的資源類型，則與您共用資源的主體可以離開資源共用。如果資源共用包含不支援離開的資源類型，則會出現訊息，通知主體他們必須聯絡共用擁有者。在此情況下，身為資源共用擁有者的您必須從資源共用中移除主體。如需不支援此動作的資源類型清單，請參閱 離開資源共用的先決條件。

Console

更新資源共用

1. 導覽至 主控台中的 AWS RAM 共用：資源共用頁面。
2. 由於 AWS RAM 資源共用存在於特定 中 AWS 區域， AWS 區域 請從主控台右上角的下拉式清單中選擇適當的 。若要查看包含全域資源的資源共用，您必須 AWS 區域 將 設定為美國東部（維吉尼亞北部）、(us-east-1)。如需共用全域資源的詳細資訊，請參閱與全球資源相比，共享區域資源。
3. 選取資源共用，然後選擇修改。
4. 在步驟 1：指定資源共用詳細資訊、檢閱資源共用詳細資訊，並視需要更新下列任何項目：
   a. （選用）若要變更資源共用的名稱，請編輯名稱。
   b. （選用）若要將資源新增至資源共用，請在資源下選擇資源類型，然後選取資源旁的核取方塊，將其新增至資源共用。只有當您在 中將區域設定為美國東部（維吉尼亞北部）、(us-east-1) 時，才會顯示全域資源 AWS Management Console。
   c. （選用）若要從資源共用中移除資源，請在選取的資源下尋找資源，然後選擇資源 ID 旁的 X。
   d. （選用）若要將標籤新增至資源共用，請在標籤下，在空白文字方塊中輸入標籤索引鍵和值。若要新增多個標籤索引鍵和值對，請選擇新增標籤。您最多可新增 50 個標籤。
   e. 若要從資源共用中移除標籤，請在標籤下找到標籤，然後選擇旁邊的移除。
5. 選擇 Next (下一步)。
6. （選用）在步驟 2：將受管許可與每個資源類型建立關聯，您可以選擇將 建立的受管許可 AWS 與資源類型建立關聯，選擇現有的客戶受管許可，或者您可以建立自己的客戶受管許可。如需詳細資訊，請參閱受管理的權限類型。

   您也可以選擇建立客戶受管許可，以建構符合共用使用案例需求的客戶受管許可。如需詳細資訊，請參閱建立客戶受管許可。完成程序後，請選擇

，

然後從受管許可下拉式清單中選取您的新客戶受管許可。

若要顯示受管許可允許的動作，請展開檢視此受管許可的政策範本。

7. 如果目前指派給資源共享的受管許可版本不是目前的預設版本，則您可以選擇更新為預設版本，以更新至預設版本。

> **Note**
>
> 在最後步驟之後儲存資源共用的變更之前，您可以選擇還原至先前版本來取消版本更新。不過，對於 AWS 受管許可，在您儲存資源共享之後，變更即為最終變更，您無法再返回先前的版本。

8. 選擇 Next (下一步)。
9. 在步驟 3：選擇允許存取的主體、檢閱選取的主體，並視需要更新下列任何項目：

   a. （選用）若要變更是否已啟用與組織內外主體的共用，請選擇下列其中一個選項：

      - 若要與組織外部的 AWS 帳戶 或個別IAM角色或使用者共用資源，請選擇允許與外部主體共用。
      - 若要將資源共用限制為組織中的主體 AWS Organizations，請選擇僅允許與組織中的主體共用。

   b. 對於委託人，請執行下列動作：

      - （選用）若要在 AWS 帳戶 組織內新增組織、組織單位 (OU) 或成員，請開啟顯示組織結構以顯示組織的樹狀檢視。然後選取您要新增的每個主體旁的核取方塊。

> **Important**
>
> 當您與組織或 OU 共用，且該範圍包含擁有資源共用的帳戶時，共用帳戶中的所有主體會自動存取共用中的資源。授予的存取權是由與共用相關聯的受管許可所定義。這是因為 AWS RAM 連接到共用中每個資源的資源型政策使用 `"Principal": "*"`。如需詳細資訊，請參閱使用 的含意 "Principal": "*" 在資源型政策中。
> 其他耗用帳戶中的委託人不會立即存取共用的資源。其他帳戶的管理員必須先將身分型許可政策連接至適當的主體。這些政策必須授予資源共享中個別資源

ARNs的 Allow 存取權。這些政策中的許可不能超過與資源共用相關聯的受管許可中指定的許可。

> **Note**
>
> 顯示組織結構切換只有在 AWS Organizations 啟用與 共用，而且您以組織管理帳戶中的主體身分登入時才會顯示。
> 您無法使用此方法指定組織 AWS 帳戶 外部的 ，或是IAM角色或使用者。相反地，您必須輸入這些主體的識別符，這些識別符會顯示在顯示組織結構切換下方的文字方塊中。請參閱下一個項目符號點。

- （選用）若要依主體識別符新增主體，請從下拉式清單中選擇主體類型，然後輸入主體ARN的 ID 或 。最後，選擇新增。

  如果您選取個人 AWS 帳戶，則只有該帳戶可以存取資源共用。您可以選擇下列其中一個選項。

  - 其他 AWS 帳戶 （資源擁有者除外）– 讓資源可供其他 帳戶使用。該帳戶的管理員必須使用以身分為基礎的許可政策，將共用資源的存取權授予個別角色和使用者，以完成此程序。這些許可不能超過附加至資源共用的受管許可中定義的許可。
  - 此 AWS 帳戶 （資源擁有者）– 資源擁有帳戶中的所有角色和使用者會自動接收附加至資源共用的受管許可所定義的存取權。
- 新增項目會立即顯示在選取的委託人清單中。

  然後，您可以透過重複此步驟來新增其他帳戶OUs、 或您的組織。
- （選用）若要移除委託人，請在選取的委託人下找到委託人，選取其核取方塊，然後選擇取消選取。

10. 選擇 Next (下一步)。
11. 在步驟 4：檢閱和更新中，檢閱資源共用的組態詳細資訊。
12. 若要變更任何步驟的組態，請選擇對應至您要返回之步驟的連結，然後進行必要的變更。

    如果任何受管許可仍在使用預設版本以外的版本，您可以選擇更新為預設版本來解決此問題。
13. 當您完成變更時，請選擇更新資源共用。

AWS CLI

更新資源共用

您可以使用下列 AWS CLI 命令來修改資源共用：

- 若要重新命名資源共享，或變更是否允許外部主體，請使用 命令 update-resource-share。 下列範例會重新命名指定的資源共用，並將其設定為僅允許其組織的主體。您必須針對包含資源共用的 AWS 區域 使用服務端點。

```
$ aws ram update-resource-share \
    --region us-east-1 \
    --resource-share-arn arn:aws:ram:us-east-1:123456789012:resource-
share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE \
    --name "my-renamed-resource-share" \
    --no-allow-external-principals
{
    "resourceShare": {
        "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE",
        "name": "my-renamed-resource-share",
        "owningAccountId": "123456789012",
        "allowExternalPrincipals": false,
        "status": "ACTIVE",
        "creationTime": 1565295733.282,
        "lastUpdatedTime": 1565303080.023
    }
}
```

- 若要將資源新增至資源共用，請使用 命令 associate-resource-share。 下列範例會將子網路新增至指定的資源共用。

```
$ aws ram associate-resource-share \
    --region us-east-1 \
    --resource-arns arn:aws:ec2:us-east-1:123456789012:subnet/
subnet-0250c25a1f4e15235 \
    --resource-share-arn arn:aws:ram:us-east-1:123456789012:resource-
share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE
{
    "resourceShareAssociations": [
        "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE",
```

```
        "associatedEntity": "arn:aws:ec2:us-east-1:123456789012:subnet/
subnet-0250c25a1f4e15235",
        "associationType": "RESOURCE",
        "status": "ASSOCIATING",
        "external": false
    ]
}
```

- 若要在資源共用中新增或取代資源類型的受管許可，請使用 命令 list-permissions 和 associate-resource-share-permission。 在資源共用中，每個資源類型只能指派一個受管許可。如果您嘗試將受管許可新增至已有受管許可的資源類型，則必須包含 `--replace`選項，否則命令會失敗並發生錯誤。

  下列範例命令會列出適用於 ARNs Amazon Elastic Compute Cloud (AmazonEC2) 子網路的受管許可的 ，然後使用其中一個ARNs來取代指定資源共用中該資源類型的目前指派 AWS 受管許可。

```
$ aws ram list-permissions \
    --resource-type ec2:Subnet
{
    "permissions": [
        {
            "arn": "arn:aws:ram::aws:permission/AWSRAMDefaultPermissionSubnet",
            "version": "1",
            "defaultVersion": true,
            "name": "AWSRAMDefaultPermissionSubnet",
            "resourceType": "ec2:Subnet",
            "creationTime": "2020-02-27T11:38:26.727000-08:00",
            "lastUpdatedTime": "2020-02-27T11:38:26.727000-08:00"
        }
    ]
}
$ aws ram associate-resource-share-permission \
    --region us-east-1 \
    --resource-share-arn arn:aws:ram:us-east-1:123456789012:resource-share/
f1d72a60-da19-4765-b4f9-e27b658b15b8 \
    --permission-arn arn:aws:ram::aws:permission/AWSRAMDefaultPermissionSubnet
{
    "returnValue": true
}
```

- 若要從資源共用中移除資源，請使用 命令 disassociate-resource-share。 下列範例會從指定的資源共用中移除具有 的 Amazon ARN EC2子網路。

```
$ aws ram disassociate-resource-share \
    --region us-east-1 \
    --resource-arns arn:aws:ec2:us-east-1:123456789012:subnet/
subnet-0250c25a1f4e15235 \
    --resource-share-arn arn:aws:ram:us-east-1:123456789012:resource-
share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE
{
    "resourceShareAssociations": [
        "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE",
        "associatedEntity": "arn:aws:ec2:us-east-1:ubnet/
subnet-0250c25a1f4e15235",
        "associationType": "RESOURCE",
        "status": "DISASSOCIATING",
        "external": false
    ]
}
```

- 若要修改連接至資源共享的標籤，請使用 命令 tag-resource 和 untag-resource。 下列範例會將標籤新增至project=lima指定的資源共用。

```
$ aws ram tag-resource \
    --region us-east-1 \
    --resource-share-arn arn:aws:ram:us-east-1:123456789012:resource-share/
f1d72a60-da19-4765-b4f9-e27b658b15b8 \
    --tags key=project,value=lima
```

下列範例project會從指定的資源共用中移除索引鍵為 的標籤。

```
$ aws ram untag-resource \
    --region us-east-1 \
    --resource-share-arn arn:aws:ram:us-east-1:123456789012:resource-share/
f1d72a60-da19-4765-b4f9-e27b658b15b8 \
    --tag-keys=project
```

標記命令成功時不會產生輸出。

檢視您在中的共用資源AWS RAM

您可以檢視在所有共享中，您已共用的個別資源。此清單可協助您判斷目前共用的資源、這些資源所包含的資源共用數目，以及可存取這些資源的主參與者數目。

Console

若要檢視您目前共用的資源

1. 在主控台中開啟「由我共用：共用資源」頁AWS RAM面。
2. 由於AWS RAM特定存在AWS 區域，因此請AWS 區域從主控台的右上角的下拉式清單中選擇適當的。若要查看包含全域唯一的共用，您必須將區域設定AWS 區域為美國東部 (維吉尼亞北部)、(us-east-1)。如需共用全域資源的相關詳細資訊，請參閱「與全球資源相比，共享區域資源」
3. 針對每項共用的資源，下列資訊可供使用：
   - ID。選擇資源的 ID 以開啟新的瀏覽器索引標籤，以便在其原生服務主控台中檢視資源。
   - 類型。
   - 上次共用日期 — 上次共用資源的日期。
   - 資源共用率 — 包含資源的資源共用數。若要查看資源共用的清單，請選擇數字。
   - 主參與者 — 可存取資源的主參與者數目。選擇要檢控主參與者。

AWS CLI

若要檢視您目前共用的資源

您可以在`--resource-owner`設定參數的情況下使用 list-resources 命令，`SELF`以顯示您目前共用之資源的詳細資訊。

下列範例顯示呼叫AWS 區域 (us-east-1) 中包含在資源共用中的資源AWS 帳戶。若要取得您在不同區域中共用的資源，請使用`--region` *<region-code>*參數。

```
$ aws ram list-resources \
    --region us-east-1 \
    --resource-owner SELF
{
    "resources": [
        {
```

```
            "arn": "arn:aws:license-manager:us-east-1:123456789012:license-
configuration:lic-ecbd5574fd92cb0d312baea260e4cece",
            "type": "license-manager:LicenseConfiguration",
            "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/818d71dd-7512-4f71-99c6-2ae57aa010bc",
            "creationTime": "2021-09-14T20:42:40.266000-07:00",
            "lastUpdatedTime": "2021-09-14T20:42:41.081000-07:00"
        },
        {
            "arn": "arn:aws:license-manager:us-east-1:123456789012:license-
configuration:lic-ecbd5574fd92cb0d312baea260e4cece",
            "type": "license-manager:LicenseConfiguration",
            "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-share/
a477f3b2-4001-4dcb-bd54-7c8d23b4f07d",
            "creationTime": "2021-07-22T11:48:11.104000-07:00",
            "lastUpdatedTime": "2021-07-22T11:48:11.971000-07:00"
        }
    ]
}
```

檢視您在中共用資源的主參與者AWS RAM

您可檢視在所有資源共享上，您與其共享上，您與其共享上的委託人。檢視此委託人清單可協助您判斷哪些人員可存取您共用資源的路由。

Console

若要檢視與您共用資源的主參與者

1. 導覽至主AWS RAM控台中的「由我共用：主參與者」頁面。
2. 由於特定區域中存在AWS RAM資源共享上AWS 區域，因此請AWS 區域從主控台的右上角的下拉式清單中選擇適當的共享路由。若要檢視包含全域資源的資源共享，您必須AWS 區域將美國東部 (維吉尼亞北部)、(us-east-1) 路由。如需共用全域資源的詳細資訊，請參閱與全球資源相比，共享區域資源路由路由
3. 套用篩選器以尋找特定主參與者。您可以套用多個篩選條件，藉此縮小搜尋範圍。選擇文字方塊以查看建議屬性欄位的下拉式清單。選擇一個之後，您可以從該字段的可用值列表中進行選擇。您可以新增其他屬性或關鍵字，直到找到所需的資源為止。
4. 對於清單中的每個主參與者，主控台會顯示下列資訊：

- 主體識別碼 — 主參與者的識別碼。選擇 ID 以開啟新的瀏覽器索引標籤，以便在其原生主控台中檢視主參與者。
- 資源共用率 — 您與指定主參與者共用的資源共用數目。選擇編號以檢視資源共享清單的編號以檢視路由路由
- 資源 — 您與主參與者共用的資源數目。選擇編號以檢視共用資源清單的編號以檢視共用資源

AWS CLI

若要檢視與您共用資源的主參與者

您可以使用 list- principal 命令來取得您在目前AWS 區域針對呼叫帳戶建立的資源共用中參照的主參與者清單。

下列範例會列出可存取在呼叫帳戶之預設 Region 中建立之共用的主參與者。在此範例中，主參與者是呼叫帳戶的組織，也是個別的組織AWS 帳戶，作為兩個不同資源共用的一部分。您必須針對包含資源共用AWS 區域的使用服務端點。

```
$ aws ram list-principals \
    --region us-east-1 \
    --resource-owner SELF
{
    "principals": [
        {
            "id": "arn:aws:organizations::123456789012:organization/o-a1b2c3dr",
            "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-share/
a477f3b2-4001-4dcb-bd54-7c8d23b4f07d",
            "creationTime": "2021-09-14T20:40:58.532000-07:00",
            "lastUpdatedTime": "2021-09-14T20:40:59.610000-07:00",
            "external": false
        },
        {
            "id": "111111111111",
            "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/6405fa7c-0786-4e15-8c9f-8aec02802f18",
            "creationTime": "2021-09-15T15:00:31.601000-07:00",
            "lastUpdatedTime": "2021-09-15T15:14:13.618000-07:00",
            "external": true
        }
    ]
```

```
}
```

刪除中的資源共用AWS RAM

您可以隨時刪除資源共享。當您刪除資源共用時，與資源共用相關聯的所有主參與者都會失去共用資源的存取權。刪除資源共用不會刪除共用資源。

> **若要刪除資AWS源**
>
> 如果您需要刪除包含在AWS資源共用中的資源，AWS建議您先確保從包含該資源共用的任何資源共用中移除該資源，或刪除資源共用。

刪除後，刪除的資源共用會在AWS RAM主控台中保持短時間內可見，但其狀態會變更為`Deleted`。

Console

刪除資源共享

1. 在主控台中開啟 [由我共用：資源共用] 頁AWS RAM面。
2. 由於特定的AWS RAM Resource NameAWS 區域，請AWS 區域從主控台右上角的下拉式清單中選擇適用的。若要查看包含全域資源的 Resource Name，您必須將設定AWS 區域為美國東部 (維吉尼亞北部`us-east-1`)。如需共用全域 Resource 的詳細資訊，請參閱與全球資源相比，共享區域資源。
3. 選取您想要刪除的 Resource Name。

   > **Warning**
   >
   > 請務必選取正確的 Resource Name。刪除資源共享後就無法復原。

4. 選擇「刪除」，然後在確認訊息中選擇「刪除」。
5. 刪除的資源共用會在兩小時後消失。在此之前，它仍然可以在主控台中顯示為已刪除的狀態。

AWS CLI

刪除資源共享

您可以使用delete-resource-share命令來刪除不再需要的 Resource Name。

下列範例首先使用get-resource-shares命令取得要刪除的 Resource Name (ARN)。然後它使delete-resource-share用刪除指定的資源共享。

```
$  aws ram get-resource-shares \
    --region us-east-1 \
    --resource-owner SELF
{
    "resourceShares": [
        {
            "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/2ebe77d7-4156-4a93-87a4-228568d04425",
            "name": "MySubnetShare",
            "owningAccountId": "123456789012",
            "allowExternalPrincipals": true,
            "status": "ACTIVE",
            "creationTime": "2021-09-10T15:38:54.449000-07:00",
            "lastUpdatedTime": "2021-09-10T15:38:54.449000-07:00",
            "featureSet": "STANDARD"
        }
    ]
}
$ aws ram delete-resource-share \
    --region us-east-1 \
    --resource-share-arn arn:aws:ram:us-east-1:123456789012:resource-
share/2ebe77d7-4156-4a93-87a4-228568d04425
{
    "returnValue": true
}
```

存取與您共用的 AWS 資源

使用 AWS Resource Access Manager (AWS RAM)，您可以檢視已新增至的資源共用、可存取的共用資源，以及與您共用資源的共用資源。 AWS 帳戶 當您不再需要存取其共用資源時，您也可以保留資源共用。

目錄

- 檢視與您共用的主參與者
- 離開資源共用

接受和拒絕資源共用邀請

若要存取共用資源，資源共用的擁有者必須將您新增為主參與者。擁有者可以將下列任何項目作為主參與者新增至資源共用。

- 您帳戶所屬的組織
- 包含您帳戶的組織單位 (OU)
- 您的個人帳戶
- 對於支援的資源類型，您的特定 IAM 角色或使用者

如果您透過身為中組織成員的資源共 AWS 帳戶 用新增至資源共用 AWS Organizations，且已啟用組織內的共用功能，則您無需接受邀請，就會自動取得共用資源的存取權。服務主體也可以在不接受邀請的情況下自動存取共用資源。如果您接收存取權的帳號稍後從組織中移除，則該帳號中的任何主參與者會自動失去透過該資源共用存取之資源的存取權。

如果您是由下列其中一項新增至資源共用，您會收到加入資源共用的邀請：

- 您組織以外的帳戶 AWS Organizations
- 未啟用與 AWS Organizations 共用時組織內的帳戶

如果您收到加入資源共用的邀請，您必須接受它才能存取其共用資源。如果您拒絕邀請，就無法存取共用的資源。

對於下列資源類型，您有七天的時間可以接受加入下列資源類型共用的邀請。如果您沒有在邀請到期前接受邀請，邀請就會自動拒絕。

> **Important**
>
> 對於不在下列清單中的共用資源類型，您有 12 小時的時間可以接受加入資源共用的邀請。在 12 小時後，邀請會過期，而且資源共用中的一般使用者主參與者會取消關聯。終端使用者無法再接受邀請。

- Amazon Aurora-數據庫集群

- Amazon EC2 — 容量保留和專用主機
- AWS License Manager — 授權組態
- AWS Outposts — 本地網關路由表，前哨站和站點
- Amazon 路線 53 — 轉發規則
- Amazon VPC — 客戶擁有的 IPv4 地址、首碼清單、子網路、流量鏡像目標、傳輸閘道、傳輸閘道多點傳送網域

Console

回應資源共用的邀請

1. 導覽至主控台中的 [與我共用：資源共用] 頁 AWS RAM 面。
2. 由於特定 AWS RAM 資源共用存在 AWS 區域，因此請 AWS 區域 從主控台右上角的下拉式清單中選擇適當的共用。若要查看包含全域資源的資源共用率，您必須將設定 AWS 區域 為美國東部 (維吉尼亞北部)、(us-east-1)。如需共用全域資源的詳細資訊，請參閱與全球資源相比，共享區域資源。
3. 複查已新增至的資源共用清單。

   「狀態」(Status) 欄會指出您目前資源共用的參與狀態。狀Pending態表示您已新增至資源共用，但您尚未接受或拒絕邀請。
4. 若要回應資源共用邀請，請選取資源共用 ID，然後選擇 [接受資源共用] 以接受邀請，或選擇 [拒絕資源共用] 以拒絕邀請。如果您拒絕邀請，則無法存取資源。如果您接受邀請，即可存取資源。

AWS CLI

回應資源共用的邀請

您可以使用下列命令來接受或拒絕資源共用的邀請：

- get-resource-share-invitations
- accept-resource-share-invitation
- reject-resource-share-invitation

1. 下列範例會從使用命get-resource-share-invitations令開始擷取所有可供使用者使用的邀請清單 AWS 帳戶。 AWS CLI query參數可讓您將輸出限制為只有status設定為的邀請

函PENDING。此範例顯示來自帳戶 111111111111 的一個邀請目前適用於指定中PENDING的目前帳戶。123456789012 AWS 區域

```
$ aws ram get-resource-share-invitations \
    --region us-east-1 \
    --query 'resourceShareInvitations[?status==`PENDING`]'
{
    "resourceShareInvitations": [
        {
            "resourceShareInvitationArn": "arn:aws:ram:us-
east-1:111111111111:resource-share-invitation/3b3bc051-
fbf6-4336-8377-06c559dfee49",
            "resourceShareName": "Test TrngAcct Resource Share",
            "resourceShareArn": "arn:aws:ram:us-east-1:111111111111:resource-
share/c4506c70-df75-4e6c-ac30-42ca03295a37",
            "senderAccountId": "111111111111",
            "receiverAccountId": "123456789012",
            "invitationTimestamp": "2021-09-21T08:56:24.977000-07:00",
            "status": "PENDING"
        }
    ]
}
```

2. 找到要接受的邀請之後，請記下輸出中的，以便resourceShareInvitationArn在下一個命令中使用以接受邀請。

```
$ aws ram accept-resource-share-invitation \
    --region us-east-1 \
    --resource-share-invitation-arn arn:aws:ram:us-east-1:111111111111:resource-
share-invitation/3b3bc051-fbf6-4336-8377-06c559dfee49
{
    "resourceShareInvitation": {
        "resourceShareInvitationArn": "arn:aws:ram:us-
east-1:111111111111:resource-share-invitation/3b3bc051-
fbf6-4336-8377-06c559dfee49",
        "resourceShareName": "Test TrngAcct Resource Share",
        "resourceShareArn": "arn:aws:ram:us-east-1:111111111111:resource-share/
c4506c70-df75-4e6c-ac30-42ca03295a37",
        "senderAccountId": "111111111111",
        "receiverAccountId": "123456789012",
        "invitationTimestamp": "2021-09-21T09:18:24.545000-07:00",
        "status": "ACCEPTED"
    }
```

```
}
```

如果成功，請注意，回應顯示status已從變更PENDING為ACCEPTED。

如果您想要拒絕邀請，請使用相同的參數執行reject-resource-share-invitation命令。

```
$ aws ram reject-resource-share-invitation \
    --region us-east-1 \
    --resource-share-invitation-arn arn:aws:ram:us-east-1:111111111111:resource-
share-invitation/3b3bc051-fbf6-4336-8377-06c559dfee49
{
    "resourceShareInvitation": {
        "resourceShareInvitationArn": "arn:aws:ram:us-east-1:111111111111:resource-
share-invitation/3b3bc051-fbf6-4336-8377-06c559dfee49",
        "resourceShareName": "Test TrngAcct Resource Share",
        "resourceShareArn": "arn:aws:ram:us-east-1:111111111111:resource-share/
c4506c70-df75-4e6c-ac30-42ca03295a37",
        "senderAccountId": "111111111111",
        "receiverAccountId": "123456789012",
        "invitationTimestamp": "2021-09-21T09:18:24.545000-07:00",
        "status": "REJECTED"
    }
}
```

檢視與您共用的資源共用率

您可以檢視您有權存取的資源共用。您可以查看哪些主參與者正在與您共用資源，以及他們正在共用哪些資源。

Console

若要檢視資源共用率

1. 導覽至主控台中的 [與我共用：資源共用] 頁AWS RAM面。
2. 由於AWS RAM資源共用率存在於特定AWS 區域，因此請AWS 區域從主控台的右上角的下拉式清單中選擇適當的共用。若要查看包含全域資源的資源共用，您必須將設定AWS 區域為美國東部 (維吉尼亞北部), (us-east-1)。如需分享全域資源的詳細資訊，請參閱與全球資源相比，共享區域資源。

3. (選擇性) 套用篩選器以尋找特定資源共用率。您可以套用多個篩選條件，藉此縮小搜尋範圍。您可以輸入關鍵字 (例如資源共用名稱的一部分)，以僅列出名稱中包含該文字的資源共用。選擇文字方塊以查看建議屬性欄位的下拉式清單。選擇一個之後，您可以從該字段的可用值列表中進行選擇。您可以新增其他屬性或關鍵字，直到找到所需的資源為止。
4. 主AWS RAM控台會顯示下列資訊：
   - 名稱 — 資源共用的名稱。
   - ID — 資源共用的 ID。選擇 ID，藉此檢視資源共用的詳細資訊頁面。
   - 「所有者」— 創建AWS 帳戶資源共享的 ID。
   - 狀態 - 資源共用的目前狀態。可能的值包括：
     - `Active`— 資源共用為作用中且可供使用。
     - `Deleted`-已刪除資源共用且無法再使用。
     - `Pending`-接受資源共用的邀請正在等待回應。

AWS CLI

若要檢視資源共用率

在將`--resource-owner`參數設定為的情況下使用get-resource-shares指令`OTHER-ACCOUNTS`。

下列範例顯示其他在指定AWS 區域與呼叫帳戶共用的資源共用清單AWS 帳戶。

```
$ aws ram get-resource-shares \
    --region us-east-1 \
    --resource-owner OTHER-ACCOUNTS
{
    "resourceShares": [
        {
            "resourceShareArn": "arn:aws:ram:us-east-1:111111111111:resource-
share/8b831ba0-63df-4608-be3c-19096b1ee16e",
            "name": "Prod Env Shared Licenses",
            "owningAccountId": "111111111111",
            "allowExternalPrincipals": true,
            "status": "ACTIVE",
            "creationTime": "2021-09-21T08:50:41.308000-07:00",
            "lastUpdatedTime": "2021-09-21T08:50:41.308000-07:00",
            "featureSet": "STANDARD"
        },
        {
```

```
            "resourceShareArn": "arn:aws:ram:us-east-1:222222222222:resource-share/
c4506c70-df75-4e6c-ac30-42ca03295a37",
            "name": "Prod Env Shared Subnets",
            "owningAccountId": "222222222222",
            "allowExternalPrincipals": true,
            "status": "ACTIVE",
            "creationTime": "2021-09-21T08:56:24.737000-07:00",
            "lastUpdatedTime": "2021-09-21T08:56:24.737000-07:00",
            "featureSet": "STANDARD"
        }
    ]
}
```

檢視與您共用的資源

您可以檢視您可以存取的共用資源。您可以看到哪些主參與者與您共用資源，以及哪些資源共用包括資源。

Console

若要檢視與您共用的資源

1. 導覽至主控台中的「與我共用：共用資源」頁AWS RAM面。
2. 由AWS RAM於特定的AWS 區域，請AWS 區域從右上角的下拉式清單中，選擇適當的。若要查看包含全域資源的。AWS 區域us-east-1如需共用全域資源的詳細資源，請參閱「與全球資源相比，共享區域資源」。
3. 套用篩選條件來尋找特定共用資源。您可以套用多個篩選條件，藉此縮小搜尋範圍。
4. 下列有效資訊：
   - 。選擇要在該服務主控台中檢視的資源 ID。
   - 。
   - 上次共用日期 — 與您共用資源的日期。
   - 資源共用率 — 包含資源的資源共用數。選擇要檢視資源共用率的值。
   - 擁有者 ID — 擁有資源的主參與者 ID。

AWS CLI

若要檢視與您共用的資源

您可以使用列表資源命令來查看與您共享的資源。

下列範例命令會顯示有關可透過指定AWS 區域來自另一個資源共用的資源共用存取之資源的詳細資訊AWS 帳戶。

```
$ aws ram list-resources \
    --region us-east-1 \
    --resource-owner OTHER-ACCOUNTS
{
    "resources": [
        {
            "arn": "arn:aws:license-manager:us-east-1:111111111111:license-
configuration:lic-36be0485f5ae379cc74cf8e9242ab143",
            "type": "license-manager:LicenseConfiguration",
            "resourceShareArn": "arn:aws:ram:us-east-1:111111111111:resource-
share/8b831ba0-63df-4608-be3c-19096b1ee16e",
            "status": "AVAILABLE",
            "creationTime": "2021-09-21T08:50:41.308000-07:00",
            "lastUpdatedTime": "2021-09-21T08:50:42.517000-07:00"
        }
    ]
}
```

檢視與您共用的主參與者

您可以檢視與您共享資源之所有委託人的清單。您可以查看他們正與您共享的資源和資源共享。

Console

檢視與您共享資源的委託人

1. 在 AWS RAMhttps://console.aws.amazon.com/ram 開啟 主控台。
2. 由於特定AWS RAM資源共享AWS 區域，所以請AWS 區域從主控台的右上角的下拉式清單中選擇適當的共享。若要查看包含全域資源的資源共享，您必須AWS 區域將美國東部 (維吉尼亞北部), (us-east-1)。如需分享全域資源的詳細資訊，請參閱「與全球資源相比，共享區域資源」。
3. 在導覽窗格中，選擇 Shared with me (與我共用)、Principals (委託人)。
4. (選擇性) 您可以套用篩選條件以尋找特定委託人。您可以套用多個篩選條件，藉此縮小搜尋範圍。

5. 主控台會顯示以下資訊：

   - 主參與者 ID — 與您共用的主體 ID。
   - 「資源共享」— 主參與者已將您添加到的資源共享數。選擇編號以檢視資源共享的清單。
   - 資源 — 主參與者與您共用的資源數目。選擇要檢視資源清單的值。

AWS CLI

檢視與您共享資源的委託人

您可以使用 list 主參與者指令來擷取與您共用資源的主參與者清單AWS 帳戶。

下列範例命令顯示與AWS 帳戶用於呼叫指定作業的帳號共用資源共用的詳細資訊AWS 區域。

```
$  aws ram list-principals \
    --region us-east-1 \
    --resource-owner OTHER-ACCOUNTS
{
    "principals": [
        {
            "id": "111111111111",
            "resourceShareArn": "arn:aws:ram:us-east-1:111111111111:resource-
share/8b831ba0-63df-4608-be3c-19096b1ee16e",
            "creationTime": "2021-09-21T08:50:41.308000-07:00",
            "lastUpdatedTime": "2021-09-21T09:06:25.545000-07:00",
            "external": true
        }
    ]
}
```

離開資源共用

如果您不再需要存取與您共用的資源，您可以隨時保留資源共用。當您離開資源共用時，您將無法存取共用資源。

離開資源共用的先決條件

- 只有當資源共用是以個AWS 帳戶人身分與您共用，而不是在組織的前後關聯中時，您才能保留該共用。如果您是由組織AWS 帳戶內部新增至資源共用，且已啟用共用，則無法保留資源共AWS Organizations用。存取組織內的資源共用是自動的。

- 若要保留資源共用，請確認資源共用是空的，或僅包含支援離開共用的資源類型。

  以下是唯一支援保留資源共用的資源類型。

服務	資源類型
Amazon Aurora	`rds:Cluster`
Amazon EC2	`ec2:CapacityReservation` `ec2:DedicatedHost`
AWS License Manager	`license-manager:LicenseConfiguration`

AWS Outposts	`ec2:LocalGatewayRouteTable`
	`outposts:Outpost`
	`outposts:Site`

Amazon Route 53	`route53resolver:ResolverRule`

Amazon VPC	`ec2:CoipPool`
	`ec2:PrefixList`
	`ec2:Subnet`
	`ec2:TrafficMirrorTarget`
	`ec2:TransitGateway`
	`ec2:TransitGatewayMulticastDomain`

如何留下資源共享

Console

若要離開資源共用

1. 導覽至主控台中的 [與我共用：資源共用] 頁AWS RAM面。
2. 由於特定AWS RAM資源共用存在AWS 區域，因此請AWS 區域從主控台右上角的下拉式清單中選擇適當的共用。若要查看包含全域資源的資源共用率，您必須將設定AWS 區域為美國東部 (維吉尼亞北部)、(us-east-1)。如需共用全域資源的詳細資訊，請參閱與全球資源相比，共享區域資源。
3. 選取您要離開的資源共用。
4. 選擇 [保留資源共用]，然後在確認對話方塊中選擇 [離開]。

AWS CLI

若要離開資源共用

您可以使用disassociate-resource-share指令來保留資源共用。

下列範例命令會導AWS 帳戶致呼叫命令失去對 ARN 指定之資源共用所共用之資源的存取權。您必須將要求導向至包含您要離開之資源共用的服務端點。AWS 區域

1. 首先，擷取資源共用清單，以擷取您要離開之資源共用的 ARN。

```
$ aws ram get-resource-shares \
    --region us-east-1 \
    --resource-owner OTHER-ACCOUNTS
{
    "resourceShares": [
        {
            "resourceShareArn": "arn:aws:ram:us-east-1:111111111111:resource-
share/8b831ba0-63df-4608-be3c-19096b1ee16e",
            "name": "Prod Environment Shared Licenses",
            "owningAccountId": "111111111111",
            "allowExternalPrincipals": true,
            "status": "ACTIVE",
            "creationTime": "2021-09-21T08:50:41.308000-07:00",
            "lastUpdatedTime": "2021-09-21T08:50:41.308000-07:00",
            "featureSet": "STANDARD"
```

```
        }
    ]
}
```

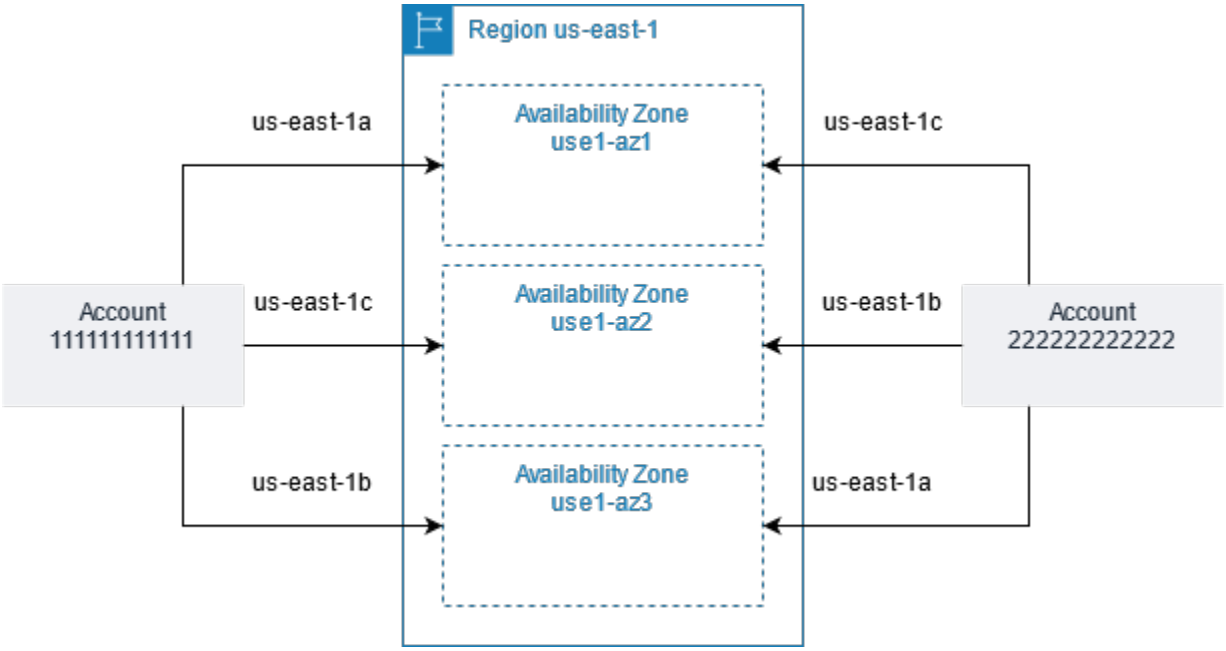
2. 然後，您可以運行命令以保留該資源共享。請注意，您還必須指定您的帳號 ID123456789012，作為要取消與指定資源共用 (由帳戶111111111111共用) 的關聯的主參與者。

```
$ aws ram disassociate-resource-share \
    --region us-east-1 \
    --resource-share-arn arn:aws:ram:us-east-1:111111111111:resource-
share/8b831ba0-63df-4608-be3c-19096b1ee16e \
    --principals 123456789012
                        {
    "resourceShareAssociations": [
        {
            "resourceShareArn": "arn:aws:ram:us-east-1:111111111111:resource-
share/8b831ba0-63df-4608-be3c-19096b1ee16e",
            "associatedEntity": "123456789012",
            "associationType": "PRINCIPAL",
            "status": "DISASSOCIATING",
            "external": false
        }
    ]
}
```

AWS資源的可用區域 ID

AWS將實體可用區域隨機對應至每個區域的可用區域名稱AWS 帳戶。這種方法有助於將資源分配到可用區域中AWS 區域，而不是可能集中在每個區域的可用區域「a」中的資源。因此，您AWS帳戶的可us-east-1a用區域可能不代表與不同帳AWS戶相同us-east-1a的實體位置。如需詳細資訊，請參閱 Amazon EC2 使用者指南中的區域和可用區域。

下圖顯示每個帳戶的 AZ ID 如何相同，即使每個帳戶的可用區域名稱對應不同。



對於某些資源，您不僅必須識別可用區域AWS 區域，還必須識別可用區域。例如，亞馬遜 VPC 子網路。在單一帳戶中，可用區域與特定名稱的對應並不重要。但是，當您使AWS RAM用與其他人共享此類資源時AWS 帳戶，映射很重要。這種隨機映射使帳號存取共用資源的能力變得更加複雜，以瞭解要參考哪個可用區域。為了協助解決此問題，此類資源還允許您使用 AZ ID 來識別與帳戶相關的資源實際位置。AZ ID 是可用區域在所有區域之間唯一且一致的識別符AWS 帳戶。例如，`use1-az1`是區域在區`us-east-1`域的 AZ ID，其在每一個AWS帳戶的位置都相同。

您可以用 AZ ID 來判斷某個帳戶資源在另一個帳戶的相對位置。例如，如果您與另一個帳戶共享 AZ ID 為 `use1-az2` 的可用區域子網，則 AZ ID 也是 `use1-az2` 之可用區域中的該帳戶就可以使用此子網。Amazon VPC 主控台會顯示各子網路的 AZ ID，其可用區域AWS CLI。

Console

檢視您帳戶中可用區域的 AZ ID

1. 導覽至主AWS RAM控台中的主AWS RAM控台頁面。
2. 您可以在您的 AZ IDAWS 區域 下檢視目前的 AZ ID。

AWS CLI

檢視您帳戶中可用區域的 AZ ID

下列範例命令顯示 us-west-2 區域中可用區域的 AZ ID，以及這些區域對應至呼叫的方式AWS 帳戶。

```
$ aws ec2 describe-availability-zones \
    --region us-west-2
{
    "AvailabilityZones": [
        {
            "State": "available",
            "OptInStatus": "opt-in-not-required",
            "Messages": [],
            "RegionName": "us-west-2",
            "ZoneName": "us-west-2a",
            "ZoneId": "usw2-az2",
            "GroupName": "us-west-2",
            "NetworkBorderGroup": "us-west-2",
            "ZoneType": "availability-zone"
        },
        {
            "State": "available",
            "OptInStatus": "opt-in-not-required",
            "Messages": [],
            "RegionName": "us-west-2",
            "ZoneName": "us-west-2b",
            "ZoneId": "usw2-az1",
            "GroupName": "us-west-2",
            "NetworkBorderGroup": "us-west-2",
            "ZoneType": "availability-zone"
        },
        {
            "State": "available",
            "OptInStatus": "opt-in-not-required",
            "Messages": [],
            "RegionName": "us-west-2",
            "ZoneName": "us-west-2c",
            "ZoneId": "usw2-az3",
            "GroupName": "us-west-2",
            "NetworkBorderGroup": "us-west-2",
            "ZoneType": "availability-zone"
        },
        {
            "State": "available",
            "OptInStatus": "opt-in-not-required",
            "Messages": [],
            "RegionName": "us-west-2",
            "ZoneName": "us-west-2d",
```

```
            "ZoneId": "usw2-az4",
            "GroupName": "us-west-2",
            "NetworkBorderGroup": "us-west-2",
            "ZoneType": "availability-zone"
        }
    ]
}
```

可共用 AWS 的資源

透過 AWS Resource Access Manager (AWS RAM)，您可以共用由其他 建立和管理的資源 AWS 服務。您可以與個人共用資源 AWS 帳戶。您也可以與 中的組織或組織單位 (OUs) 中的帳戶共用資源 AWS Organizations。某些支援的資源類型也可讓您與個別 AWS Identity and Access Management (IAM) 角色和使用者共用資源。

下列各節列出您可以使用 來共用的 資源類型 AWS 服務，分組依據為 AWS RAM。資料表中的資料欄會指定每個資源類型支援的功能：

可以與IAM使用者和角色共用	 – 除了帳戶之外，您還可以與個別 AWS Identity and Access Management (IAM) 角色和使用者共用此類型的資源。  – 您只能與 帳戶共用此類型的資源。	是 否
可以與其組織外部的帳戶共用	 – 您只能與組織內部或外部的個別帳戶共用此類型的資源。如需詳細資訊，請參閱考量事項。  – 您只能與屬於相同組織的帳戶共用此類型的資源。	是 否
可以使用客戶受管許可	AWS RAM 支援 AWS 受管許可的所有資源類型，但此欄中為是表示此資源類型也支援客戶受管許可。	

	 – 此類型的資源支援使用客戶受管許可。	是
	 – 此類型的資源不支援使用客戶受管許可。	否
可以與服務主體共用	 – 您可以與 共用此類型的資源 AWS 服務。	是
	 – 您無法與 共用此類型的資源 AWS 服務。	否

Amazon API Gateway

您可以使用 共用下列 Amazon API Gateway 資源 AWS RAM。

資源類型和程式碼	使用案例	可以與IAM使用者和角色共用	可以與其組織外部的帳戶共用	可以使用客戶受管許可	可以與服務主體共用
網域名稱 `apigateway:DomainNames`	集中建立和管理網域名稱，並與其他 AWS 帳戶 或您的組織共用。這可讓多個帳戶叫用映射到私有 的網域名稱 APIs。如需詳細資訊，請參閱《Amazon API	 否	 是 可與任何共用 AWS 帳戶。	 否	 否

資源類型和程式碼	使用案例	可以與IAM使用者和角色共用	可以與其組織外部的帳戶共用	可以使用客戶受管許可	可以與服務主體共用
	Gateway 開發人員指南》中的API閘道APIs中的私有自訂網域名稱。				

AWS App Mesh

您可以使用 共用下列 AWS App Mesh 資源 AWS RAM。

資源類型和程式碼	使用案例	可以與IAM使用者和角色共用	可以與其組織外部的帳戶共用	可以使用客戶受管許可	可以與服務主體共用
網格 `appmesh:Mesh`	集中建立和管理網格，並與其他 AWS 帳戶 或您的組織共用。共用網格可讓不同 建立的資源在同一個網格中彼此 AWS 帳戶 通訊。如需詳細資訊，請參閱AWS App Mesh 《 使用者指南》中的使用共用網格。	是	是 可與任何共用 AWS 帳戶。	否	否

AWS AppSync GraphQL API

您可以使用 共用下列 AWS AppSync GraphQL API 資源 AWS RAM。

資源類型和程式碼	使用案例	可以與IAM使用者和角色共用	可以與其組織外部的帳戶共用	可以使用客戶受管許可	可以與服務主體共用
GraphyQL API `appsync:Apis`	Manage AWS AppSync GraphQL APIs集中，並與其他 AWS 帳戶 或您的組織共用。這可讓多個帳戶共用 AWS AppSync APIs，做為建立統一 AWS AppSync 合併的一部分API，該合併可以存取相同區域中不同帳戶APIs之間來自多個子結構描述的資料。如需詳細資訊，請參閱《 AWS AppSync 開發人員指南》中的合併APIs。	是	是 可與任何共用 AWS 帳戶。	是	否

Amazon Aurora

您可以使用 共用下列 Amazon Aurora 資源 AWS RAM。

資源類型和程式碼	使用案例	可以與IAM使用者和角色共用	可以與其組織外部的帳戶共用	可以使用客戶受管許可	可以與服務主體共用
資料庫叢集 `rds:Cluster`	集中建立和管理資料庫叢集，並與其他 AWS 帳戶 或您的組織共用。這可讓多個 AWS 帳戶複製共用、集中受管的資料庫叢集。如需詳細	否	是	否	否

資源類型和程式碼	使用案例	可以與IAM使用者和角色共用	可以與其組織外部的帳戶共用	可以使用客戶受管許可	可以與服務主體共用
	資訊，請參閱《Amazon Aurora 使用者指南》中的使用 AWS RAM 和 Amazon Aurora 進行跨帳戶複製。		可與任何共用 AWS 帳戶。		

AWS Backup

您可以使用 來共用下列 AWS Backup 資源 AWS RAM。

資源類型和程式碼	使用案例	可以與IAM使用者和角色共用	可以與其組織外部的帳戶共用	可以使用客戶受管許可	可以與服務主體共用
BackupVault `backup:BackupVault`	集中建立和管理邏輯氣隙隔離保存庫，並將其與其他 AWS 帳戶 或您的組織共用。此選項可讓多個帳戶從保存庫（多個）存取和還原備份。如需詳細資訊，請參閱《 AWS Backup 開發人員指南》中的邏輯氣隙保存庫概觀。	 是	 是 可與任何共用 AWS 帳戶。	 是	 否

Amazon Bedrock

您可以使用 共用下列 Amazon Bedrock 資源 AWS RAM。

資源類型和程式碼	使用案例	可以與IAM使用者和角色共用	可以與其組織外部的帳戶共用	可以使用客戶受管許可	可以與服務主體共用
自訂模型 `bedrock:CustomModel`	集中建立和管理自訂模型，並與其他 AWS 帳戶 或您的組織共用。這可讓多個帳戶針對生成式 AI 應用程式使用相同的自訂模型。如需詳細資訊，請參閱《Amazon Bedrock 使用者指南》中的為另一個帳戶共用模型。	 是	 否 只能在自己的組織中與 AWS 帳戶 共用。	 是	 否

AWS Billing 檢視服務

您可以使用 共享下列 AWS Billing View Service 資源 AWS RAM。

資源類型和程式碼	使用案例	可以與IAM使用者和角色共用	可以與其組織外部的帳戶共用	可以使用客戶受管許可	可以與服務主體共用
帳單檢視 `billing:billingview`	集中建立和管理自訂帳單檢視，並與其他 AWS 帳戶 或您的組織共用。這可讓應用程式和業務單位擁有者從成員帳戶存取業務單位層級 AWS 的花費。如需詳細資訊，請參閱AWS Cost Management 《 使用者指南》中的使用 Billing	 否	 否 只能在自己的組織中與 AWS 帳戶 共用。	 是	 否

資源類型和程式碼	使用案例	可以與IAM使用者和角色共用	可以與其組織外部的帳戶共用	可以使用客戶受管許可	可以與服務主體共用
	View 控制成本管理資料存取。				

AWS Private Certificate Authority

您可以使用 共用下列 AWS 私有 CA 資源 AWS RAM。

資源類型和程式碼	使用案例	可以與IAM使用者和角色共用	可以與其組織外部的帳戶共用	可以使用客戶受管許可	可以與服務主體共用
私有憑證授權機構 (CA) `acm-pca:CertificateAuthority`	為您的組織的內部公有金鑰基礎設施 (CAs) 建立和管理私有憑證授權機構 (PKI)，並CAs與其他 AWS 帳戶 或您的組織共用。這可讓其他帳戶中 AWS Certificate Manager 的使用者發行由共用 CA 簽署的 X.509 憑證。如需詳細資訊，請參閱AWS Private Certificate Authority 《使用者指南》中的控制私有 CA 的存取。	是	是 可與任何共用 AWS 帳戶。	否	是

Amazon DataZone

您可以使用 共用下列 DataZone 資源 AWS RAM。

資源類型和程式碼	使用案例	可以與IAM使用者和角色共用	可以與其組織外部的帳戶共用	可以使用客戶受管許可	可以與服務主體共用
DataZone 網域 `datazone:Domain`	集中建立和管理網域，並與其他 AWS 帳戶 或您的組織共用。這可讓多個帳戶建立 Amazon DataZone 網域。如需詳細資訊，請參閱《Amazon 使用者指南》中的什麼是 DataZone Amazon DataZone 。	 否	 是 可以與任何 共用 AWS 帳戶。	 否	 否

AWS CloudHSM

您可以使用 來共用下列 AWS CloudHSM 資源 AWS RAM。

資源類型和程式碼	使用案例	可以與IAM使用者和角色共用	可以與其組織外部的帳戶共用	可以使用客戶受管許可	可以與服務主體共用
AWS CloudHSM 備份 `cloudhsm:Backup`	集中管理 AWS CloudHSM 備份，並與其他 AWS 帳戶 或您的組織共用備份。這可讓多個 AWS 帳戶 和 使用者檢視備份的相關資訊，並使用它來還	 是	 是	 是	 否

資源類型和程式碼	使用案例	可以與IAM使用者和角色共用	可以與其組織外部的帳戶共用	可以使用客戶受管許可	可以與服務主體共用
	原 AWS CloudHSM 叢集。如需詳細資訊，請參閱AWS CloudHSM《使用者指南》中的管理 AWS CloudHSM 備份。				

AWS CodeBuild

您可以使用 來共用下列 AWS CodeBuild 資源 AWS RAM。

資源類型和程式碼	使用案例	可以與IAM使用者和角色共用	可以與其組織外部的帳戶共用	可以使用客戶受管許可	可以與服務主體共用
專案 `codebuild:Project`	建立專案，並使用它來執行組建。與其他 AWS 帳戶 或您的組織共用專案。這可讓多個 AWS 帳戶 和 使用者檢視專案的相關資訊，並分析其建置。如需詳細資訊，請參閱 AWS CodeBuild《使用者指南》中的使用共用專案。	是	是 可與任何共用 AWS 帳戶。	是	否
報告群組 `codebuild:ReportGroup`	建立報告群組，並在您建置專案時使用它來建立報告。與其他 AWS 帳戶 或您的組織共用報告群組。這可讓多	是	是	是	否

資源類型和程式碼	使用案例	可以與IAM使用者和角色共用	可以與其組織外部的帳戶共用	可以使用客戶受管許可	可以與服務主體共用
	個 AWS 帳戶 和 使用者檢視報告群組及其報告，以及每個報告的測試案例結果。報告建立後 30 天內可以檢視，然後過期且不再可供檢視。如需詳細資訊，請參閱AWS CodeBuild《 使用者指南》中的使用共用專案。		可與任何共用 AWS 帳戶。		

Amazon EC2

您可以使用 共用下列 Amazon EC2 資源 AWS RAM。

資源類型和程式碼	使用案例	可以與IAM使用者和角色共用	可以與其組織外部的帳戶共用	可以使用客戶受管許可	可以與服務主體共用
容量保留 `ec2:CapacityReservation`	集中建立和管理容量保留，並與其他 AWS 帳戶 或您的組織共用保留容量。這可讓多個 Amazon EC2執行個體 AWS 帳戶 啟動到集中受管預留容量。如需詳細資訊，請參閱《Amazon EC2使用者指南》中的使用共用容量保留。	否	是 可與任何共用 AWS 帳戶。	否	否

資源類型和程式碼	使用案例	可以與IAM使用者和角色共用	可以與其組織外部的帳戶共用	可以使用客戶受管許可	可以與服務主體共用
	Important 如果您不符合共用容量保留的所有先決條件，共用操作可能會失敗。如果發生這種情況，且使用者嘗試在該容量保留中啟動Amazon EC2執行個體，則會以可產生較高成本的隨需執行個體啟動。我們建議您驗證您是否可以透過嘗試在Amazon EC2主控台中檢視共用容量保留來存取共用容量保留。您也可以監控失敗的資源共用，以便在使用者啟動執行個體之前採取更正動作，以提高成本。如需詳細資訊，請參閱範例：資源共用失敗警示。				

資源類型和程式碼	使用案例	可以與IAM使用者和角色共用	可以與其組織外部的帳戶共用	可以使用客戶受管許可	可以與服務主體共用
專用執行個體 `ec2:DedicatedHost`	集中配置和管理Amazon EC2專用主機，並與其他 AWS 帳戶 或您的組織共用主機的執行個體容量。這可讓多個 上的 Amazon EC2執行個體 AWS 帳戶 啟動到集中管理的專用主機。如需詳細資訊，請參閱《Amazon EC2使用者指南》中的使用共用專用主機。	 否	 是 可與任何共用 AWS 帳戶。	 否	 否
置放群組 `ec2:PlacementGroup`	在組織 AWS 帳戶內外共享您擁有的置放群組。您可以從與 共用的任何帳戶啟動 Amazon EC2執行個體，並加入共用置放群組。如需詳細資訊，請參閱《Amazon EC2使用者指南》中的共用置放群組。	 是	 是 可與任何共用 AWS 帳戶。	 否	 否

EC2 映像建置器

您可以使用 共用下列 EC2 Image Builder 資源 AWS RAM。

資源類型和程式碼	使用案例	可以與IAM使用者和角色共用	可以與其組織外部的帳戶共用	可以使用客戶受管許可	可以與服務主體共用
元件 `imagebuilder:Component`	集中建立和管理元件，並與其他 AWS 帳戶 或您的組織共用這些元件。管理誰可以在其映像配方中使用預先定義的建置和測試元件。如需詳細資訊，請參閱《EC2映像建置器使用者指南》中的共用映像建置器資源。 EC2	 是	 是 可與任何共用 AWS 帳戶。	 是	 否
容器配方 `imagebuilder:ContainerRecipe`	集中建立和管理容器配方，並與其他 AWS 帳戶 或您的組織共用。這可讓您管理誰可以使用預先定義的文件來複製容器映像組建。如需詳細資訊，請參閱《EC2映像建置器使用者指南》中的共用映像建置器資源。 EC2	 是	 是 可與任何共用 AWS 帳戶。	 是	 否
映像 `imagebuilder:Image`	集中建立和管理黃金映像，並與其他 AWS 帳戶 或您的組織共用。管理誰可以使用整個組織中使用 Image Builder 建立EC2的映像。如需詳細資訊，請參閱《EC2映像建置器使用	 是	 是 可與任何共用 AWS 帳戶。	 是	 否

資源類型和程式碼	使用案例	可以與IAM使用者和角色共用	可以與其組織外部的帳戶共用	可以使用客戶受管許可	可以與服務主體共用
	者指南》中的共用映像建置器資源。 EC2				
影像配方 `imagebuilder:ImageRecipe`	集中建立和管理映像配方，並與其他 AWS 帳戶 或您的組織共用。這可讓您管理誰可以使用預先定義的文件來複製AMI組建。如需詳細資訊，請參閱《EC2映像建置器使用者指南》中的共用映像建置器資源。 EC2	 是	 是 可與任何共用 AWS 帳戶。	 是	 否

AWS End User Messaging SMS

您可以使用 共用下列 AWS End User Messaging SMS 資源 AWS RAM。

資源類型和程式碼	使用案例	可以與IAM使用者和角色共用	可以與其組織外部的帳戶共用	可以使用客戶受管許可	可以與服務主體共用
OptOutList `sms-voice:opt-out-list`	建立 OptOutList 並與 AWS 帳戶 組織中的其他 共用。您可以共用 ，OptOutList 以便其他應用程式可以從不同的 選擇退出使用者的電話號碼 AWS 帳戶 ，或者他們可以檢查使用者電話號碼的狀態。如需詳細	 否	 是 可與任何共用 AWS 帳戶。	 是	 否

資源類型和程式碼	使用案例	可以與IAM使用者和角色共用	可以與其組織外部的帳戶共用	可以使用客戶受管許可	可以與服務主體共用
	資訊，請參閱 AWS End User Messaging SMS 《使用者指南》中的使用共用資源。				
PhoneNumber `sms-voice:phone-number`	建立和管理電話號碼，以與其他 AWS 帳戶 或您的組織共用。這可讓多個使用共用電話號碼 AWS 帳戶 傳送訊息。如需詳細資訊，請參閱 AWS End User Messaging SMS 《使用者指南》中的使用共用資源。	 否	 是 可與任何共用 AWS 帳戶。	 是	 是
集區 `sms-voice:pool`	建立和管理集區，以與其他 AWS 帳戶 或您的組織共用集區。這可讓多個使用共用集區 AWS 帳戶 傳送訊息。如需詳細資訊，請參閱 AWS End User Messaging SMS 《使用者指南》中的使用共用資源。	 否	 是 可與任何共用 AWS 帳戶。	 是	 是

資源類型和程式碼	使用案例	可以與IAM使用者和角色共用	可以與其組織外部的帳戶共用	可以使用客戶受管許可	可以與服務主體共用
SenderId `sms-voice:sender-id`	建立和管理 SenderId，並與其他 AWS 帳戶 或您的組織共用。這可讓多個使用共用 AWS 帳戶 傳送訊息 SenderId。如需詳細資訊，請參閱 AWS End User Messaging SMS 《使用者指南》中的使用共用資源。	 否	 是 可與任何共用 AWS 帳戶。	 是	 是

Amazon FSx for OpenZFS

您可以使用 共用下列 Amazon FSx for OpenZFS 資源 AWS RAM。

資源類型和程式碼	使用案例	可以與IAM使用者和角色共用	可以與其組織外部的帳戶共用	可以使用客戶受管許可	可以與服務主體共用
FSx 磁碟區 `fsx:Volume`	集中建立和管理 FSx OpenZFS 磁碟區，並與其他 AWS 帳戶 或您的組織共用。這可讓多個帳戶透過 FSxAPIsCreateVolume 或 使用共用磁碟區下的 OpenZfs 快照來執行資料複寫CopySnapshotAndUpdateVolume 。如	 是	 是 可以與任何 共用 AWS 帳戶。	 是	 否

資源類型和程式碼	使用案例	可以與IAM使用者和角色共用	可以與其組織外部的帳戶共用	可以使用客戶受管許可	可以與服務主體共用
	需詳細資訊，請參閱《Amazon FSx for OpenZFS 使用者指南》中的隨需資料複寫。				

AWS Glue

您可以使用 共用下列 AWS Glue 資源 AWS RAM。

資源類型和程式碼	使用案例	可以與IAM使用者和角色共用	可以與其組織外部的帳戶共用	可以使用客戶受管許可	可以與服務主體共用
資料目錄 `glue:Catalog`	管理中央資料目錄，並與 AWS 帳戶 或您的組織共用資料庫和資料表的中繼資料。這可讓使用者跨多個帳戶對資料執行查詢。如需詳細資訊，請參閱《 AWS Lake Formation 開發人員指南》中的跨 AWS 帳戶共用資料目錄資料表和資料庫。	否	是 可與任何共用 AWS 帳戶。	否	否
資料庫 `glue:Database`	集中建立和管理資料目錄資料庫，並與 AWS 帳戶 或您的組織共用。資料庫是資料目錄資料表的集合。這可讓使用者執行查詢，以及擷	否	是	否	否

資源類型和程式碼	使用案例	可以與IAM使用者和角色共用	可以與其組織外部的帳戶共用	可以使用客戶受管許可	可以與服務主體共用
	取、轉換和載入 (ETL) 任務，以跨多個帳戶聯結和查詢資料。如需詳細資訊，請參閱《 AWS Lake Formation 開發人員指南》中的跨 AWS 帳戶共用資料目錄資料表和資料庫。		可與任何共用 AWS 帳戶。		
資料表 `glue:Table`	集中建立和管理資料目錄資料表，並與 AWS 帳戶 或您的組織共用。資料目錄資料表包含 Amazon S3、JDBC 資料來源、Amazon Redshift、串流來源和其他資料存放區中資料表的中繼資料。這可讓使用者執行可跨多個帳戶聯結和查詢資料的查詢和ETL任務。如需詳細資訊，請參閱《 AWS Lake Formation 開發人員指南》中的跨 AWS 帳戶共用資料目錄資料表和資料庫。	否	是 可與任何共用 AWS 帳戶。	否	否

AWS License Manager

您可以使用 共用下列 AWS License Manager 資源 AWS RAM。

資源類型和程式碼	使用案例	可以與IAM使用者和角色共用	可以與其組織外部的帳戶共用	可以使用客戶受管許可	可以與服務主體共用
授權組態 `license-manager:LicenseConfiguration`	集中建立和管理授權組態，並與其他 AWS 帳戶 或您的組織共用。這可讓您強制執行以跨多個企業協議條款為基礎的集中受管授權規則 AWS 帳戶。如需詳細資訊，請參閱《License Manager 使用者指南》中的 License Manager 中的授權組態。	否	是 可與任何共用 AWS 帳戶。	否	否

AWS Marketplace

您可以使用 共用下列 AWS Marketplace 資源 AWS RAM。

資源類型和程式碼	使用案例	可以與IAM使用者和角色共用	可以與其組織外部的帳戶共用	可以使用客戶受管許可	可以與服務主體共用
Marketplace Catalog 實體 `aws-marketplace:Entity`	建立、管理和共用組織中 AWS 帳戶 的實體 AWS Marketplace。如需詳細資訊，請參閱 AWS Marketplace Catalog API 參考中的資源共用 AWS RAM。	是	是 可與任何共用 AWS 帳戶。	否	否

AWS Migration Hub Refactor Spaces

您可以使用 共用下列 AWS Migration Hub Refactor Spaces 資源 AWS RAM。

資源類型和程式碼	使用案例	可以與IAM使用者和角色共用	可以與其組織外部的帳戶共用	可以使用客戶受管許可	可以與服務主體共用
重構空間環境 `refactor-spaces:Environment`	建立 Refactor Spaces 環境，並使用它來包含您的 Refactor Spaces 應用程式。與組織中的其他 AWS 帳戶 或所有帳戶共用環境。這可讓多個 AWS 帳戶 和 使用者檢視環境及其應用程式的相關資訊。如需詳細資訊，請參閱AWS Migration Hub Refactor Spaces 《使用者指南》中的使用 共用 Refactor Spaces 環境 AWS RAM。	 是	 是 可以與任何 共用 AWS 帳戶。	 是	 否

AWS Network Firewall

您可以使用 來共用下列 AWS Network Firewall 資源 AWS RAM。

資源類型和程式碼	使用案例	可以與IAM使用者和角色共用	可以與其組織外部的帳戶共用	可以使用客戶受管許可	可以與服務主體共用
防火牆政策 `network-firewall:FirewallPolicy`	集中建立和管理防火牆政策，並與其他 AWS 帳戶 或您的組織共用。這可讓組織中的多個帳戶共用一組常見的網路監控、保護和篩選行為。如需詳細資訊，請參閱《 AWS Network Firewall 開發人員指南》中的共用防火牆政策和規則群組。	 是	 是 可與任何共用 AWS 帳戶。	 否	 否

規則群組
 	
`network-firewall:StatefulRuleGroup`
 	
`network-firewall:StatelessRuleGroup`
	集中建立和管理無狀態和有狀態規則群組，並與其他 AWS 帳戶 或您的組織共用。這可讓中的組織中的多個帳戶 AWS Organizations 共用一組檢查和處理網路流量的條件。如需詳細資訊，請參閱《 AWS Network Firewall 開發人員指南》中的共用防火牆政策和規則群組。	 是	 是
			
			可與任何共用 AWS 帳戶。
				 否	 否

AWS Outposts

您可以使用 來共用下列 AWS Outposts 資源 AWS RAM。

資源類型和程式碼	使用案例	可以與IAM使用者和角色共用	可以與其組織外部的帳戶共用	可以使用客戶受管許可	可以與服務主體共用
Outpost `outposts:Outpost`	集中建立和管理Outpost，並與 AWS 帳戶 組織中的其他 共用。這可讓多個帳戶在您的共用、集中管理的Outpost 上建立子網路和EBS磁碟區。如需詳細資訊，請參閱AWS Outposts 《 使用者指南》中的使用共用 AWS Outposts 資源。	否	否 只能在自己的組織中與 AWS 帳戶 共用。	是	否
本機閘道路由表 `ec2:LocalGatewayRouteTable`	集中建立和管理與本機閘道的VPC關聯，並與 AWS 帳戶 組織中的其他閘道共用。這可讓多個帳戶建立與本機閘道的VPC關聯，並檢視路由表和虛擬介面組態。如需詳細資訊，請參閱AWS Outposts 《 使用者指南》中的可共用 Outpost 資源。	否	否 只能在自己的組織中與 AWS 帳戶 共用。	否	否
網站 `outposts:Site`	建立和管理 Outpost 網站，並與 AWS 帳戶 組織中的其他網站共用。這可讓多個帳戶在共用網站建立和管理 Outpost，並支援 Outpost 資源和網站之間的分割控制。如需詳	否	是 可以與任何 共用 AWS 帳戶。	否	否

資源類型和程式碼	使用案例	可以與IAM使用者和角色共用	可以與其組織外部的帳戶共用	可以使用客戶受管許可	可以與服務主體共用
	細資訊，請參閱AWS Outposts 《使用者指南》中的使用共用 AWS Outposts 資源。				

Amazon S3 on Outposts

您可以使用 共用下列 Amazon S3 on Outposts 資源 AWS RAM。

資源類型和程式碼	使用案例	可以與IAM使用者和角色共用	可以與其組織外部的帳戶共用	可以使用客戶受管許可	可以與服務主體共用
S3 on Outpost `s3-outposts:Outpost`	在 Outpost 上建立和管理 Amazon S3 儲存貯體、存取點和端點。這可讓多個帳戶在共用網站建立和管理 Outpost，並支援 Outpost 資源和網站之間的分割控制。如需詳細資訊，請參閱AWS Outposts 《使用者指南》中的使用共用 AWS Outposts 資源。	否	否 只能在自己的組織中與 AWS 帳戶 共用。	是	否

AWS 資源總管

您可以使用 共用下列 AWS 資源總管 資源 AWS RAM。

資源類型和程式碼	使用案例	可以與IAM使用者和角色共用	可以與其組織外部的帳戶共用	可以使用客戶受管許可	可以與服務主體共用
檢視 `resource-explorer-2:View`	集中建立和設定 Resource Explorer 檢視，並與 AWS 帳戶 組織中的其他 共用。這可讓多個角色和使用者 AWS 帳戶 搜尋並探索可透過 檢視存取的資源。如需詳細資訊，請參閱AWS 資源總管《使用者指南》中的共用 Resource Explorer 檢視。	 否	 否 只能在自己的組織中與 AWS 帳戶 共用。	 否	 否

AWS Resource Groups

您可以使用 共用下列 AWS Resource Groups 資源 AWS RAM。

資源類型和程式碼	使用案例	可以與IAM使用者和角色共用	可以與其組織外部的帳戶共用	可以使用客戶受管許可	可以與服務主體共用
資源群組 `resource-groups:Group`	集中建立和管理主機資源群組，並與 AWS 帳戶 組織中的其他 共用。這可讓多個 AWS 帳戶 共用使用 建立的 Amazon EC2 專用主機群組 AWS License Manager。如需詳細資訊，請參閱AWS	 否	 是 可與任何共用 AWS 帳戶。	 否	 否

資源類型和程式碼	使用案例	可以與IAM使用者和角色共用	可以與其組織外部的帳戶共用	可以使用客戶受管許可	可以與服務主體共用
	License Manager 《使用者指南》中的託管資源群組 AWS License Manager。				

Amazon Route 53

您可以使用 共用下列 Amazon Route 53 資源 AWS RAM。

資源類型和程式碼	使用案例	可以與IAM使用者和角色共用	可以與其組織外部的帳戶共用	可以使用客戶受管許可	可以與服務主體共用
Route 53 解析程式DNS防火牆規則群組 `route53resolver:FirewallRuleGroup`	集中建立和管理 Route 53 Resolver DNS Firewall 規則群組，並與其他 AWS 帳戶 或您的組織共用。這可讓多個帳戶共用一組條件，以檢查和處理經過 Route 53 Resolver 的傳出DNS查詢。如需詳細資訊，請參閱《Amazon Route 53 開發人員指南》中的在 之間共用 Route 53 解析程式DNS防火牆規則群組 AWS 帳戶。	 是	 是 可以與任何 共用 AWS 帳戶。	 否	 否

資源類型和程式碼	使用案例	可以與IAM使用者和角色共用	可以與其組織外部的帳戶共用	可以使用客戶受管許可	可以與服務主體共用
Route 53 Profiles `route53profiles:Profile`	建立和管理 Route 53 Profiles 集中，並與其他 AWS 帳戶 或您的組織共用。這可讓多個帳戶套用 Route 53 中指定的DNS組態 Profiles 到多個 VPCs。如需詳細資訊，請參閱 Amazon Route 53 Profiles Amazon Route 53 開發人員指南。	 是	 是 可與任何共用 AWS 帳戶。	 是	 否
解析程式規則 `route53resolver:ResolverRule`	集中建立和管理解析程式規則，並與其他 AWS 帳戶 或您的組織共用。這可讓多個帳戶將DNS查詢從虛擬私有雲端 (VPCs) 轉送到共用、集中管理解析程式規則中定義的目標 IP 地址。如需詳細資訊，請參閱《Amazon Route 53 開發人員指南》中的與其他 共用解析程式規則 AWS 帳戶 和使用共用規則。	 否	 是 可以與任何 共用 AWS 帳戶。	 否	 否

資源類型和程式碼	使用案例	可以與IAM使用者和角色共用	可以與其組織外部的帳戶共用	可以使用客戶受管許可	可以與服務主體共用
查詢日誌 `route53resolver:ResolverQueryLogConfig`	集中建立和管理查詢日誌，並與其他 AWS 帳戶 或您的組織共用。這可讓多個 AWS 帳戶 將源自其 的DNS查詢記錄VPCs到集中受管查詢日誌。如需詳細資訊，請參閱《Amazon Route 53 開發人員指南》中的與其他 共用解析程式查詢記錄組態 AWS 帳戶。	是	是 可與任何共用 AWS 帳戶。	是	否

Amazon Application Recovery Controller (ARC)

您可以使用 共用下列 Amazon Application Recovery Controller (ARC) 資源 AWS RAM。

資源類型和程式碼	使用案例	可以與IAM使用者和角色共用	可以與其組織外部的帳戶共用	可以使用客戶受管許可	可以與服務主體共用
ARC 叢集 `route53-recovery-control:Cluster`	集中建立和管理ARC叢集，並與其他 AWS 帳戶 或您的組織共用叢集。這可讓多個帳戶在單一共用叢集中建立控制面板和路由控制，從而降低複雜性和組織所需的叢集總數。如需詳細資訊，請參閱《Amazon	是	是 可與任何共用 AWS 帳戶。	是	否

資源類型和程式碼	使用案例	可以與IAM使用者和角色共用	可以與其組織外部的帳戶共用	可以使用客戶受管許可	可以與服務主體共用
	Application Recovery Controller (ARC) 開發人員指南》中的跨帳戶共用叢集。				

Amazon Simple Storage Service

您可以使用 共用下列 Amazon Simple Storage Service 資源 AWS RAM。

資源類型和程式碼	使用案例	可以與IAM使用者和角色共用	可以與其組織外部的帳戶共用	可以使用客戶受管許可	可以與服務主體共用
存取授與 `s3:AccessGrants`	集中建立和管理 S3 Access Grants 執行個體，並與其他 AWS 帳戶 或您的組織共用。這可讓多個帳戶檢視和刪除共用資源。如需詳細資訊，請參閱 Amazon Simple Storage Service 使用者指南中的 S3 Access Grants 跨帳戶存取。	是	是 可與任何共用 AWS 帳戶。	是	是

Amazon SageMaker AI

您可以使用 共用下列 Amazon SageMaker AI 資源 AWS RAM。

資源類型和程式碼	使用案例	可以與IAM使用者和角色共用	可以與其組織外部的帳戶共用	可以使用客戶受管許可	可以與服務主體共用
SageMaker AI 目錄 `sagemaker:SagemakerCatalog`	為方便探索 – 允許帳戶擁有者將 SageMaker AI 目錄中所有特徵群組資源的可探索性許可授予其他帳戶。授予存取權後，這些帳戶的使用者可以檢視從目錄中與其共用的功能群組。如需詳細資訊，請參閱《Amazon SageMaker AI 開發人員指南》中的跨帳戶功能群組可探索性和存取。 **Note** 可探索性和存取是 SageMaker AI 中的個別許可。	否	是 可與任何共用 AWS 帳戶。	是	否
SageMaker AI 功能群組 `sagemaker:FeatureGroup`	對於存取 – 允許帳戶擁有者將存取許可授予其他帳戶，以選取功能群組資源。一旦授予存取權，這些帳戶的使用者可以使用已與其共用的功能群組。如需詳細資訊，請參閱《Amazon SageMaker AI 開發人員	是	是 可與任何共用 AWS 帳戶。	是	否

資源類型和程式碼	使用案例	可以與IAM使用者和角色共用	可以與其組織外部的帳戶共用	可以使用客戶受管許可	可以與服務主體共用
	指南》中的跨帳戶功能群組可探索性和存取。 **Note** 可探索性和存取是 SageMaker AI 中的個別許可。				
SageMaker AI JumpStart `sagemaker:Hub`	使用 Amazon SageMaker AI JumpStart，您可以`sagemaker:Hub` 集中建立和管理，並與同一組織中 AWS 帳戶 的其他人共用。如需詳細資訊，請參閱《Amazon SageMaker AI 開發人員指南》中的使用私有策畫中樞控制基礎模型存取 JumpStart。SageMaker	 是	 是 可與任何共用 AWS 帳戶。	 是	 否

資源類型和程式碼	使用案例	可以與IAM使用者和角色共用	可以與其組織外部的帳戶共用	可以使用客戶受管許可	可以與服務主體共用
譜系群組 `sagemaker:LineageGroup`	Amazon SageMaker AI 可讓您建立管道中繼資料的譜系群組，以更深入了解其歷史記錄和關係。與組織中的其他 AWS 帳戶 或 帳戶共用譜系群組。這可讓多個 AWS 帳戶 和 使用者檢視有關譜系群組的資訊，並查詢其中的追蹤實體。如需詳細資訊，請參閱《Amazon SageMaker AI 開發人員指南》中的跨帳戶譜系追蹤。	 是	 是 可與任何共用 AWS 帳戶。	 否	 否

資源類型和程式碼	使用案例	可以與IAM使用者和角色共用	可以與其組織外部的帳戶共用	可以使用客戶受管許可	可以與服務主體共用
SageMaker AI 模型卡 `sagemaker:ModelCard`	Amazon SageMaker AI 會建立模型卡，在單一位置記錄機器學習 (ML) 模型的關鍵詳細資訊，以簡化管理和報告。與組織中的其他 AWS 帳戶 或 帳戶共用您的模型卡，以實現機器學習操作的多帳戶策略。這可讓 AWS 帳戶 將模型卡的 ML 活動存取權分享給其他 帳戶。如需詳細資訊，請參閱《Amazon SageMaker AI 開發人員指南》中的 Amazon AI 模型卡。 SageMaker	 是	 是 可與任何共用 AWS 帳戶。	 否	 否
SageMaker AI 模型登錄模型套件群組 `sagemaker:model-package-group`	透過 Amazon SageMaker AI Model Registry，您可以`sagemaker:model-package-group` 集中建立和管理，並與其他 共用 AWS 帳戶 以註冊模型版本。如需詳細資訊，請參閱《Amazon SageMaker AI 開發人員指南》中的 Amazon AI Model Registry。 SageMaker	 是	 是	 是	 否

資源類型和程式碼	使用案例	可以與IAM使用者和角色共用	可以與其組織外部的帳戶共用	可以使用客戶受管許可	可以與服務主體共用
SageMaker AI 管道 `sagemaker:Pipeline`	透過 Amazon SageMaker AI Model Building Pipelines，您可以大規模建立、自動化和管理 end-to-end 機器學習工作流程。與組織中的其他 AWS 帳戶 或 帳戶共用管道，以實現機器學習操作的多帳戶策略。這可讓多個 AWS 帳戶 和 使用者檢視管道及其執行的相關資訊，並可選擇從其他帳戶啟動、停止和重試管道。如需詳細資訊，請參閱《Amazon SageMaker AI 開發人員指南》中的 AI 管道跨帳戶支援。 SageMaker	是	是 可與任何共用 AWS 帳戶。	是	否

AWS Service Catalog AppRegistry

您可以使用 共用下列 AWS Service Catalog AppRegistry 資源 AWS RAM。

資源類型和程式碼	使用案例	可以與IAM使用者和角色共用	可以與其組織外部的帳戶共用	可以使用客戶受管許可	可以與服務主體共用
應用程式 `servicecatalog:Application`	建立應用程式，並使用它來追蹤整個 AWS 環境中屬於該應用程式的資源。與其他 AWS 帳戶 或您的組織共用應用程式。這可讓多個 AWS 帳戶 和 使用者在本機檢視應用程式及其相關資源的相關資訊。如需詳細資訊，請參閱 Service Catalog 使用者指南中的建立應用程式。	 否	 否 只能在自己的組織中與 AWS 帳戶 共用。	 是	 否
屬性群組 `servicecatalog:AttributeGroup`	建立屬性群組，並使用它來存放與您應用程式相關的中繼資料。與其他 AWS 帳戶 或您的組織共用屬性群組。這可讓多個 AWS 帳戶 和使用者檢視屬性群組的相關資訊。如需詳細資訊，請參閱 Service Catalog 使用者指南中的建立屬性群組。	 否	 否 只能在自己的組織中與 AWS 帳戶 共用。	 是	 否

AWS Systems Manager Incident Manager

您可以使用 來共用下列 AWS Systems Manager Incident Manager 資源 AWS RAM。

資源類型和程式碼	使用案例	可以與IAM使用者和角色共用	可以與其組織外部的帳戶共用	可以使用客戶受管許可	可以與服務主體共用
聯絡人 `ssm-contacts:Contact`	集中建立和管理聯絡人和呈報計劃，並與其他 AWS 帳戶 或您的組織共用聯絡人詳細資訊。這可讓許多 AWS 帳戶 檢視在事件期間發生的參與。如需詳細資訊，請參閱 AWS Systems Manager Incident Manager 使用者指南中的使用共用聯絡人和回應計劃。	 是	 是 可與任何共用 AWS 帳戶。	 是	 否
回應計劃 `ssm-incidents:ResponsePlan`	集中建立和管理回應計劃，並與其他 AWS 帳戶 或您的組織共用。這可讓這些 將 Amazon CloudWatch 警示和 Amazon EventBridge 事件規則 AWS 帳戶 連接到回應計劃，並在偵測到事件時自動建立事件。事件也可以存取這些其他 的指標 AWS 帳戶。如需詳細資訊，請參閱 AWS Systems Manager Incident Manager 使用者指南中的使用共用聯絡人和回應計劃。	 是	 是 可與任何共用 AWS 帳戶。	 是	 否

AWS Systems Manager 參數存放區

您可以使用 共用下列 AWS Systems Manager 參數存放區資源 AWS RAM。

資源類型和程式碼	使用案例	可以與IAM使用者和角色共用	可以與其組織外部的帳戶共用	可以使用客戶受管許可	可以與服務主體共用
參數 `ssm:Parameter`	建立 參數，並使用它來存放組態資料，您可以在指令碼、命令、SSM文件以及組態和自動化工作流程中參考。與其他 AWS 帳戶 或您的組織共用 參數。這可讓多個 AWS 帳戶 和 使用者檢視有關字串的資訊，並透過將資料與程式碼分開來提高安全性。如需詳細資訊，請參閱AWS Systems Manager 《使用者指南》中的使用共用參數。	 是	 是 可與任何共用 AWS 帳戶。	 是	 否

Amazon VPC

您可以使用 共用下列 Amazon Virtual Private Cloud (Amazon VPC) 資源 AWS RAM。

資源類型和程式碼	使用案例	可以與IAM使用者和角色共用	可以與其組織外部的帳戶共用	可以使用客戶受管許可	可以與服務主體共用
客戶擁有IPv4的地址 `ec2:CoipPool`	在 AWS Outposts 安裝過程中，會根據您提供的內部部署網路相關資訊，AWS 建立稱為客戶擁有 IP 地址集區的地址集區。 客戶擁有的 IP 地址透過內部部署網路，提供本機或外部連線至 Outposts 子網路中的資源。您可以將這些地址指派給 Outpost 上的資源，例如EC2執行個體、使用彈性 IP 地址或使用會自動指派客戶擁有 IP 地址的子網路設定。如需詳細資訊，請參閱AWS Outposts 使用者指南中的客戶擁有的 IP 位址。	✗ 否	✗ 否 只能在自己的組織中與 AWS 帳戶 共用。	✗ 否	✗ 否
IP Address Manager (IPAM) 集區 `ec2:IpamPool`	集中與其他 AWS 帳戶、IAM角色或使用者，或整個組織或組織單位 (OU) 共用 Amazon VPCIPAM集區 AWS Organizations。這可讓這些委託人CIDRs從集區配置到各自帳戶中 AWS 的資源VPCs，例如 。如需詳細資訊，請	✓ 是	✓ 是 可與任何共用 AWS 帳戶。	✓ 是	✗ 否

資源類型和程式碼	使用案例	可以與IAM使用者和角色共用	可以與其組織外部的帳戶共用	可以使用客戶受管許可	可以與服務主體共用
	參閱《Amazon VPC IP Address Manager 使用者指南》中的使用 共用IPAM集 AWS RAM區。				
IP Address Manager (IPAM) 資源探索 `ec2:IpamResourceDiscovery`	與其他 共用資源探索 AWS 帳戶。資源探索是一種 Amazon VPCIPAM元件，IPAM可讓 管理和監控屬於擁有帳戶的資源。如需詳細資訊，請參閱《Amazon VPCIPAM使用者指南》中的使用資源探索。	否	是 可以與任何 共用 AWS 帳戶。	否	否
字首清單 `ec2:PrefixList`	集中建立和管理字首清單，並與其他 AWS 帳戶 或您的組織共用。這可讓多個 AWS 帳戶參考字首清單在其資源中，例如VPC安全群組和子網路路由表。如需詳細資訊，請參閱《Amazon VPC使用者指南》中的使用共用字首清單。	否	是 可與任何共用 AWS 帳戶。	否	否

資源類型和程式碼	使用案例	可以與IAM使用者和角色共用	可以與其組織外部的帳戶共用	可以使用客戶受管許可	可以與服務主體共用
子網路 `ec2:Subnet`	集中建立和管理子網路，並在 AWS 帳戶 組織內與子網路共用。這可讓多個 將其應用程式資源 AWS 帳戶 啟動到集中管理的 VPCs。這些資源包括 Amazon EC2執行個體、Amazon Relational Database Service (RDS) 資料庫、Amazon Redshift 叢集和 AWS Lambda 函數。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的使用VPC共用。 **Note** 若要在建立資源共享時包含子網路，除了 之外，您還必須擁有 `ec2:DescribeSubnets` 和 `ec2:DescribeVpcs` 許可`ram:CreateResourceShare` 。	否	只能在自己的組織中與 AWS 帳戶 共用。	否	否

資源類型和程式碼	使用案例	可以與IAM使用者和角色共用	可以與其組織外部的帳戶共用	可以使用客戶受管許可	可以與服務主體共用
	預設子網路不可共用。您只能共用自己建立的子網路。				
安全群組 `ec2:SecurityGroup`	集中建立和管理安全群組，並與其他 AWS 帳戶 或您的組織共用。這可讓多個 將安全群組與其彈性網路介面建立 AWS 帳戶 關聯。如需詳細資訊，請參閱《Amazon VPC使用者指南》中的共用安全群組。	 是	 否 只能在自己的組織中與 AWS 帳戶 共用。	 是	 否
流量鏡射目標 `ec2:TrafficMirrorTarget`	集中建立和管理流量鏡射目標，並與其他 AWS 帳戶 或您的組織共用。這可讓多個 AWS 帳戶 將鏡像網路流量從其帳戶中的流量鏡像來源傳送至共用、集中受管的流量鏡像目標。如需詳細資訊，請參閱《流量鏡像指南》中的跨帳戶流量鏡像目標。	 否	 是 可與任何共用 AWS 帳戶。	 否	 否

資源類型和程式碼	使用案例	可以與IAM使用者和角色共用	可以與其組織外部的帳戶共用	可以使用客戶受管許可	可以與服務主體共用
傳輸閘道 `ec2:TransitGateway`	集中建立和管理傳輸閘道，並與其他 AWS 帳戶 或您的組織共用。這可讓多個 AWS 帳戶路由流量透過共用、集中管理的傳輸閘道，在其 VPCs和內部部署網路之間進行。如需詳細資訊，請參閱 Amazon Transit Gateways 中的共用傳輸閘道。 VPC **Note** 若要在建立資源共享時包含傳輸閘道，除了 之外，您還必須擁有 `ec2:DescribeTransitGateway` 許可`ram:CreateResourceShare` 。	否	是 可與任何共用 AWS 帳戶。	否	否

資源類型和程式碼	使用案例	可以與IAM使用者和角色共用	可以與其組織外部的帳戶共用	可以使用客戶受管許可	可以與服務主體共用
傳輸閘道多點傳送網域 `ec2:TransitGatewayMulticastDomain`	集中建立和管理傳輸閘道多點傳送網域，並將其與其他 AWS 帳戶 或您的組織共用。這可讓多點傳送網域中的多個 AWS 帳戶 註冊和取消註冊群組成員或群組來源。如需詳細資訊，請參閱 Transit Gateways 指南中的使用共用多點傳送網域。	 否	 是 可與任何共用 AWS 帳戶。	 否	 否
AWS Verified Access 群組 `ec2:VerifiedAccessGroup`	集中建立和管理 AWS Verified Access 群組，然後與其他 AWS 帳戶或您的組織共用。這可讓多個帳戶中的應用程式使用一組單一的共用 AWS Verified Access 端點。如需詳細資訊，請參閱AWS Verified Access 《使用者指南》中的透過 共用您的 AWS Verified Access 群組 AWS Resource Access Manager。	 是	 是 可與任何共用 AWS 帳戶。	 否	 否

Amazon VPC Lattice

您可以使用 共用下列 Amazon VPC Lattice 資源 AWS RAM。

資源類型和程式碼	使用案例	可以與IAM使用者和角色共用	可以與其組織外部的帳戶共用	可以使用客戶受管許可	可以與服務主體共用
Amazon VPC Lattice 服務 `vpc-lattice:Service`	集中建立和管理 Amazon VPC Lattice 服務，並與個人或 AWS 帳戶 組織共用。這可讓服務擁有者在多帳戶環境中連線、保護和觀察 service-to-service通訊。如需詳細資訊，請參閱 VPC Lattice 使用者指南中的使用共用資源。	否	是 可與任何共用 AWS 帳戶。	是	否
Amazon VPC Lattice 服務網路 `vpc-lattice:ServiceNetwork`	集中建立和管理 Amazon VPC Lattice 服務網路，並與個人或 AWS 帳戶 組織共用。這可讓服務網路擁有者在多帳戶環境中連線、保護和觀察 service-to-service通訊。如需詳細資訊，請參閱《Amazon VPC Lattice 使用者指南》中的使用共用資源。	否	是 可與任何共用 AWS 帳戶。	是	否

AWS 雲端 WAN

您可以使用 共用下列 AWS 雲端WAN資源 AWS RAM。

資源類型和程式碼	使用案例	可以與IAM使用者和角色共用	可以與其組織外部的帳戶共用	可以使用客戶受管許可	可以與服務主體共用
雲端WAN核心網路 `networkmanager:CoreNetwork`	集中建立和管理雲端WAN核心網路，並與其他網路共用 AWS 帳戶。這可讓單一雲端WAN核心網路上的多個 AWS 帳戶 存取和佈建主機。如需詳細資訊，請參閱 AWS 雲端WAN使用者指南中的共用核心網路。	 是	 是 可以與任何 共用 AWS 帳戶。	 否	 否

管理權限AWS RAM

在中AWS RAM，受管理的權限有兩種類型：受AWS管理的權限和客戶管理的權限。

受管理的權限定義取用者如何對資源共用中的資源採取行動。建立資源共用時，必須針對資源共用中包含的每個資源類型指定要使用哪個 Managed 權限。受管理權限中的原則範本包含以資源為基礎的策略所需的一切 (主參與者和資源除外)。資源共享 (ARN) 和與資源共享相關聯的 Pource Name (ARN) 和與資源共享的 ARN 完成以資源共享為基礎的政策共享。 AWS RAM然後編寫以資源為基礎的策略，它附加到該資源共用中的所有資源。

每個受管理的許可可可可以有或多一或多一或多 系統會將一個版本指定為該受管理權限的預設版本。有時，建立新版本並將該新版本指定為預設版本，以AWS更新資源類型的AWS受管理權限。您也可以透過建立新版本來更新客戶管理的權限。已附加至資源共用的受管理權限不會自動更新。AWS RAM控制台確實指示何時有新的默認版本可用，並且您可以查看與前一個版本相比的新默認版本中的更改。

> **Note**
>
> 我們建議您盡快更新至新版的AWS受管理權限。這些更新通常增加了對可以使用共享其他資源類型的新的或更AWS 服務新的支持AWS RAM。新的預設版本也可以解決和修正安全性弱點。

> **Important**
>
> 您只能將受管理權限的預設版本附加至新的資源共用。

您可以隨時擷取可用的受管理許可。如需詳細資訊，請參閱檢視受管理權限。

主題

檢視受管理權限

您可以檢視有關可指派給資源共用資源類型之受管理權限的詳細資訊。您可以識別指派給資源共用的受管理權限。若要查看這些詳細資料，請使用AWS RAM主控台中的受管理權限程式庫。

Console

若要檢視可用的受管理權限的詳細資訊AWS RAM

1. 導覽至主控台中的 [受管理的權限程式庫] 頁AWS RAM面。
2. 由於AWS RAM資源共用存在於特定AWS 區域，請AWS 區域從主控台的右上角的下拉清單中選擇適當的。若要查看包含全域資源的資源共用，您必須AWS 區域將美國東部 (維吉尼亞北部)、(us-east-1)。如需分享全域資源的詳細資訊，請參閱「與全球資源相比，共享區域資源」。雖然所有區域都共用相同的可用AWS受管理權限，但這會影響中每個受管理權限顯示的關聯資源共用數目Step 5。客戶受管許可只適用於建立該許可的區域。
3. 在 [受管理的權限] 清單中，選擇您要檢視其詳細資料的受管理權限。您可以使用搜尋方塊，藉由輸入部分名稱或資源類型，或從下拉清單中選擇 Managed 許可類型，來篩選 Managed 許可清單。
4. (選擇性) 若要變更顯示偏好設定，請選擇許可面板右上角的齒輪圖示。您可以變更下列偏好設定：

   - 頁面大小 — 每個頁面上顯示的資源數量。
   - 換行 — 是否在表格列中換行。
   - 欄 — 是否顯示或隱藏有關資源類型和關聯共用的資訊。

   完成設定顯示偏好設定後，請選擇「確認」。
5. 清單中會針對每個 Managed 許可，都會顯示下列資訊：

   - 受管理的權限名稱 — 受管理權限的名稱。
   - 資源類型 — 與受管理權限相關聯的資源類型。
   - 受管理的權限類型 — 受管理的權限是AWS受管理的權限還是客戶受管理的權限。
   - 關聯共用 — 與受管理權限相關聯的資源共用數目。如果出現數字，則您可以選擇數字來顯示具有下列資訊的資源共用率表格：
     - 資源共用名稱 — 與受管理權限相關聯的資源共用名稱。
     - 受管理的權限版本 — 附加至此資源共用的受管理權限版本。

- 「所有者」— 資源共享所有者的AWS 帳戶號碼。
- 允許外部主參與者 — 該資源共用是否允許與中組織外部的主參與者共用AWS Organizations。
- 狀態-資源共用和受管許可之間的關聯目前狀態。

- 狀態 — 描述受管理的權限是否為：
  - 可附加 — 您可以將受管理的權限附加至資源共用。
  - 無法附加 — 您無法將受管理權限附加至資源共用。
  - [刪除] — 受管理的權限不再有效，很快就會刪除。
  - [已刪除] — 已刪除受管理的權限。它會在「受管理」權限程式庫中消失之前保持可見兩個小時。

您可以選擇受管理權限的名稱，以顯示有關該受管理權限的詳細資訊。受管許可的詳細資訊頁面會顯示下列資訊：

- 資源類型 — 此受管理權限套用的AWS資源類型。
- 許可-您最多可以有五個版本的客戶管理許可。
- 預設版本 — 指定哪個版本為預設版本，因此會自動指定給使用此受管理權限的所有新資源共用。任何使用不同版本的現有資源共用都會顯示提示，讓您將資源共用更新為預設版本。
- ARN-受管許可的 Amazon Resource Name (ARN)。AWS受管許可的 ARN 會使用下列格式：

  ```
  arn:aws:ram::aws:permission/
  AWSRAM[DefaultPermission]ShareableResourceType
  ```

  子字串*[DefaultPermission]* (實際 ARN 中沒有括號) 僅存在於該資源類型 (指定為預設值) 的一個受管理權限的名稱中。
- 受管理的權限版本 — 您可以選擇要在此下拉式清單下方的索引標籤中顯示哪個版本的資訊。
  - 詳細資料標籤：
    - 建立時間 — 建立此受管理權限版本的日期和時間。
    - 上次更新時間 — 上次更新此受管理權限版本的日期和時間。
  - 策略範本標籤 — 此受管理權限版本允許主參與者對關聯的資源類型執行的服務動作與條件 (如果適用) 清單。
  - 關聯的資源共用 — 使用此版本受管理權限的資源共用清單。

AWS CLI

若要檢視可用的受管理權限的詳細資訊AWS RAM

您可以使用此list-permissions命令取得可用AWS 區域於呼叫帳戶目前資源共用的受管理權限清單。

```
$ aws ram list-permissions
{
    "permissions": [
        {
            "arn": "arn:aws:ram::aws:permission/
AWSRAMBlankEndEntityCertificateAPICSRPassthroughIssuanceCertificateAuthority",
            "version": "1",
            "defaultVersion": true,
            "name":
 "AWSRAMBlankEndEntityCertificateAPICSRPassthroughIssuanceCertificateAuthority",
            "resourceType": "acm-pca:CertificateAuthority",
            "status": "ATTACHABLE",
            "creationTime": "2022-06-30T13:03:31.732000-07:00",
            "lastUpdatedTime": "2022-06-30T13:03:31.732000-07:00",
            "isResourceTypeDefault": false,
            "permissionType": "AWS_MANAGED"
        },
        {
            "arn": "arn:aws:ram::aws:permission/
AWSRAMBlankEndEntityCertificateAPIPassthroughIssuanceCertificateAuthority",
            "version": "1",
            "defaultVersion": true,
            "name":
 "AWSRAMBlankEndEntityCertificateAPIPassthroughIssuanceCertificateAuthority",
            "resourceType": "acm-pca:CertificateAuthority",
            "status": "ATTACHABLE",
            "creationTime": "2022-11-18T07:05:46.976000-08:00",
            "lastUpdatedTime": "2022-11-18T07:05:46.976000-08:00",
            "isResourceTypeDefault": false,
            "permissionType": "AWS_MANAGED"
        },

        ... TRUNCATED FOR BREVITY ... RUN COMMAND TO SEE COMPLETE LIST OF
 PERMISSIONS ...

        {
            "arn": "arn:aws:ram::aws:permission/
AWSRAMVPCPermissionsNetworkManagerCoreNetwork",
```

```
            "version": "1",
            "defaultVersion": true,
            "name": "AWSRAMVPCPermissionsNetworkManagerCoreNetwork",
            "resourceType": "networkmanager:CoreNetwork",
            "status": "ATTACHABLE",
            "creationTime": "2022-06-30T13:03:46.557000-07:00",
            "lastUpdatedTime": "2022-06-30T13:03:46.557000-07:00",
            "isResourceTypeDefault": false,
            "permissionType": "AWS_MANAGED"
        },       {
            "arn": "arn:aws:ram:us-east-1:123456789012:permission/My-Test-CMP",
            "version": "1",
            "defaultVersion": true,
            "name": "My-Test-CMP",
            "resourceType": "ec2:IpamPool",
            "status": "ATTACHABLE",
            "creationTime": "2023-03-08T06:54:10.038000-08:00",
            "lastUpdatedTime": "2023-03-08T06:54:10.038000-08:00",
            "isResourceTypeDefault": false,
            "permissionType": "CUSTOMER_MANAGED"
        }
    ]
}
```

您也可以在`list-permissions`AWS CLI命令的`--query`參數中依其名稱尋找特定受管理權限的 ARN。下列範例會篩選輸出，使其在`permissions`陣列結果中僅包含符合指定名稱的元素。我們還指定我們只希望在結果中查看 ARN 字段，並以純文本格式而不是默認的 JSON 查看。

```
$ aws ram list-permissions \
    --query "permissions[?name == 'My-Test-CMP'].arn \
    --output text
arn:aws:ram:us-east-1:123456789012:permission/My-Test-CMP
```

找到您感興趣的特定受管理權限的 ARN 之後，您可以執行命令來擷取其詳細資料，包括其 JSON 原則文字get-permission。

```
$ aws ram get-permission \
    --permission-arn arn:aws:ram:us-east-1:123456789012:permission/My-Test-CMP
{
    "permission": {
        "arn": "arn:aws:ram:us-east-1:123456789012:permission/My-Test-CMP",
        "version": "1",
```

```
        "defaultVersion": true,
        "name": "My-Test-CMP",
        "resourceType": "ec2:IpamPool",
        "permission": "{\n\t\"Effect\": \"Allow\",\n\t\"Action\": [\n
\t\t\"ec2:GetIpamPoolAllocations\",\n\t\t\"ec2:GetIpamPoolCidrs\",\n\t
\t\"ec2:AllocateIpamPoolCidr\",\n\t\t\"ec2:AssociateVpcCidrBlock\",\n
\t\t\"ec2:CreateVpc\",\n\t\t\"ec2:ProvisionPublicIpv4PoolCidr\",\n\t\t
\"ec2:ReleaseIpamPoolAllocation\"\n\t]\n}",
        "creationTime": "2023-03-08T06:54:10.038000-08:00",
        "lastUpdatedTime": "2023-03-08T06:54:10.038000-08:00",
        "isResourceTypeDefault": false,
        "permissionType": "CUSTOMER_MANAGED",
        "featureSet": "STANDARD",
        "status": "ATTACHABLE"
    }
}
```


在中建立和使用客戶受管理的權限AWS RAM

AWS Resource Access Manager(AWS RAM) 為您可以共用的每個資源類型提供至少一個AWS Managed 權限。不過，這些受管理的權限可能無法為您的共用使用案例提供最少的權限存取。當其中一個提供的AWS受管理權限無法運作時，您可以建立自己的客戶受管權限。

客戶管理的權限是您編寫和維護的受管理權限，方法是精確指定在哪些情況下可以執行哪些動作與使用共用的資源AWS RAM。例如，您想要限制 Amazon VPC IP 位址管理員 (IPAM) 集區的讀取存取權限，以協助您大規模管理 IP 地址。您可以為開發人員建立客戶管理權限以指派 IP 位址，但無法檢視其他開發人員帳戶指派的 IP 位址範圍。您可以遵循最低權限的最佳實務，只授予最低權限的許可。

此外，您可以視需要更新或刪除客戶管理的權限。

主題

- 建立客戶受管許可
- 建立新版本的客戶受管許可
- 選擇不同版本作為客戶管理權限的預設版本
- 刪除客戶管理的權限版本
- 刪除客戶管理的權限

建立客戶受管許可

客戶管理的權限專屬於AWS 區域. 請務必在適當的區域中建立此客戶管理權限。

Console

建立客戶受管許可

1. 執行下列任意一項：
   - 瀏覽至受管理的權限庫，然後選擇 [建立客戶受管理的權限]。
   - 直接瀏覽至主控台中的 [建立客戶管理權限] 頁面。
2. 如需客戶受管權限詳細資訊，請輸入客戶受管理的權限名稱。
3. 選擇此受管理權限套用的資源類型。
4. 對於策略範本，您可以定義允許對此資源類型執行哪些作業。
   - 您可以選擇 [匯入受管理的權限]，以使用現有受管理權限的動作。
   - 在視覺化編輯器中選取或取消選取存取層級資訊，以符合您的需求。
   - 使用 JSON 編輯器新增或修改條件。
5. (選擇性) 若要將標籤附加至受管理的權限，請針對「標籤」輸入標籤金鑰和值。選擇「新增標籤」以新增其他標籤。若需要則重複此步驟。
6. 當您完成時，請選擇 [建立客戶受管權限]。

AWS CLI

建立客戶受管許可

- 執行建立權限命令，並指定名稱、客戶受管理權限套用的資源類型，以及政策範本內文。

  下列範例命令會建立`imagebuilder:Component`資源類型的受管理權限。

```
$ aws ram create-permission \
    --name TestCMP \
    --resource-type imagebuilder:Component \
    --policy-template "{\"Effect\":\"Allow\",\"Action\":
[\"imagebuilder:ListComponents\"]}"
{
    "permission": {
        "arn": "arn:aws:ram:us-east-1:123456789012:permission/TestCMP",
```

```
        "version": "1",
        "defaultVersion": true,
        "isResourceTypeDefault": false,
        "name": "TestCMP",
        "resourceType": "imagebuilder:Component",
        "status": "ATTACHABLE",
        "creationTime": 1680033769.401,
        "lastUpdatedTime": 1680033769.401
    }
}
```

建立新版本的客戶受管許可

如果客戶受管權限的使用案例發生變更，您可以建立受管理權限的新版本。這不會影響您現有的資源共用，只會影響未來使用此客戶管理權限的新資源共用。

每個受管理的權限最多可以有五個版本，但您只能關聯預設版本。

Console

建立新版本的客戶受管許可

1. 導覽至受管理的權限程式庫。
2. 依「客戶管理」篩選受管理的權限清單，或搜尋您要變更的客戶受管理權限名稱。
3. 從受管理的權限詳細資料頁面的 [受管理的權限版本] 區段下，選擇 [建立版本]。
4. 對於策略範本，您可以使用視覺化編輯器或 JSON 編輯器新增或移除動作和條件。

   您也可以選擇 [匯入受管理的權限]，以使用現有的原則範本。
5. 當您完成時，請選擇頁面底部的 [建立版本]。

AWS CLI

建立新版本的客戶受管許可

1. 找到您要為其建立新版本的受管許可的 Amazon Resource Name (ARN)。透過使用`--permission-type CUSTOMER_MANAGED`參數呼叫清單權限以僅包含客戶管理的權限來執行此操作。

   ```
   $ aws ram-cmp list-permissions --permission-type CUSTOMER_MANAGED
   ```

```
{
    "permissions": [
        {
            "arn": "arn:aws:ram:us-east-1:123456789012:permission/TestCMP",
            "version": "2",
            "defaultVersion": true,
            "isResourceTypeDefault": false,
            "name": "TestCMP",
            "permissionType": "CUSTOMER_MANAGED",
            "resourceType": "imagebuilder:Component",
            "status": "ATTACHABLE",
            "creationTime": 1680035597.346,
            "lastUpdatedTime": 1680035597.346
        }
    ]
}
```

2. 擁有 ARN 之後，您可以呼叫create-permission-version作業並提供更新的原則範本。

```
$ aws ram create-permission-version \
    --permission-arn arn:aws:ram:us-east-1:123456789012:permission/TestCMP \
    --policy-template {"Effect":"Allow","Action":
["imagebuilder:ListComponents"]}
{
    "permission": {
        "arn": "arn:aws:ram:us-east-1:123456789012:permission/TestCMP",
        "version": "2",
        "defaultVersion": true,
        "isResourceTypeDefault": false,
        "name": "TestCMP",
        "status": "ATTACHABLE",
        "resourceType": "imagebuilder:Component",
        "permission": "{\"Effect\":\"Allow\",\"Action\":
[\"imagebuilder:ListComponents\"]}",
        "creationTime": 1680038973.79,
        "lastUpdatedTime": 1680038973.79
    }
}
```

輸出包括新版本的版本號碼。

選擇不同版本作為客戶管理權限的預設版本

您可以將另一個客戶管理的權限版本設定為新的預設版本。

Console

若要為客戶管理的權限設定新的預設版本

1. 導覽至受管理的權限程式庫。
2. 依「客戶管理」篩選受管理的權限清單，或搜尋您要變更的客戶受管理權限名稱。
3. 在 [客戶管理的權限詳細資料] 頁面的 [受管理的權限版本] 區段下，使用下拉式清單選擇您要設定為新預設值的版本。
4. 選擇「設為預設版本」。
5. 當對話方塊出現時，請確認您希望此版本成為使用此客戶管理權限之所有新資源共用的預設版本。如果您同意，請選擇「設定為預設版本」。

AWS CLI

若要為客戶管理的權限設定新的預設版本

1. 通過調用找到要設置為默認版本的版本號list-permission-versions。

   下列範例命令會擷取指定受管權限的目前版本。

```
$ aws ram list-permission-versions \
    --permission-arn arn:aws:ram:us-east-1:123456789012:permission/TestCMP
{
    "permissions": [
        {
            "arn": "arn:aws:ram:us-east-1:123456789012:permission/TestCMP",
            "version": "1",
            "defaultVersion": false,
            "isResourceTypeDefault": false,
            "name": "TestCMP",
            "permissionType": "CUSTOMER_MANAGED",
            "featureSet": "STANDARD",
            "resourceType": "imagebuilder:Component",
            "status": "UNATTACHABLE",
            "creationTime": 1680033769.401,
```

```
            "lastUpdatedTime": 1680035597.345
        },
        {
            "arn": "arn:aws:ram:us-east-1:123456789012:permission/TestCMP",
            "version": "2",
            "defaultVersion": true,
            "isResourceTypeDefault": false,
            "name": "TestCMP",
            "permissionType": "CUSTOMER_MANAGED",
            "featureSet": "STANDARD",
            "resourceType": "imagebuilder:Component",
            "status": "ATTACHABLE",
            "creationTime": 1680035597.346,
            "lastUpdatedTime": 1680035597.346
        }
    ]
}
```

2. 將版本號設定為預設值之後，您可以呼叫該set-default-permission-version作業。

```
$ aws ram-cmp set-default-permission-version \
    --permission-arn arn:aws:ram:us-east-1:123456789012:permission/TestCMP \
    --version 2
```

如果成功，此命令不會傳回任何輸出。您可以list-permission-versions再次執行，並確認所選版本的`defaultVersion`欄位現在已設定為`true`。

刪除客戶管理的權限版本

您最多可以擁有每個客戶受管權限的五個版本。當版本不再需要的版本，而且不再需要的版本，可以將其刪除。您無法刪除客戶受管權限的預設版本。刪除的版本在控制台中保持可見最多兩個小時，並且在完全刪除之前會顯示已刪除的狀態。

Console

刪除客戶受管理的權限版本

1. 導覽至受管理的權限程式庫。
2. 依「客戶管理」篩選受管理的權限清單，或搜尋客戶受管理權限的名稱以及您要刪除的版本。
3. 請確定要刪除的版本不是預設版本。

4. 在頁面的 [版本] 段落中，選擇 [關聯的資源共用率] 索引標籤，查看是否有任何共用使用此版本。

   如果有任何關聯的共用，您必須先變更客戶管理的權限版本，才能刪除此版本。

5. 選擇「版本」部分右側的「刪除版本」。
6. 在確認對話方塊中，選取 [刪除] 以確認您要刪除此版本的客戶管理權限。

   如果您不想要刪除此版本的客戶受管權限，請選擇 [取消]。

AWS CLI

刪除客戶受管權限的版本

1. 呼叫作list-permission-versions業以擷取可用的版本號碼。
2. 取得版本號碼之後，請將其作為參數提供給delete-permission-version。

```
$ aws ram-cmp delete-permission-version \
    --permission-arn arn:aws:ram:us-east-1:123456789012:permission/TestCMP \
    --version 1
```

如果成功，此命令不會傳回任何輸出。您可以list-permission-versions再次執行，並確認該版本不再包含在輸出中。

刪除客戶管理的權限

如果不再需要客戶管理的權限，而且不使用中，您可以將其刪除。您無法刪除已和 Resource Name 建立關聯的客戶受管權限。刪除的客戶管理權限會在兩小時後消失。在此之前，它仍然可以在「受管理」權限程式庫中顯示為「已刪除」狀態。

Console

若要刪除客戶受管理的權限

1. 導覽至受管理的權限程式庫。
2. 依「客戶管理」篩選受管理的權限清單，或搜尋您要刪除的客戶受管理權限名稱。
3. 在選取客戶受管理的權限之前，請確認受管理的權限清單中有 0 個關聯的共用。

如果仍然存在與受管理權限相關聯的資源共用，則必須為所有資源共用指派另一個受管理的權限，然後才能繼續。

4. 在 [客戶受管權限詳細資料] 頁面的右上角，選擇 [刪除受管權限]。
5. 出現確認對話方塊時，選擇 [刪除] 以刪除受管理的權限。

AWS CLI

刪除客戶受管權限

1. 使用--permission-type CUSTOMER_MANAGED參數呼叫清單權限以僅包含客戶管理的權限，以尋找您要刪除之受管理權限的 ARN。

```
$ aws ram-cmp list-permissions --permission-type CUSTOMER_MANAGED
{
    "permissions": [
        {
            "arn": "arn:aws:ram:us-east-1:123456789012:permission/TestCMP",
            "version": "2",
            "defaultVersion": true,
            "isResourceTypeDefault": false,
            "name": "TestCMP",
            "permissionType": "CUSTOMER_MANAGED",
            "resourceType": "imagebuilder:Component",
            "status": "ATTACHABLE",
            "creationTime": 1680035597.346,
            "lastUpdatedTime": 1680035597.346
        }
    ]
}
```

2. 擁有要刪除之受管理權限的 ARN 之後，請將其作為參數提供以刪除權限。

```
$ aws ram delete-permission \
    --permission-arn arn:aws:ram:us-east-1:123456789012:permission/TestCMP
{
    "returnValue": true,
    "permissionStatus": "DELETING"
}
```

將AWS受管理的權限更新至較新版本

偶爾會AWS更新可附加至特定資源類型之資源共用的AWS受管理權限。執行AWS此操作時，會建立AWS受管理權限的新版本。包含指定資源類型的資源共用不會自動更新為使用受管理權限的最新版本。您必須明確更新每個資源共用的受管理權限。此額外步驟為必要步驟，以便在將變更套用至資源共用之前評估變更。

Console

每當控制台顯示一個頁面列出與資源共用相關聯的權限，並且其中一個或多個權限使用權限預設版本以外的版本時，控制台就會在控制台頁面的頂端顯示一個橫幅。標題表示您的資源共用使用的是預設值以外的版本。

此外，當目前版本號碼不是預設版本時，個別權限可以在目前版本號碼旁顯示 [更新為預設版本] 按鈕。

選擇該按鈕會啟動 [更新資源共用精靈]。在精靈的步驟 2 中，您可以更新任何非預設權限的版本，以使用其預設版本。

在精靈的最後一頁中選擇「送出」以完成精靈之前，系統不會儲存變更。

> **Note**
>
> 您只能附加預設版本，而且無法還原至其他版本。
> 對於客戶管理的權限，在您將權限更新為預設版本之後，除非您先將該版本設定為預設值，否則無法將其他版本套用至資源共用。例如，如果您更新了預設版本的權限，然後發現要復原的錯誤，則可以將先前的版本指定為預設版本。或者，您可以建立不同的新版本，然後將其指定為預設版本。執行其中一個選項之後，您就會更新資源共用，以使用現在的預設版本。

AWS CLI

更新受AWS管理權限的版本

1. get-resource-shares使用`--permission-arn`參數執行命令，以指定您要更新的受管權限的 Amazon 資源名稱 (ARN)。這會導致命令只傳回那些使用該 Managed 權限的資源共用。

   例如，下列範例命令會針對使用 Amazon EC2 容量保留的預設AWS受管許可的每個資源共用傳回詳細資料。

```
$ aws ram get-resource-shares \
    --resource-owner SELF \
    --permission-arn arn:aws:ram::aws:permission/
AWSRAMDefaultPermissionCapacityReservation
```

輸出包含每個資源共用的 ARN，其存取權由該 Managed 權限控制至少一個資源。

2. 針對上一個命令中指定的每個資源共用，執行命令associate-resource-share-permission。包含以指定`--resource-share-arn`要更新的資源共用、指定`--permission-arn`要更新的AWS Managed 權限，以及指定您要更新共用以使用該受管理權限的最新版本的`--replace`參數。您不需要指定版本號碼；系統會自動使用預設版本。

```
$ aws ram associate-resource-share-permission \
    --resource-share-arn < ARN of one of the shares from the output of the
 previous command > \
    --permission-arn arn:aws:ram::aws:permission/
AWSRAMDefaultPermissionCapacityReservation \
    --replace
```

3. 針對您在步驟 1 中從指令的結果中收到的每個`ResourceShareArn`指令重複上一個步驟中的指令。

在 中使用客戶受管許可的考量 AWS RAM

客戶受管許可僅適用於您在其中建立許可 AWS 區域 的 。並非所有資源類型都支援客戶受管許可。如需 中支援的資源類型清單 AWS Resource Access Manager，請參閱 可共用 AWS 的資源。

不支援具有多個陳述式的客戶受管許可。您只能在客戶受管許可中使用單一非負運算子。

客戶受管許可不支援下列條件：

- 用於比對主體屬性的條件索引鍵：
  - `aws:PrincipalOrgId`
  - `aws:PrincipalOrgPaths`
  - `aws:PrincipalAccount`

- 用於限制服務主體存取的條件金鑰：
  - `aws:SourceArn`

  - aws:SourceAccount
  - aws:SourceOrgPaths
  - aws:SourceOrgID
- 系統標籤：
  - aws:PrincipalTag/aws:
  - aws:ResourceTag/aws:
  - aws:RequestTag/aws:

> **Note**
>
> 分享給服務主體時，會自動填入該aws:SourceAccount值。

管理權限的運作方式

如需快速概觀，請觀看下列影片，其中示範受管理的權限如何讓您將最低權限存取的最佳作法套用至資AWS源。

此影片示範如何依照最低權限的最佳實務，建立客戶受管理的許可，並建立與建立關聯。如需詳細資訊，請參閱 ???。

建立資源共用時，您可以將AWS受管理的權限與您要共用的每個資源類型建立關聯。如果受管理的權限具有多個版本，則新資源共用一律會使用指定為預設的版本。

建立資源共用之後，AWS RAM會使用受管理的權限來產生附加至每個共用資源的資源型政策。

受管理權限中的原則範本會指定下列項目：

Effect

指出是Allow否要Deny對共用資源執行作業的主參與者權限。對於受管理的權限而言，效果永遠是Allow。如需詳細資訊，請參閱《IAM 使用者指南》中的 Eff ect。

動作

主體被授與執行權限的作業清單。這可以是AWS Command Line Interface (AWS CLI)AWS Management Console 或AWS API 中的作業中的動作。動作由AWS權限定義。如需詳細資訊，請參閱 IAM 使用者指南中的動作。

Condition

主參與者可以何時與資源共用中的資源互動。條件為您的共用資源增加了一層額外的安全性。使用它們來限制對共用資源進行敏感動作的存取。例如，您可以納入要求動作源自特定公司 IP 位址範圍的條件，或者動作必須由經過多重要素驗證驗證的使用者執行。如需有關條件的詳細資訊，請參閱《IAM 使用者指南》中的AWS全域條件內容金鑰。如需有關特定條件的詳細資訊，請參閱《服務授權參考》中的AWS服務的動作、資源與條件索引鍵。

> **Note**
>
> 條件適用於客戶受管理的權限和受AWS管理權限的支援資源類型。
> 如需排除不與客戶管理權限搭配使用之條件的相關資訊，請參閱在 中使用客戶受管許可的考量 AWS RAM。

受管理的權限類型

建立資源共用時，您可以選擇受管理的權限，以與您包含在資源共用中的每個資源類型相關聯。 AWS受管理的權限由AWS資源擁有的服務定義，並由管理AWS RAM。您可以編寫並維護自己的客戶管理權限。

- AWS受管理權限 — 每種AWS RAM支援的資源類型都有一個預設受管理權限可用。除非您明確選擇其中一個其他 Managed 權限，否則預設 Managed 權限是用於資源類型的權限。預設 Managed 權限旨在支援最常見的客戶案例，以共用指定類型的資源。預設 Managed 權限可讓主參與者執行由服務針對資源類型定義的特定動作。例如，對於 Amazon VPC`ec2:Subnet` 資源類型，預設受管權限允許主體執行下列動作：
  - `ec2:RunInstances`
  - `ec2:CreateNetworkInterface`
  - `ec2:DescribeSubnets`

  預設AWS受管理權限的名稱使用下列格`AWSRAMDefaultPermission`*`ShareableResourceType`*式：例如，對於資`ec2:Subnet`源類型，預設AWS受管理權限的名稱為`AWSRAMDefaultPermissionSubnet`。

> **Note**
>
> 預設受管理權限與受管理權限的預設版本不同。所有受管理的權限 (不論是預設或某些資源類型支援的其他受管理權限之一) 都是獨立的完整權限，具有不同效果，以及支援不同共用案例 (例如讀寫與唯讀存取) 的動作。任何受管理的權限，無論客戶管理AWS或客戶管理都可以有多個版本，其中一個版本是該權限的預設版本。

例如，當您共用同時支援完整存取 (`Read`和`Write`) 受管理權限和唯讀受管理權限的資源類型時，您可以為具有完整存取受管理權限的管理員建立一個資源共用。然後，您可以使用唯讀 Managed 權限為其他開發人員建立個別的資源共用，以遵循授與最少權限的做法。

> **Note**
>
> 所有AWS RAM支援至少一個預設受管理權限的AWS服務。您可以在 [受管理的權限程式庫] 頁面AWS 服務上檢視每個項目的可用權限。此頁面提供每個可用 Managed 權限的詳細資訊，包括目前與權限相關聯的任何資源共用，以及是否允許與外部主參與者共用 (如果適用)。如需詳細資訊，請參閱檢視受管理權限。
>
> 對於不支援其他受管理權限的服務，當您建立資源共用時，AWS RAM會自動套用為您選擇的資源類型定義的預設權限。如果支援，您也可以在 [關聯受管理權限] 頁面上選擇 [建立客戶受管理的權限]。

- 客戶受管權限 — 客戶管理的權限是您編寫和維護的受管理權限，方法是透過精確指定可在哪些情況下與使用共用資源執行的動作AWS RAM。例如，您想要限制 Amazon VPC IP 位址管理員 (IPAM) 集區的讀取存取權限，以協助您大規模管理 IP 地址。您可以為開發人員建立客戶管理權限以指派 IP 位址，但無法檢視其他開發人員帳戶指派的 IP 位址範圍。您可以遵循最低權限的最佳實務，只授予在共享資源上執行任務所需的許可。

中的安全性 AWS RAM

的雲端安全 AWS 是最高優先順序。作為 AWS 客戶，您受益於資料中心和網路架構，該架構旨在滿足最安全敏感組織的需求。

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

- 雲端的安全性 – AWS 負責保護在 中執行 AWS 服務的基礎設施 AWS 雲端。 AWS 也提供您可以安全使用的服務。在 AWS 合規計畫中，第三方稽核員會定期測試並驗證我們的安全功效。若要了解適用於 AWS Resource Access Manager (AWS RAM) 的合規計劃，請參閱合規計劃範圍內的AWS 服務。
- 雲端安全性 – 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 時套用共同的責任模型 AWS RAM。下列主題說明如何設定 AWS RAM 以符合您的安全和合規目標。您也會了解如何使用 AWS 其他服務來協助您監控和保護 AWS RAM 資源。

主題

- 中的資料保護 AWS RAM
- 的身分和存取管理 AWS RAM
- 在 中登入和監控 AWS RAM
- AWS RAM 中的恢復能力
- 中的基礎設施安全 AWS RAM
- 存取 AWS Resource Access Manager 使用介面端點 (AWS PrivateLink)

中的資料保護 AWS RAM

AWS 共同責任模型適用於 中的資料保護 AWS Resource Access Manager。如本模型所述， 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。FAQ如需歐洲資料保護的相關資訊，請參閱AWS 安全部落格 上的AWS 共同責任模型和GDPR部落格文章。

為了資料保護目的，我們建議您保護 AWS 帳戶 憑證，並使用 AWS IAM Identity Center 或 AWS Identity and Access Management （ ） 設定個別使用者IAM。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：

- 對每個帳戶使用多重要素驗證 （MFA）。
- 使用 SSL/TLS 與 AWS 資源通訊。我們需要 TLS 1.2 和 建議 TLS 1.3。
- 使用 設定 API和使用者活動日誌 AWS CloudTrail。如需使用 CloudTrail 線索擷取 AWS 活動的資訊，請參閱 AWS CloudTrail 使用者指南 中的使用 CloudTrail 線索。
- 使用 AWS 加密解決方案，以及 中的所有預設安全控制項 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 透過命令列介面或 FIPS 存取 時需要 140-3 個經過驗證的密碼編譯模組API，請使用FIPS端點。如需可用FIPS端點的詳細資訊，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 AWS RAM 或其他 AWS 服務 使用主控台API AWS CLI、 或 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。如果您將URL提供給外部伺服器，強烈建議您在 中不要包含憑證資訊，URL以驗證您對該伺服器的請求。

的身分和存取管理 AWS RAM

AWS Identity and Access Management （IAM） 是一種 AWS 服務，可協助管理員安全地控制對 AWS 資源的存取。管理員可IAM控制誰可以驗證 （登入） 和授權 （具有許可） 使用 AWS 資源。透過使用 IAM，您可以在 中建立主體，例如角色、使用者和群組 AWS 帳戶。您可以控制這些主體使用 AWS 資源執行任務的許可。您可以使用 IAM 而無需額外付費。如需管理和建立自訂IAM政策的詳細資訊，請參閱 IAM 使用者指南 中的管理IAM政策。

主題

- AWS RAM 如何使用 IAM
- AWS RAM 的 AWS 受管政策
- 使用 AWS RAM 的服務連結角色
- 適用於 AWS RAM 的範例 IAM 政策
- AWS Organizations 和 的服務控制政策範例 AWS RAM
- 停用資源共用 AWS Organizations

AWS RAM 如何使用 IAM

根據預設，IAM主體沒有建立或修改 AWS RAM 資源的許可。若要允許IAM主體建立或修改資源並執行任務，請執行下列其中一個步驟。這些動作授予使用特定資源和API動作的許可。

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。

- IAM 透過身分提供者在 中管理的使用者：

  建立聯合身分的角色。請遵循 IAM 使用者指南 中為第三方身分提供者（聯合）建立角色的指示。

- IAM 使用者：
  - 建立您的使用者可擔任的角色。請遵循 IAM 使用者指南 中為IAM使用者建立角色的指示。
  - (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 中的將許可新增至使用者（主控台）中的指示。

AWS RAM 提供數個 AWS 受管政策，您可以使用這些政策來解決許多使用者的需求。如需這些項目的詳細資訊，請參閱AWS RAM 的 AWS 受管政策。

如果您需要更精細地控制授予使用者的許可，您可以在IAM主控台中建構自己的政策。如需建立政策並將其連接至IAM角色和使用者的相關資訊，請參閱 AWS Identity and Access Management 使用者指南中的政策和許可IAM。

下列各節提供建置IAM許可政策 AWS RAM 的特定詳細資訊。

內容

政策結構

IAM 許可政策是包含下列陳述式JSON的文件：效果、動作、資源和條件。IAM 政策通常採用下列形式。

```
{
    "Statement":[{
        "Effect":"<effect>",
        "Action":"<action>",
        "Resource":"<arn>",
        "Condition":{
            "<comparison-operator>":{
                "<key>":"<value>"
            }
        }
    }]
}
```

Effect

效果陳述式指出政策是否允許或拒絕主體執行動作的許可。可能的值包括： `Allow`和 `Deny`。

動作

動作陳述式指定 AWS RAM API政策允許或拒絕許可的動作。如需允許動作的完整清單，請參閱 IAM 使用者指南 中的 定義的動作 AWS Resource Access Manager。

資源

資源陳述式會指定受政策影響 AWS RAM 的資源。若要在陳述式中指定資源，您需要使用其唯一的 Amazon Resource Name （ ARN ）。如需允許資源的完整清單，請參閱 IAM 使用者指南 中的 定義的資源 AWS Resource Access Manager。

條件

條件陳述式為選用。它們可用於進一步完善政策適用的條件。 AWS RAM 支援下列條件索引鍵：

- `aws:RequestTag/${TagKey}` – 測試服務請求是否包含具有指定標籤金鑰的標籤，並具有指定的值。
- `aws:ResourceTag/${TagKey}` – 測試由服務請求執行的資源是否具有附加標籤，其中包含您在政策中指定的標籤金鑰。

下列範例條件會檢查服務請求中參考的資源是否具有附加標籤，其金鑰名稱為「擁有者」且值為「開發團隊」。

```
"Condition" : {
    "StringEquals" : {
        "aws:ResourceTag/Owner" : "Dev Team"
    }
}
```

- `aws:TagKeys` – 指定必須用來建立或標記資源共用的標籤金鑰。
- `ram:AllowsExternalPrincipals` – 測試服務請求中的資源共用是否允許與外部主體共用。外部主體是 中您組織的 AWS 帳戶 外部 AWS Organizations。如果這評估為 `False`，則您只能與相同組織中的帳戶共用此資源共用。
- `ram:PermissionArn` – 測試服務請求中ARN指定的許可是否與您在政策中指定的ARN字串相符。
- `ram:PermissionResourceType` – 測試服務請求中指定的許可是否適用於您在政策中指定的資源類型。使用可共用資源類型清單中顯示的格式指定資源類型。
- `ram:Principal` – 測試在服務請求中指定的主體ARN的 是否符合您在政策中指定的ARN字串。
- `ram:RequestedAllowsExternalPrincipals` – 測試服務請求是否包含 `allowExternalPrincipals` 參數，以及其引數是否符合您在政策中指定的值。
- `ram:RequestedResourceType` – 測試正在執行的資源類型是否符合您在政策中指定的資源類型字串。使用可共用資源類型清單中顯示的格式指定資源類型。
- `ram:ResourceArn` – 測試由服務請求執行ARN的資源的 是否符合ARN您在政策中指定的 。
- `ram:ResourceShareName` – 測試服務請求所執行的資源共用名稱是否符合您在政策中指定的字串。
- `ram:ShareOwnerAccountId` – 測試由服務請求執行之資源共用的帳戶 ID 號碼，符合您在政策中指定的字串。

AWS RAM 的 AWS 受管政策

AWS Resource Access Manager目前提供了幾個AWS RAM受管理的策略，如本主題所述。

AWS 受管政策

- AWS 受管政策：AWSResourceAccessManagerReadOnlyAccess
- AWS 受管政策：AWSResourceAccessManagerFullAccess
- AWS 受管政策：AWSResourceAccessManagerResourceShareParticipantAccess

- AWS 受管政策：AWSResourceAccessManagerServiceRolePolicy
- AWS 受管政策的 AWS RAM 更新項目

在上述清單中，您可以將前三個政策附加到 IAM 角色、群組和使用者，以授予權限。清單中的最後一個策略會保留給AWS RAM服務的服務連結角色。

AWS 受管政策是由 AWS 建立和管理的獨立政策。AWS 受管政策的設計在於為許多常見使用案例提供許可，如此您就可以開始將許可指派給使用者、群組和角色。

請記住，AWS 受管政策可能不會授與您特定使用案例的最低權限許可，因為它們可供所有 AWS 客戶使用。我們建議您定義使用案例專屬的客戶管理政策，以便進一步減少許可。

您無法更改 AWS 受管政策中定義的許可。如果 AWS 更新 AWS 受管政策中定義的許可，更新會影響政策連接的所有主體身分 (使用者、群組和角色)。在推出新的 AWS 服務 或有新的 API 操作可供現有服務使用時，AWS 很可能會更新 AWS 受管政策。

如需詳細資訊，請參閱《IAM 使用者指南》https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_managed-vs-inline.html#aws-managed-policies中的 AWS 受管政策。

AWS 受管政策：AWSResourceAccessManagerReadOnlyAccess

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

此原則為您所擁有的資源共用提供唯讀權限AWS 帳戶。

它通過授予運行任何的權限來執行此操作`Get*`或者`List*`操作。它不提供任何修改資源共享的能力。

許可詳細資訊

此政策包含以下許可。

- `ram`— 可讓主參與者檢視帳號所擁有之資源共用的詳細資訊。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ram:Get*",
                "ram:List*"
```

```
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

AWS 受管政策：AWSResourceAccessManagerFullAccess

您可將 AWSResourceAccessManagerFullAccess 政策連接到 IAM 身分。

此原則提供完整的管理存取權，以檢視或修改您所擁有的資源共用AWS 帳戶。

它通過授予運行任何權限來做到這一點ram操作。

許可詳細資訊

此政策包含以下許可。

- ram— 允許主參與者檢視或修改有關資源共用的任何資訊，這些資訊由AWS 帳戶。

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

AWS 受管政策：AWSResourceAccessManagerResourceShareParticipantAccess

您可將 AWSResourceAccessManagerResourceShareParticipantAccess 政策連接到 IAM 身分。

此原則可讓主參與者接受或拒絕與此共用的資源共用AWS 帳戶，並檢視有關這些資源共用率的詳細資訊。它不提供任何修改這些資源共享的能力。

它通過授予運行一些權限來做到這一點ram操作。

許可詳細資訊

此政策包含以下許可。

- ram— 允許主參與者接受或拒絕資源共用邀請，以及檢視與帳號共用之資源共用的詳細資訊。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ram:AcceptResourceShareInvitation",
                "ram:GetResourcePolicies",
                "ram:GetResourceShareInvitations",
                "ram:GetResourceShares",
                "ram:ListPendingInvitationResources",
                "ram:ListPrincipals",
                "ram:ListResources",
                "ram:RejectResourceShareInvitation"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

AWS 受管政策：AWSResourceAccessManagerServiceRolePolicy

該AWS受管理政策AWSResourceAccessManagerServiceRolePolicy只能與下列項目的服務連結角色搭配使用AWS RAM。您無法附加、卸離、修改或刪除此原則。

本政策提供AWS RAM具有組織結構的唯讀存取權。當您啟用之間的整合
AWS RAM和AWS Organizations,AWS RAM自動建立名為的服務連結角色AWSServiceRoleForResourceAccessManager該服務假設何時需要查詢有關您組織及其帳戶的資訊，例如，當您在AWS RAM控制台。

它通過授予只讀權限來運行organizations:Describe和organizations:List提供組織結構和帳戶詳細資訊的作業。

許可詳細資訊

此政策包含以下許可。

- organizations— 允許主參與者檢視有關組織結構的資訊，包括組織單位，以及AWS 帳戶它們包含.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:ListAccounts",
                "organizations:ListAccountsForParent",
                "organizations:ListChildren",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListParents",
                "organizations:ListRoots"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowDeletionOfServiceLinkedRoleForResourceAccessManager",
            "Effect": "Allow",
            "Action": [
                "iam:DeleteRole"
            ],
            "Resource": [
                "arn:aws:iam::*:role/aws-service-role/ram.amazonaws.com/*"
            ]
        }
    ]
}
```

AWS 受管政策的 AWS RAM 更新項目

檢視自 AWS RAM 開始追蹤 AWS 受管政策變更以來的更新詳細資訊。如需有關此頁面變更的自動提醒，請訂閱 AWS RAM文件歷史記錄頁面上的 RSS 摘要。

變更	描述	日期
AWS Resource Access Manager 已開始追蹤變更	AWS RAM記錄其現有的受管理策略，並開始追蹤變更。	2021 年 9 月 16 日

使用 AWS RAM 的服務連結角色

AWS Resource Access Manager 會使用 AWS Identity and Access Management (IAM) 的服務連結角色。服務連結角色是直接連結至AWS RAM服務的唯一 IAM 角色類型。服務連結角色由預先定義，AWS並包含代表您呼叫其他AWS服務所AWS RAM需的所有權限。

服務連結角色可讓您AWS RAM更輕鬆地設定，因為您不需要手動新增必要的權限。 AWS RAM定義其服務連結角色的權限，除非另有定義，否則只AWS RAM能使用其服務連結角色。定義的許可包括信任政策和許可政策，而且該許可政策無法附加到任何其他 IAM 實體。

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

AWS RAM 服務連結角色許可

AWS RAM使用當您啟用共用`AWSServiceRoleForResourceAccessManager`時指定的服務連結角色。AWS Organizations此角色會授與AWS RAM服務檢視組織詳細資料的權限，例如成員帳戶清單以及每個帳戶所在的組織單位。

此服務連結角色會信任下列服務擔任該角色：

- `ram.amazonaws.com`

名為 AWSResourceAccessManagerServiceRolePolicy 的角色權限原則會附加至此服務連結角色，並允許AWS RAM對指定的資源完成下列動作：

- 動作：擷取組織結構詳細資訊的唯讀動作。如需完整的動作清單，您可以在 IAM 主控台中檢視政策：AWSResourceAccessManagerServiceRolePolicy。

若要讓主體在組織內開啟AWS RAM共用功能，該主體 (IAM 實體，例如使用者、群組或角色) 必須具有建立服務連結角色的權限。如需詳細資訊，請參閱《IAM 使用者指南》中的服務連結角色許可。

建立 的服務連結角色AWS RAM

您不需要手動建立一個服務連結角色。當您在中的組織內開啟AWS RAM共用功能AWS Management Console，或使用AWS CLI或 AWS API EnableSharingWithAwsOrganization在您的帳戶中執行時，AWS RAM會為您建立服務連結角色。

呼叫`enable-sharing-with-aws-organizations`以在您的帳戶中建立服務連結角色。

如果您刪除此服務連結角色，則AWS RAM不再具有檢視組織結構詳細資料的權限。

為 AWS RAM 編輯服務連結角色

AWS RAM不允許您編輯 AWSResourceAccessManagerServiceRolePolicy 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。然而，您可使用 IAM 來編輯角色描述。如需詳細資訊，請參閱《IAM 使用者指南》中的編輯服務連結角色。

刪除 AWS RAM 的服務連結角色

您可以使用 IAM 主控台、AWS CLI 或 AWS API 來手動刪除服務連結角色。

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 `AWSResourceAccessManagerServiceRolePolicy` 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。

AWS RAM 服務連結角色的支援區域

AWS RAM 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 中的 Amazon Web Services 一般參考 區域與端點。

適用於 AWS RAM 的範例 IAM 政策

本主題包含 IAM 政策範例，AWS RAM說明共用特定資源和資源類型，以及限制共用。

IAM 政策的範例

- 範例 1：允許共用特定資源
- 範例 2：允許共用特定資源類型
- 範例 3：限制與外部共用 AWS 帳戶

範例 1：允許共用特定資源

您可以使用 IAM 權限政策限制主體僅將特定資源與資源共用關聯。

例如，下列政策將主體限制為僅與指定的 Amazon 資源名稱 (ARN) 共用解析器規則。如果請求不包含`ResourceArn`參數，或者如果請求包含該參數，則運算符`StringEqualsIfExists`允許請求，它的值與指定的 ARN 完全匹配。

有關何時以及為什麼使用`...IfExists`運算符的更多信息，請參閱... IfExistsIAM 使用者指南中的條件運算子。

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": ["ram:CreateResourceShare", "ram:AssociateResourceShare"],
        "Resource": "*",
        "Condition": {
            "StringEqualsIfExists": {
                "ram:ResourceArn": "arn:aws:route53resolver:us-
west-2:123456789012:resolver-rule/rslvr-rr-5328a0899aexample"
            }
        }
    }]
}
```

範例 2：允許共用特定資源類型

您可以使用 IAM 政策限制主體僅將特定資源類型與資源共用關聯。

例如，下列原則將主參與者限制為僅共用解析器規則。

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": ["ram:CreateResourceShare", "ram:AssociateResourceShare"],
        "Resource": "*",
        "Condition": {
            "StringEqualsIfExists": {
                "ram:RequestedResourceType": "route53resolver:ResolverRule"
            }
```

```
        }
    }]
}
```

範例 3：限制與外部共用 AWS 帳戶

您可以使用 IAM 政策來防止主體與AWS 帳戶其AWS組織外部人員共用資源。

例如，下列 IAM 政策可防止主體將外部新增AWS 帳戶至資源共用。

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": "ram:CreateResourceShare",
        "Resource": "*",
        "Condition": {
            "Bool": {
                "ram:RequestedAllowsExternalPrincipals": "false"
            }
        }
    }]
}
```

AWS Organizations 和 的服務控制政策範例 AWS RAM

AWS RAM 支援服務控制政策 （SCPs）。SCPs 是您附加到組織中元素的政策，以管理該組織中的許可。SCP 會套用至 AWS 帳戶 您連接 之 元素下的所有 SCP。SCPs 可讓您集中控制組織中所有帳戶的可用許可上限。他們可以協助您確保 AWS 帳戶 遵守組織的存取控制準則。如需詳細資訊，請參閱《AWS Organizations 使用者指南》中的服務控制政策。

必要條件

若要使用 SCPs，您必須先執行下列動作：

- 啟用您組織的所有功能。如需詳細資訊，請參閱 AWS Organizations 使用者指南中的啟用組織中的所有功能
- 啟用 SCPs以在組織內使用。如需詳細資訊，請參閱 AWS Organizations 使用者指南中的啟用和停用政策類型
- 建立您需要SCPs的 。如需建立 的詳細資訊SCPs，請參閱 AWS Organizations 使用者指南 中的建立和更新SCPs。

服務控制政策的範例

內容

下列範例展示您可以如何控制組織中資源共享的各個層面。

範例 1：防止外部共用

下列SCP內容可防止使用者建立允許與共用使用者組織外部的主體共用的資源共用。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ram:CreateResourceShare",
                "ram:UpdateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "ram:RequestedAllowsExternalPrincipals": "true"
                }
            }
        }
    ]
}
```

範例 2：防止使用者接受來自組織外部帳戶的資源共用邀請

下列內容會SCP阻止受影響帳戶中的任何主體接受使用資源共用的邀請。與共用帳戶共用到相同組織中其他帳戶的資源共用不會產生邀請，因此不受此 影響SCP。

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "ram:AcceptResourceShareInvitation",
            "Resource": "*"
        }
    ]
}
```

範例 3：允許特定帳戶共用特定資源類型

下列SCP僅允許 帳戶111111111111和 222222222222 建立新的資源共用，以共用 Amazon EC2字首清單或將字首清單與現有資源共用建立關聯。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ram:AssociateResourceShare",
                "ram:CreateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalAccount": [
                        "111111111111",
                        "222222222222"
                    ]
                },
                "StringEqualsIfExists": {
                    "ram:RequestedResourceType": "ec2:PrefixList"
                }
            }
        }
    ]
}
```

範例 4：防止與整個組織或組織單位共用

下列SCP內容可防止使用者建立與整個組織或任何組織單位共用資源的資源共用。使用者可以與 AWS 帳戶 組織中的個人共用，也可以與IAM角色或使用者共用。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ram:CreateResourceShare",
                "ram:AssociateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "ram:Principal": [
                        "arn:aws:organizations::*:organization/*",
                        "arn:aws:organizations::*:ou/*"
                    ]
                }
            }
        }
    ]
}
```

範例 5：僅允許與特定主體共用

下列範例SCP允許使用者僅與組織o-12345abcdef,組織單位 ou-98765fedcba、 和 AWS 帳戶 共用資源111111111111。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ram:AssociateResourceShare",
        "ram:CreateResourceShare"
      ],
      "Resource": "*",
      "Condition": {
```

```
        "StringNotEquals": {
          "ram:Principal": [
            "arn:aws:organizations::123456789012:organization/o-12345abcdef",
            "arn:aws:organizations::123456789012:ou/o-12345abcdef/ou-98765fedcba",
            "111111111111"
          ]
        },
        "Null": {
          "ram:Principal": "false"
        }
      }
    }
  ]
}
```

停用資源共用 AWS Organizations

如果您先前已啟用共用功能，AWS Organizations且不再需要與整個組織或組織單位 (OU) 共用資源，您可以停用共用功能。當您停用與共用時AWS Organizations，所有組織或 OU 都會從您建立的資源共用中移除，而且這些組織或 OU 會失去共用資源的存取權。外部帳號 (透過邀請新增至資源共用的帳號) 不會受到影響，且會繼續與資源共用產生關聯。

若要停用共用 AWS Organizations

1. 使用AWS Organizationsdisable-aws-service-accessAWS CLI命令停AWS Organizations用受信任的存取權。

   ```
   $  aws organizations disable-aws-service-access --service-principal
    ram.amazonaws.com
   ```

   > **Important**
   >
   > 當您停用受信任的存取權時AWS Organizations，組織內的主參與者會從所有資源共用中移除，並失去對這些共用資源的存取權。

2. 使用 IAM 主控台AWS CLI、或 IAM API 操作刪除AWSServiceRoleForResourceAccessManager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。

在 中登入和監控 AWS RAM

監控是維護 和 AWS 解決方案可靠性、可用性 AWS RAM 和效能的重要部分。您應該從 AWS 解決方案的所有部分收集監控資料，以便在發生多點故障時更輕鬆地進行偵錯。 AWS 提供數種工具來監控 AWS RAM 資源和回應潛在事件：

Amazon EventBridge

提供 near-real-time描述 AWS resources. EventBridge enables 自動化事件驅動運算變更的系統事件串流，因為您可以在發生這些事件時，撰寫規則來監控特定事件並觸發其他服務 AWS 中的自動動作。如需詳細資訊，請參閱AWS RAM 使用 監控 EventBridge。

AWS CloudTrail

擷取 或 代表您進行的API呼叫和相關事件，並將日誌檔案 AWS 帳戶 傳遞至您指定的 Amazon S3 儲存貯體。您可以識別名為 的使用者和帳戶 AWS、進行呼叫的來源 IP 地址，以及呼叫的時間。如需詳細資訊，請參閱使用 AWS CloudTrail 記錄 AWS RAM API 呼叫。

AWS RAM 使用 監控 EventBridge

您可以使用 Amazon EventBridge為 中的特定事件設定自動通知 AWS RAM。來自 的事件 AWS RAM 會以 EventBridge 近乎即時的方式交付至 。您可以設定 EventBridge 來監控事件並叫用目標，以回應指出資源共用變更的事件。資源共用擁有者和授予資源共用存取權的主體對資源共用觸發事件的變更。

當您建立事件模式時，來源是 `aws.ram`。

> **Note**
>
> 請小心撰寫程式碼，這些程式碼取決於這些事件。我們無法保證這些事件，但會盡最大努力發出。如果 AWS RAM 嘗試發出事件時發生錯誤，服務會嘗試多次。不過，它可能會逾時，並導致失去該特定事件。

如需詳細資訊，請參閱 Amazon EventBridge 使用者指南。

範例：資源共用失敗警示

考慮您要與組織中的其他帳戶共用 Amazon EC2容量保留的案例。這樣做是降低成本的好方法。

但是，如果您不符合共用容量保留 的所有先決條件，則可能會無聲地執行共用資源中涉及的非同步任務。如果共用操作失敗，而您其他帳戶中的使用者嘗試啟動具有其中一個容量保留的執行個體，則

Amazon 會像容量保留已滿一樣EC2運作，而是將執行個體作為隨需執行個體啟動。這可能會導致高於預期的成本。

若要監控資源共用失敗，請設定 Amazon EventBridge 規則，以便在 AWS RAM 資源共用失敗時提醒您。下列教學程序使用 Amazon Simple Notification Service （SNS） 主題，在 EventBridge 發現資源共用失敗時通知所有主題訂閱者。如需 Amazon 的詳細資訊SNS，請參閱 Amazon Simple Notification Service 開發人員指南 。

建立規則，在資源共用失敗時通知您

1. 開啟 Amazon EventBridge 主控台 。
2. 在導覽窗格中，選擇規則 ，然後在規則清單中，選擇建立規則 。
3. 輸入規則的名稱和選用描述，然後選擇下一步。
4. 向下捲動至事件模式方塊，然後選擇自訂模式 （JSON 編輯器）。
5. 複製並貼上下列事件模式：

```
{
  "source": ["aws.ram"],
  "detail-type": ["Resource Sharing State Change"],
  "detail": {
    "event": ["Resource Share Association"],
    "status": ["failed"]
  }
}
```

6. 選擇 Next (下一步)。
7. 針對目標 1，在目標類型 下，選擇 AWS 服務。
8. 在選取目標 下，選擇SNS主題 。
9. 針對主題 ，選擇您要發佈通知SNS的主題。此主題必須已存在。
10. 選擇下一個 ，然後再次選擇下一個 以查看以檢閱您的組態。
11. 當您對選項感到滿意時，請選擇建立規則 。
12. 返回規則頁面，確保您的新規則標記為已啟用。如有必要，請選擇規則名稱旁的選項按鈕，然後選擇啟用 。

只要啟用該規則，任何失敗 AWS RAM 的資源共用都會向您發佈主題的收件人發出SNS警示。

您也可以嘗試從這些帳戶 Amazon EC2主控台中檢視共用容量保留，以確認共用容量保留可供共用的帳戶存取。

使用 AWS CloudTrail 記錄 AWS RAM API 呼叫

AWS RAM與整合AWS CloudTrail，提供由使用者、角色或服AWS務所採取之動作的記錄AWS RAM。CloudTrail 將的所有 API 呼叫擷取AWS RAM為事件。擷取的呼叫包括從 AWS RAM 主控台進行的呼叫，以及針對 AWS RAM API 操作的程式碼呼叫。如果您建立追蹤，就可以持續傳送 CloudTrail 事件至您指定的 Amazon S3 儲存貯體，包括的事件AWS RAM。即使未設定追蹤，您依然可以在 CloudTrail 主控台歷史記錄中檢視最新事件。使用由 CloudTrail 收集的資訊，以判斷對 AWS RAM 提出的請求、發出請求 IP 地址、請求者、提出請求的時間，以及其他詳細資訊。

若要取得有關的更多資訊 CloudTrail，請參閱AWS CloudTrail使用者指南。

AWS RAM中的資訊 CloudTrail

CloudTrail 當您建立帳戶AWS 帳戶時，系統即會在中啟用。此外AWS，發生活動時AWS RAM，系統便會將該 CloudTrail 活動記錄到事件歷史記錄中。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 事件歷程記錄檢視事件。

如需您 AWS 帳戶 帳戶中正在進行事件的記錄 (包含 AWS RAM 的事件)，請建立追蹤。線索能 CloudTrail 將日誌檔案交付至 Amazon S3 儲存貯體。根據預設，當您在主控台建立線索時，線索會套用到所有 AWS 區域。該追蹤會記錄來自 AWS 分割區中所有區域的事件，並將日誌檔案交付到您指定的 Amazon S3 儲存貯體。此外，您可以設定其他AWS服務，以進一步分析和處理 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 AWS 帳戶 的追蹤
- AWS 服務與 CloudTrail 記錄檔整合
- 設定的 Amazon SNS 通知 CloudTrail
- 接收多個區域的 CloudTrail 日誌檔案及接收多個帳戶的 CloudTrail 日誌檔案

所有AWS RAM動作均由「API 參考」記錄 CloudTrail 並記錄在「AWS RAMAPI 參考」中。例如，對 `CreateResourceShare`、`AssociateResourceShare` 及 `EnableSharingWithAwsOrganization` 動作發出的呼叫會在 CloudTrail 日誌檔案中產生項目。

每個事件或日誌項目都會包含可幫助您確定請求發出者的資訊。

- AWS 帳戶根認證

- AWS Identity and Access Management (IAM) 角色或聯合身分使用者提供的暫時安全憑證。
- IAM 使用者提供的長期安全憑證。
- 其他 AWS 服務。

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

了解 AWS RAM 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至您指定的 Amazon S3 儲存貯體。 CloudTrail 日誌檔案包含一個或多個日誌項目。一個事件為任何來源提出的單一請求，並包含請求動作、請求的日期和時間、請求參數等資訊。 CloudTrail 日誌檔案並非依公有 API 呼叫的堆疊追蹤排序，因此不會以任何特定順序出現。

以下範例會顯示`CreateResourceShare`動作的 CloudTrail 日誌項目。

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "NOPIOSFODNN7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/admin",
        "accountId": "111122223333",
        "accessKeyId": "BCDIOSFODNN7EXAMPLE",
        "userName": "admin"
    },
    "eventTime": "2018-11-03T04:23:19Z",
    "eventSource": "ram.amazonaws.com",
    "eventName": "CreateResourceShare",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.1.0",
    "userAgent": "aws-cli/1.16.2 Python/2.7.10 Darwin/16.7.0 botocore/1.11.2",
    "requestParameters": {
        "name": "foo"
    },
    "responseElements": {
        "resourceShare": {
            "allowExternalPrincipals": true,
            "name": "foo",
            "owningAccountId": "111122223333",
            "resourceShareArn": "arn:aws:ram:us-east-1:111122223333:resource-share/
EXAMPLE0-1234-abcd-1212-987656789098",
```

```
            "status": "ACTIVE"
        }
    },
    "requestID": "EXAMPLE0-abcd-1234-mnop-987654567876",
    "eventID": "EXAMPLE0-1234-abcd-hijk-543234565434",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```


AWS RAM 中的恢復能力

AWS 全球基礎架構是以 AWS 區域 與可用區域為中心建置的。AWS 區域 提供多個分開且隔離的實際可用區域，並以具備低延遲、高輸送量和高度備援特性的聯網相互連結。透過可用區域，您所設計與操作的應用程式和資料庫，就能夠在可用區域之間自動容錯移轉，而不會發生中斷。可用區域的可用性、容錯能力和擴充能力，均較單一或多個資料中心的傳統基礎設施還高。

如需 AWS 區域 與可用區域的詳細資訊，請參閱AWS全球基礎架構。

中的基礎設施安全 AWS RAM

作為受管服務， AWS Resource Access Manager 受到 AWS 全球網路安全的保護。如需有關 AWS 安全服務以及如何 AWS 保護基礎設施的資訊，請參閱 AWS Cloud Security 。若要使用基礎設施安全性的最佳實務來設計您的 AWS 環境，請參閱 Security Pillar AWS Well-Architected Framework 中的基礎設施保護。

您可以使用 AWS 已發佈的API呼叫 AWS RAM 透過網路存取 。使用者端必須支援下列專案：

- Transport Layer Security （ TLS ）。我們需要 TLS 1.2 和 建議 TLS 1.3。
- 具有完美前向秘密 （ PFS ） 的加密套件，例如 DHE （ Ephemeral Diffie-Hellman ） 或 ECDHE （ Elliptic Curve Ephemeral Diffie-Hellman ）。現代系統(如 Java 7 和更新版本)大多會支援這些模式。

此外，必須使用與IAM委託人相關聯的存取金鑰 ID 和秘密存取金鑰來簽署請求。或者，您可以使用 AWS Security Token Service (AWS STS) 以產生暫時安全憑證以簽署請求。

存取 AWS Resource Access Manager 使用介面端點 (AWS PrivateLink)

您可以使用... AWS PrivateLink 在您的VPC和之間創建私人連接 AWS Resource Access Manager。您可以訪問 AWS RAM 就好像它在你的VPC，沒有使用互聯網網關，NAT設備，VPN連接或 AWS Direct Connect 連接。您中的執行個體VPC不需要公用 IP 位址即可存取 AWS RAM.

您可以通過創建一個接口端點來建立此私人連接，由 AWS PrivateLink。 我們會在您為介面端點啟用的每個子網路中建立端點網路介面。這些是由請求者管理的網路介面，可做為目的地流量的入口點 AWS RAM.

如需詳細資訊，請參閱存取 AWS 服務 通過 AWS PrivateLink 中的 AWS PrivateLink 指南。

的注意事項 AWS RAM

設定的介面端點之前 AWS RAM，檢閱「注意事項」中的 AWS PrivateLink 指南。

AWS RAM 支援透過介面端點呼叫其所有API動作。

VPC端點策略支援 AWS RAM。 默認情況下，完全訪問 AWS RAM 允許透過介面端點。

建立的介面端點 AWS RAM

您可以為下列項目建立介面端點 AWS RAM 使用 Amazon VPC 控制台或 AWS Command Line Interface (AWS CLI). 如需詳細資訊，請參閱在 AWS PrivateLink 指南。

建立的介面端點 AWS RAM 使用下列服務名稱：

```
com.amazonaws.region.ram
```

如果您DNS為介面端點啟用私有，您可以API向 AWS RAM 使用其默認的區域DNS名稱。例如：`ram.us-east-1.amazonaws.com`。

為您的介面端點建立端點政策

端點策略是您可以附加到介面端點的IAM資源。預設端點策略允許完整存取 AWS RAM 通過接口端點。若要控制允許的存取 AWS RAM 從您的VPC，將自定義端點策略附加到接口端點。

端點政策會指定以下資訊：

- 可以執行動作的主參與者 (AWS 帳戶、IAM使用者和IAM角色)。
- 可執行的動作。
- 可供執行動作的資源。

有關詳情，請參閱使用端點策略控制對服務的存取 AWS PrivateLink 指南。

範例：VPC端點策略 AWS RAM actions

以下是自訂端點政策的範例。當您將此原則附加到介面端點時，它會授予對列出的存取權 AWS RAM 所有資源上所有主參與者的動作。

```
{
    "Version": "2012-10-17",
    "Statement":
        [
            {
            "Effect": "Allow",
            "Principal": "*",
            "Action": [
                "ram:CreateResourceShare"
            ],
            "Resource": "*"
            }
        ]
}
```

對 的問題進行故障診斷 AWS RAM

使用指南本節中的資訊，協助您診斷和修正使用 AWS Resource Access Manager () 時的常見問題 AWS RAM。

主題

錯誤：「您的帳戶 ID 不存在於 AWS 組織中」

案例

嘗試與組織中的帳戶或組織單位 () 共用資源時，您會收到錯誤「您的帳戶 ID 不存在 AWS 於組織中」。OUs

原因

如果您開啟 AWS Resource Access Manager 和 之間的整合時AWSServiceRoleForResourceAccessManager，未成功建立服務連結角色，則可能會發生此錯誤 AWS Organizations。

解決方案

若要重新建立所需的服務連結角色，請執行下列步驟來關閉整合，然後再次開啟。

> **Important**
>
> 當您停用可信任存取時 AWS Organizations，組織內的主體會從所有資源共用中移除，並失去這些共用資源的存取權。

1. 使用具有管理許可IAM的角色或使用者登入組織的管理帳戶。
2. 導覽至 AWS Organizations 主控台中的服務頁面。
3. 選擇 RAM。
4. 選擇停用受信任的存取。
5. 導覽至AWS RAM 主控台中的設定頁面。
6. 選取方塊 啟用與 共用 AWS Organizations，然後選擇儲存設定。

您現在應該能夠使用 AWS RAM 與 帳戶和OUs組織中的 共用資源。

錯誤："AccessDeniedException"

案例

嘗試共用資源或檢視資源共用時，您會收到存取遭拒例外狀況。

原因

如果您嘗試在沒有必要的許可時建立資源共享，則可能會收到此錯誤。這可能是由於連接到您的 AWS Identity and Access Management (IAM) 委託人之政策的許可不足所致。也可能因為服務 AWS Organizations 控制政策 (SCP) 對 造成影響的限制而發生這種情況 AWS 帳戶。

解決方案

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。
- IAM 透過身分提供者在 中管理的使用者：

建立聯合身分的角色。遵循 IAM 使用者指南中為第三方身分提供者（聯合）建立角色的指示。

- IAM 使用者：
  - 建立您的使用者可擔任的角色。遵循 IAM 使用者指南中為IAM使用者建立角色的指示。
  - (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。遵循 IAM 使用者指南中新增許可給使用者（主控台）的指示。

若要解決錯誤，您需要確保發出請求的委託人所使用的許可政策中的Allow陳述式授予許可。此外，您組織的 不得封鎖許可SCPs。

若要建立資源共享，您需要下列兩個許可：

- `ram:CreateResourceShare`

- `ram:AssociateResourceShare`

若要檢視資源共用，您需要下列許可：

- `ram:GetResourceShares`

若要將許可連接到資源共享，您需要下列許可：

- *`resourceOwningService`*`:`*`PutPolicyAction`*

  這是預留位置。您必須將其取代為擁有您要共用資源之服務的「PutPolicy」許可（或同等許可）。例如，如果您共用 Route 53 解析程式規則，則所需的許可為：`route53resolver:PutResolverRulePolicy`。如果您想要允許建立包含多種資源類型的資源共享，則必須包含要允許的每個資源類型的相關許可。

下列範例顯示這類IAM許可政策的外觀。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ram:CreateResourceShare",
```

```
                "ram:AssociateResourceShare",
                "ram:GetResourceShares",
                "resourceOwningService:PutPolicyAction"
            ],
            "Resource": "*"
        }
    ]
}
```

錯誤："UnknownResourceException"

案例

您發生下列其中一個錯誤：

- "CannotCreateResourceShare： UnknownResourceException： OrganizationalUnit ou-*xxxx* 找不到"
- "CannotUpdateResourceShare： UnknownResourceException： OrganizationalUnit ou-*xxxx* 找不到 。

原因

如果您使用 Organizations AWS Organizations 主控台或 Organizations E Access 而非使用 AWS RAM 主控台來啟用 AWS RAM 和 之間的整合，則可能會發生這些錯誤。nableAWSService API當您使用 Organizations 主控台或 啟用整合時API，服務不會在您的帳戶中建立`AWSServiceRoleForResourceAccessManager`角色。存取組織的相關資訊需要該角色。由於角色尚未建立， AWS RAM 因此無法存取您組織中帳戶或組織單位 (OUs) 的詳細資訊。

解決方案

若要解決此問題，請關閉 AWS RAM 和 之間的整合 AWS Organizations。然後呼叫 AWS RAM EnableSharingWithAwsOrganizationAPI操作，或使用 執行下列步驟 AWS Management Console ，再次將其開啟。

> **Important**
>
> 當您停用可信任存取時 AWS Organizations，組織內的主體會從所有資源共用中移除，並失去這些共用資源的存取權。

1. 使用具有管理許可IAM的角色或使用者登入組織的管理帳戶。
2. 導覽至 AWS Organizations 主控台中的服務頁面。
3. 選擇 RAM。
4. 選擇停用受信任的存取。
5. 導覽至AWS RAM 主控台中的設定頁面。
6. 選取方塊 啟用與 共用 AWS Organizations，然後選擇儲存設定。

您現在應該能夠使用 AWS RAM 與 帳戶和OUs組織中的 共用資源。

嘗試與組織外部帳戶共用時發生錯誤

案例

當您嘗試與組織外部的帳戶共用資源時，會收到下列其中一個錯誤：

- 「您無法在組織外部共用資源。」
- 「您嘗試共用的資源只能在您的 AWS 組織內共用。」
- "InvalidParameterException：主要帳戶 ID 不在您的 AWS 組織中。您沒有將外部新增至資源共用 AWS 帳戶 的許可。」
- "OperationNotPermittedException：您嘗試共用的資源只能在您的 AWS 組織內共用。"

可能的原因和解決方案

有些資源類型只能與相同組織中的帳戶共用

有些資源類型無法與非該組織成員的任何帳戶共用。具有此限制的範例資源類型是屬於 Amazon Elastic Compute Cloud (Amazon VPCs) 一部分的虛擬私有連線 ()EC2。

若要驗證您是否可與組織外部的帳戶和主體共用特定資源類型，請參閱可 AWS 共用資源。

服務連結角色未成功建立

如果您開啟 AWS RAM 和 之間的整合時`AWSServiceRoleForResourceAccessManager`，服務連結角色未成功建立，則可能會發生此問題 AWS Organizations。

如果您在嘗試與屬於您組織一部分的帳戶共用資源時收到這些錯誤之一，請執行下列步驟來刪除並重新建立服務連結角色。

> **Important**
>
> 當您停用可信任存取時 AWS Organizations，組織內的主體會從所有資源共用中移除，並失去這些共用資源的存取權。

1. 使用具有管理許可IAM的角色或使用者登入組織的管理帳戶。
2. 導覽至 AWS Organizations 主控台中的服務頁面。
3. 選擇 RAM。
4. 選擇停用受信任的存取。
5. 導覽至AWS RAM 主控台中的設定頁面。
6. 選取方塊 啟用與 共用 AWS Organizations，然後選擇儲存設定。

在目的地帳戶中看不到共用資源

案例

使用者看不到他們認為從其他 與他們共用的資源 AWS 帳戶。

可能的原因和解決方案

使用 Organizations 而非 AWS Organizations 開啟與 的共用 AWS RAM

如果 是使用 Organizations 而非 AWS Organizations 開啟 AWS RAM，則組織內的共用會失敗。若要檢查這是否為問題的原因，請導覽至主控台中的 AWS RAM 設定頁面，並確認已選取啟用與 共用 AWS Organizations核取方塊。

- 如果選取核取方塊，則這不是原因。
- 如果未選取核取方塊，則可能是原因。尚未選取核取方塊。執行下列步驟以修正情況。

> **Important**
>
> 當您停用可信任存取時 AWS Organizations，組織內的主體會從所有資源共用中移除，並失去這些共用資源的存取權。

1. 使用具有管理許可IAM的角色或使用者登入組織的管理帳戶。
2. 導覽至 AWS Organizations 主控台中的服務頁面。
3. 選擇 RAM。
4. 選擇停用受信任的存取。
5. 導覽至AWS RAM 主控台中的設定頁面。
6. 選取方塊 啟用與 共用 AWS Organizations，然後選擇儲存設定。

您可能需要更新共用，並指定組織內要共用的帳戶或組織單位。

資源共用不會將此帳戶指定為主體

在 AWS 帳戶 建立資源共用的 中，檢視 主控台中的資源共用。 AWS RAM確認無法存取資源的帳戶列為委託人。如果不是，則更新共用以將帳戶新增為主體。

帳戶中的角色或使用者沒有所需的最低許可

當您將帳戶 A 中的資源分享給另一個帳戶 B 時，帳戶 B 中的角色和使用者不會自動存取共用中的資源。帳戶 B 的管理員必須先將許可授予帳戶 B 中需要存取資源IAM的角色和使用者。例如，以下政策顯示如何授予 B 帳戶中角色和使用者的唯讀存取權，以從帳戶 A 取得資源。政策會依其 Amazon Resource Name (ARN) 指定資源。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ram:Get*",
                "ram:List*"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:<service>:<Region-code>:<Account-A-ID>:<resource-id>"
        }
    ]
}
```

資源與目前的主控台設定 AWS 區域 不同

AWS RAM 是區域性服務。資源存在於特定 中 AWS 區域，若要查看它們， AWS Management Console 必須設定 來檢視該區域中的資源。

主控台目前正在存取 AWS 區域 的 會顯示在主控台的右上角。若要變更它，請選擇目前的區域名稱，然後從下拉式功能表中選擇您要查看其資源的區域。

錯誤：超過限制

案例

您在嘗試共用資源時收到「您已達到可共用資源的數量限制」或「ResourceShareLimitExceededException」。

原因

當您使用 AWS RAM 服務或 AWS 服務 建立您嘗試共用之資源的 達到可共用的資源數量上限時，就會發生這些錯誤。此配額 （先前稱為限制） 可能會影響共用帳戶或您要共用資源的帳戶。

解決方案

1. 若要檢視配額，請在您看到錯誤的 AWS 帳戶 中，導覽至下列其中一個頁面，視您到達的配額類型而定：
   - AWS RAM Service Quotas 主控台中的頁面
   - 資源受配額影響的 頁面 AWS 服務
2. 向下捲動並選擇相關的配額。
3. 如果可用於此配額，請選擇請求配額增加。
4. 輸入配額的新值，然後選擇請求。
5. 請求會出現在 Quota 請求歷史記錄頁面上，您可以在該頁面上查看請求的狀態，直到完成為止。

我組織中的另一個帳戶從未收到邀請

案例

當您與由 管理的同一組織中的另一個帳戶共用資源時 AWS Organizations，他們不會收到邀請。

原因

如果您的 帳戶在組織內已開啟共用， AWS則這是預期的行為。

當開啟此選項，且您與您組織中的另一個帳戶共用時，不會傳送邀請，也不需要接受。您參考為資源共享中主體的所有組織帳戶都可以立即開始存取共享中的資源。

如果您的帳戶尚未開啟組織內的共用 AWS ，則當您與其他帳戶共用時，即使它們位於同一個 AWS 組織中，它們也會被視為獨立帳戶。邀請會傳送，且必須先接受，使用者才能存取共享中的資源。

您無法共用VPC子網路

案例

當您嘗試使用 與其他帳戶 AWS RAM 共用VPC子網路時，共用操作會成功。不過，耗用帳戶會在 AWS RAM 主控台中`LIMIT EXCEEDED`顯示該資源。

原因

有些個別資源類型具有服務特定的限制，與 強制執行的限制不同 AWS RAM。即使您尚未達到其中的其中一個限制，其中一些限制仍可能會有效地防止共用 AWS RAM。限制是這些限制的範例。Amazon Virtual Private Cloud (Amazon VPC) 會限制您可以與其他個別帳戶共用的子網路數量。如果您嘗試與已包含最大子網路數量的耗用帳戶共用子網路，則該耗用帳戶會顯示在該資源的 主控台`LIMIT EXCEEDED`中。如需此限制的詳細資訊，請參閱《Amazon Virtual Private Cloud 使用者指南》中的 Amazon VPC Quotas – VPC共用。 Amazon Virtual Private Cloud

若要解決此問題，請先檢查是否有其他資源共享可能與受影響的帳戶共用指定的資源，並移除您可能不再需要的共享。您也可以請求提高支援調整的限制。使用 Service Quotas 主控台請求提高限制。

> **Note**
>
> AWS RAM 不會自動偵測限制增加變更。您必須將資源或主體重新與 的資源共用建立關聯，RAM才能偵測變更。

的服務配額 AWS RAM

您AWS 帳戶有下列與 AWS Resource Access Manager (AWS RAM) 相關的限制。您可以對一部分限制請求提高限制。聯絡 Support 以請求增加限制。

> **Note**
>
> 下列定義適用於下列配額中的說明：
>
> - 資源 — 您要共用的個別AWS 服務建立元素，例如 Amazon S3 儲存貯體或 Amazon EC2 執行個體。根據此配額，資源共用中參照的每個資源都算作一個資源。如果您在三個不同的資源共用中共用相同的資源，則會將此配額的計數增加三個。
> - 資源共用 — 可用來共用資源的AWS RAM已建立容器。每個資源共用 (無論其包含多少資源) 都會計為一個配額。
> - 共用主參與者 — 您已與資源共用相關聯的識別元。這可以是 AWS Identity and Access Management (IAM) 角色或使用者、AWS 帳戶識別碼、組織單位或整個組織。您在資源共用中參照的每個共用主參與者都會在配額使用中新增一個主參與者。如果您透過參照組織的 ID 與整個組織共用，這個配額只會計為一個組織。
> - 客戶受管理的權限 — 您建立的受管理權限，這些權限是為了解決使用最低權限存取的特定使用案例，以管理共用資源使用方式

資源	預設限制
每個資源共用數目上限 AWS 區域	25,000
每個資源共用的最大資源關聯數	5,000
每個資源共用的主參與者關聯數目上限	5,000
客戶管理權限的最大數量	1,500
每個資源類型的客戶管理權限數目上限	10
每個客戶受管理權限的版本數目上限	5
中所有資源共用之資源關聯的最大資源關聯數 AWS 區域	25,000

資源	預設限制
Note 資源共用中包含的每個資源都會計入此限制。如果資源包含在 10 個不同的資源共用率中，則此限制會計為 10。	
中所有資源共用的主參與者關聯數目上限 AWS 區域 **Note** 資源共用中包含的每個主參與者都會計入此限制。如果主參與者包含在 10 個不同的資源共用中，則會計入 10 個限制。	25,000
每個共享帳戶的待處理邀請數目上限 • 此配額僅適用於與不屬於相同帳戶共用的傳送帳戶AWS Organizations。 • 沒有配額限制可以限制接收帳戶可以擁有多少邀請擱置中。 • 在屬於相同帳號的帳號之間共用，AWS Organizations且您已在中開啟資源共用功能時，不會使用邀請AWS Organizations。	250

搭配 AWS SDK 使用 AWS RAM

AWS 軟體開發套件 (SDK) 適用於許多常用的程式設計語言。每個 SDK 都提供 API、程式碼範例和說明文件，讓開發人員能夠更輕鬆地以偏好的語言建置應用程式。

SDK 文件	程式碼範例
AWS SDK for C++	AWS SDK for C++ 程式碼範例
AWS SDK for Go	AWS SDK for Go 程式碼範例
AWS SDK for Java	AWS SDK for Java 程式碼範例
AWS SDK for JavaScript	AWS SDK for JavaScript 程式碼範例
AWS SDK for .NET	AWS SDK for .NET 程式碼範例
AWS SDK for PHP	AWS SDK for PHP 程式碼範例
AWS SDK for Python (Boto3)	AWS SDK for Python (Boto3) 程式碼範例
AWS SDK for Ruby	AWS SDK for Ruby 程式碼範例

可用性範例

找不到所需的內容嗎？ 要求含有意見反應連結的程式碼範例。

AWS RAM 使用者指南的文件歷史記錄

下表說明 AWS Resource Access Manager 文件的重要新增項目。我們也更新文件，以處理您傳送給我們的意見回饋。

如需這些更新的通知，您可以訂閱摘要 AWS RAM RSS。

變更	描述	日期
已新增共享 AWS Billing 資源的支援。	您現在可以與 AWS 帳戶 組織中的其他 共用 AWS Billing 檢視。	2024 年 12 月 20 日
新增了共用 Amazon API Gateway 資源的支援。	您現在可以與組織中的其他 AWS 帳戶 或 共用API閘道網域名稱。	2024 年 11 月 21 日
新增了共用 Amazon VPC 資源的支援。	您現在可以與組織中的其他 AWS 帳戶 或 共用 Amazon VPC Security 群組。	2024 年 10 月 30 日
已新增共享 AWS End User Messaging SMS 資源的支援。	您可以與其他 AWS 帳戶 或您的組織共用 AWS End User Messaging SMS 資源 AWS RAM。	2024 年 9 月 24 日
AWS PrivateLink	使用 AWS PrivateLink for AWS RAM，您可以使用虛擬私有雲端 () RAM 中的介面端點直接連線至 VPC。	2024 年 9 月 9 日
新增了共用的支援 AWS Backup。	您可以在組織之間 AWS 帳戶 或內部共用邏輯氣隙隔離保存庫。	2024 年 8 月 7 日
新增了共享 Amazon Bedrock 自訂模型的支援	您現在可以使用 與其他 AWS 帳戶 和您的組織 AWS RAM	2024 年 8 月 1 日

	共用 Amazon Bedrock 自訂模型。	
新增了共用 AWS CloudHSM 備份的支援。	您可以與其他 AWS 帳戶 或您的組織共用 AWS CloudHSM 備份 AWS RAM。	2024 年 6 月 28 日
新增了共用 Amazon SageMaker AI 的支援 Model Registry 資源。	您現在可以在組織之間 AWS 帳戶 或內部安全且有效率地共用進階參數。	2024 年 6 月 27 日
新增了共用 Amazon SageMaker AI 的支援 JumpStart。	您現在可以與組織 AWS 帳戶 或在組織內共用 Amazon SageMaker AI JumpStart Hub。	2024 年 6 月 27 日
新增了共用的支援 Amazon Route 53 ResolverProfiles.	您現在可以使用 AWS RAM 來共用 Amazon Route 53 Resolver Profiles AWS 帳戶 組織中的其他 。	2024 年 4 月 22 日
新增了共用 AWS Systems Manager 參數存放區資源的支援。	您現在可以在組織之間 AWS 帳戶 或內部安全且有效率地共用進階參數。	2024 年 2 月 21 日
新增了共用 Amazon FSx for OpenZFS Snapshots 的支援。	您現在可以與 AWS 帳戶 組織內的其他 共用 Amazon FSx for OpenZFS Snapshots。	2023 年 12 月 19 日
新增了共用 Amazon Simple Storage Service 資源的支援。	您現在可以與其他 AWS 帳戶 或您的組織共用 Amazon Simple Storage Service Access Grants 執行個體 AWS RAM。	2023 年 11 月 27 日
新增了共用 AWS 資源總管 檢視的支援。	您現在可以與 AWS 帳戶 組織內的其他 共用 AWS 資源總管檢視。	2023 年 11 月 14 日

新增了共用 Amazon Application Recovery Controller (ARC) 資源的支援。	您現在可以與其他 AWS 帳戶 或您的組織共用 Amazon Application Recovery Controller (ARC) 叢集 AWS RAM。	2023 年 10 月 18 日
新增了共用 Amazon DataZone 資源的支援。	您現在可以與其他 AWS 帳戶 或您的組織共用 Amazon DataZone 資源。	2023 年 10 月 4 日
新增對服務主體共用的支援。	您現在可以將服務主體與資源共用建立關聯。這可讓指定的服務代表您管理客戶資源的必要動作。	2023 年 8 月 29 日
新增共享 SageMaker 模型卡資源的支援。	您現在可以與其他 AWS 帳戶 或您的組織共用 SageMaker 模型卡資源。	2023 年 8 月 18 日
新增對 Amazon SageMaker AI Feature Store 功能群組和 SageMaker AI Catalog 的支援，做為可共用的資源。	您現在可以與其他 AWS 帳戶 或您的組織共用 Amazon SageMaker AI Feature Store 功能群組和 SageMaker AI Catalog 資源。	2023 年 7 月 20 日
待定邀請的服務配額限制增加。	每個共用帳戶的待處理邀請數量上限已從 20 個增加到 250 個。	2023 年 6 月 8 日
新增對 AWS AppSync GraphQL 的支援APIs做為可共用的資源。	您現在可以 AWS 帳戶 使用 APIs 與其他 共用 AWS AppSync GraphQL AWS RAM。	2023 年 5 月 24 日
新增對 AWS Verified Access 群組的支援做為可共用的資源。	您現在可以集中建立和管理 AWS Verified Access 群組，然後與其他 AWS 帳戶 或您的組織共用。	2023 年 4 月 27 日

在 AWS RAM 主控台中新增對客戶受管許可的支援。	您現在可以安全地為支援的資源類型撰寫和維護精細的資源存取控制。	2023 年 4 月 19 日
新增對 Amazon VPC Lattice 服務和服務網路可共用資源的支援。	您現在可以與其他 共用 Amazon VPC Lattice 服務和服務網路資源 AWS 帳戶。	2023 年 3 月 31 日
新增對 AWS Marketplace 目錄實體的支援做為可共用的資源。	您現在可以在 Marketplace AWS 帳戶 中與其他 共用實體。	2023 年 3 月 27 日
新增在 AWS RAM 主控台中管理許可版本的支援。	您現在可以使用 AWS RAM 主控台來檢視版本詳細資訊，並將許可更新為指定為預設值的任何版本。	2023 年 1 月 16 日
IAM 最佳實務更新。	更新指南以符合IAM最佳實務。如需詳細資訊，請參閱 中的安全最佳實務IAM。	2023 年 1 月 3 日
新增對 Amazon EC2置放群組的支援做為可共用的資源。	您現在可以與其他 共用 Amazon EC2置放群組 AWS 帳戶 ，以在其中啟動其執行個體。	2022 年 11 月 8 日
已新增兩個相關介紹影片的連結 AWS RAM。	新增了概觀影片，說明 AWS RAM 並逐步解說如何與其他 共用資源 AWS 帳戶。	2022 年 8 月 29 日
新增對 Amazon SageMaker AI 管道的支援。	您現在可以與其他 共用 SageMaker AI 管道 AWS 帳戶。	2022 年 8 月 2 日
新增對 AWS Service Catalog AppRegistry 應用程式和屬性群組的支援，做為可共用的資源類型。	您現在可以與其他 共用 AppRegistry 應用程式和屬性群組 AWS 帳戶。	2022 年 6 月 17 日

AWS Resource Access Manager 接收SOC和ISO認證。	AWS RAM 已驗證為符合 Service Organization Control (SOC) 和 International Organization for Standardization ISO (ISO) ISO 9001、27001、ISO27017、27018 ISO 和 ISO 27701 標準。	2022 年 5 月 31 日
AWS Resource Access Manager 會收到聯準會RAMP認證。	AWS RAM 已驗證為符合聯邦風險與授權管理計劃 (FedRAMP)。	2022 年 4 月 8 日
AWS Resource Access Manager 會收到PCIDSS憑證。	AWS RAM 已驗證為符合支付卡產業 (PCI) 資料安全標準 ()DSS。	2022 年 2 月 27 日
新增對 Amazon VPC IPAM 資源探索的支援做為可共用的資源。此外，您現在可以與組織外部的帳戶共用IPAM集區。	您現在可以與其他 共用IPAM資源探索 AWS 帳戶。	2022 年 1 月 25 日
新增共享全域資源的支援	您現在可以與其他 共用全域資源 AWS 帳戶。	2021 年 12 月 2 日
新增對 AWS 雲端WAN核心網路的支援做為可共用的全域資源。	您現在可以與其他 共用雲端WAN核心網路 AWS 帳戶。	2021 年 12 月 2 日
支援共用 Amazon VPC IP Address Manager (IPAM) 集區	您可以使用 AWS RAM 來共用 Amazon VPCIPAM集區。如需詳細資訊，請參閱AWS RAM《使用者指南》中的可分割 AWS 資源。	2021 年 12 月 1 日

支援共用 Amazon SageMaker AI 資源	您可以使用 AWS RAM 來共用 SageMaker AI 譜系群組。如需詳細資訊，請參閱AWS RAM《使用者指南》中的可 AWS 分割資源。	2021 年 11 月 30 日
支援共用 AWS Migration Hub Refactor Spaces 資源	您可以使用 AWS RAM 來共用 Migration Hub 環境。如需詳細資訊，請參閱AWS RAM《使用者指南》中的可 AWS 分割資源。	2021 年 11 月 29 日
新增受 AWS RAMAWS管IAM許可政策的相關資訊。	發佈了有關可用 AWS受管許可政策的詳細資訊，您可以在IAM主控台中存取這些政策，並將其連接到 中的IAM主體 AWS 帳戶。	2021 年 9 月 16 日
新增了共用 S3 on Outposts 資源的支援	您現在可以使用 AWS RAM 與其他 共用 S3 on Outposts AWS 帳戶。	2021 年 8 月 5 日
新增對其他受管許可和與IAM委託人共用資源的支援	對於支援的資源類型，您可以從其他 AWS RAM 受管許可中選擇，並與個別IAM角色和使用者共用資源。	2021 年 6 月 10 日
新增共享 AWS Systems Manager Incident Manager 資源的支援	您現在可以使用 AWS RAM 與其他 共用 AWS Systems Manager Incident Manager 聯絡人和回應計劃 AWS 帳戶。	2021 年 5 月 10 日
新增了共用 Amazon Route 53 資源的支援	您現在可以使用 與其他 AWS RAM 共用 Amazon Route 53 Resolver DNS Firewall 規則群組 AWS 帳戶。	2021 年 3 月 31 日

已新增共享 AWS Transit Gateway 資源的支援	您現在可以使用 AWS RAM 與其他 共用傳輸閘道多點傳送網域 AWS 帳戶。	2020 年 12 月 10 日
已新增共享 AWS Network Firewall 資源的支援	您現在可以使用 AWS RAM 與其他 共用 AWS Network Firewall 防火牆政策和規則群組 AWS 帳戶。	2020 年 11 月 17 日
新增對 Outpost 和本機閘道路由表共用的支援	您現在可以使用 AWS RAM 與其他 共用 Outpost 和本機閘道路由表 AWS 帳戶。	2020 年 10 月 15 日
新增共用 Route 53 查詢日誌的支援	您現在可以使用 與其他 AWS RAM 共用 Route 53 查詢日誌 AWS 帳戶。	2020 年 9 月 7 日
已新增共享 AWS Private Certificate Authority 資源的支援。	您現在可以使用 AWS RAM 與其他 共用 AWS 私有 CA 私有憑證授權單位 (CAs) AWS 帳戶。	2020 年 8 月 17 日
新增了共享 AWS Glue 資料目錄、資料庫和資料表的支援。	您現在可以使用 AWS 與其他 AWS RAM 共享 Glue 資料目錄、資料庫和資料表 AWS 帳戶。	2020 年 7 月 7 日
新增了共用 Amazon VPC字首清單的支援。	您現在可以使用 AWS RAM 來共用字首清單。	2020 年 6 月 29 日
新增了共用 AWS Outposts 客戶擁有IPv4地址的支援。	您現在可以使用 與其他 AWS RAM 共用 AWS Outposts 客戶擁有IPv4的地址 AWS 帳戶。	2020 年 4 月 22 日
新增了共用 AWS App Mesh 網格的支援	您現在可以使用 AWS RAM 與其他 共用網格 AWS 帳戶。	2020 年 1 月 17 日

新增了共享 AWS CodeBuild 專案和報告群組的支援	您現在可以使用 AWS RAM 與其他 共用 AWS CodeBuild 專案和報告群組 AWS 帳戶。	2019 年 12 月 13 日
新增了共用其他資源的支援	您現在可以使用 與其他 AWS RAM 共用 Amazon EC2 專用主機、 AWS Resource Groups 資源群組和 Amazon EC2 Image Builder 元件、映像和映像配方 AWS 帳戶。	2019 年 12 月 2 日
新增共享隨需容量預留的支援	您現在可以使用 與其他 AWS RAM 共用隨需容量預留 AWS 帳戶。	2019 年 7 月 29 日
新增共享 Aurora 資料庫叢集的支援	您現在可以使用 與其他 AWS RAM 共用 Aurora 資料庫叢集 AWS 帳戶。	2019 年 7 月 2 日
新增了共用流量鏡像目標的支援	您現在可以使用 與其他 AWS RAM 共用流量鏡像目標 AWS 帳戶。	2019 年 6 月 25 日
新增了共用授權組態的支援	您現在可以使用 AWS RAM 與其他 共用 AWS License Manager 授權組態 AWS 帳戶。	2018 年 12 月 5 日
新增了共用子網路的支援	您現在可以使用 與其他 AWS RAM 共用 Amazon VPC子網路 AWS 帳戶。	2018 年 11 月 27 日
新增了共用傳輸閘道的支援	您現在可以使用 與其他 AWS RAM 共用 Amazon VPC Transit 閘道 AWS 帳戶。	2018 年 11 月 26 日

新增了共享解析程式規則的支援	您現在可以使用 與其他 AWS RAM 共用 Route 53 Resolver 規則 AWS 帳戶。	2018 年 11 月 20 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。