使用者指南

AWS Resource Access Manager

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Resource Access Manager: 使用者指南

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Table of Contents

什麼是 AWS RAM？ 1
影片概觀 1
的優勢 AWS RAM 1
使用資源型政策進行跨帳戶存取會如何？ 2
資源共用的運作方式 2
共用您的 資源 3
使用共用資源 3
存取 AWS RAM 4
的定價 AWS RAM 5
合規和國際標準 5
PCI DSS 5
FedRAMP 5
SOC 和 ISO 5
開始使用 6
術語和概念 6
資源共享 6
共用帳戶 7
取用主體 7
以資源為基礎政策 8
受管許可 12
受管許可版本 13
共用您的 資源 13
在 中啟用資源共用 AWS Organizations 14
建立資源共用 15
使用共用資源 22
回應資源共享邀請 23
使用與您共用的資源 25
使用共用資源 26
區域和全球資源 26
區域資源和全球資源有何不同？ 27
資源共用及其區域 28
您擁有的資源 29
檢視您建立的資源共用 29
建立資源共享 31

更新資源共享 38
檢視您的共用資源 45
檢視您共用的主體 46
刪除資源共用 48
與您共用的資源 49
接受和拒絕邀請 50
檢視與您共用的資源共用 53
檢視與您共用的資源 55
檢視與您共用的委託人 56
離開資源共享 57
可用區域 ID 60
可共用的資源 63
AWS App Mesh 64
AWS AppSync GraphQL API 65
Amazon API Gateway 66
Amazon Application Recovery Controller (ARC) 66
Amazon Aurora 67
AWS Backup 68
Amazon Bedrock 68
AWS Billing 檢視服務 69
AWS CloudHSM 69
AWS CodeBuild 70
AWS CodeConnections 71
Amazon DataZone 72
Amazon EC2 72
EC2 Image Builder 75
Elastic Load Balancing 77
AWS End User Messaging SMS 77
Amazon FSx for OpenZFS 79
AWS Glue 80
AWS License Manager 82
AWS Marketplace 83
AWS Migration Hub Refactor Spaces 83
多方核准 84
AWS Network Firewall 85
AWS Outposts 86

Amazon S3 on Outposts ... 88
AWS Private Certificate Authority ... 88
AWS 資源總管 ... 89
AWS Resource Groups ... 90
Amazon Route 53 ... 91
Amazon Simple Storage Service ... 92
Amazon SageMaker AI ... 93
AWS Service Catalog AppRegistry ... 98
AWS Systems Manager Incident Manager ... 99
AWS Systems Manager ... 101
Amazon VPC ... 102
Amazon VPC Lattice ... 108
AWS 雲端 WAN ... 110
在 中管理許可 AWS RAM ... 112
檢視受管許可 ... 113
建立和使用客戶受管許可 ... 117
建立客戶受管許可 ... 117
建立新的客戶受管許可版本 ... 119
選擇不同的版本做為客戶受管許可的預設值 ... 120
刪除客戶受管許可版本 ... 122
刪除客戶受管許可 ... 123
更新受管許可版本 ... 124
客戶受管許可考量 ... 126
受管許可的運作方式 ... 127
受管許可的類型 ... 128
安全 ... 130
資料保護 ... 130
身分與存取管理 ... 131
AWS RAM 如何使用 IAM ... 132
AWS 受管政策 ... 134
使用服務連結角色 ... 139
範例 IAM 政策 ... 140
SCP 範例 ... 143
停用與 Organizations 的共用 ... 147
日誌記錄和監控 ... 147
使用 EventBridge 監控 ... 148

使用 記錄 AWS RAM API 呼叫 AWS CloudTrail 149
恢復能力 152
基礎架構安全 152
AWS PrivateLink 152
考量事項 153
建立介面端點 153
建立端點政策 153
故障診斷 155
錯誤：帳戶 ID 不存在 155
案例 155
原因 155
解決方案 155
錯誤：存取遭拒的例外狀況 156
案例 156
原因 156
解決方案 156
錯誤：不明的資源例外狀況 158
案例 158
原因 158
解決方案 158
錯誤：不允許在組織外部共用 159
案例 159
可能的原因和解決方案 159
錯誤：看不到共用資源 160
案例 160
可能的原因和解決方案 160
錯誤：限制超過例外狀況 162
案例 162
原因 162
解決方案 162
未收到邀請 162
案例 162
原因 162
無法共用 VPC 163
案例 163
原因 163

Service Quotas 164
使用 AWS SDKs 166
文件歷史紀錄 167
..... clxxvi

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 (OUs) 之間 AWS 帳戶，以及支援資源類型的 AWS Identity and Access Management (IAM) 角色和使用者之間安全地共用資源。如果您有多個 AWS 帳戶，您可以建立資源一次，並使用 AWS RAM 讓其他帳戶使用該資源。如果您的帳戶由 管理 AWS Organizations，您可以與組織中的所有其他帳戶共用資源，或僅與一或多個指定組織單位 (OUs包含的帳戶共用資源。您也可以 AWS 帳戶 依帳戶 ID 與特定 共用，無論帳戶是否為組織的一部分。某些支援的資源類型也可讓您與指定的 IAM 角色和使用者共用它們。

目錄

- 影片概觀
- 的優勢 AWS RAM
- 資源共用的運作方式
- 存取 AWS RAM
- 的定價 AWS RAM
- 合規和國際標準

影片概觀

下列影片提供 的簡介 AWS RAM ，並說明如何建立資源共享。如需詳細資訊，請參閱???。

下列影片示範如何將 AWS 受管許可套用至您的 AWS 資源。如需詳細資訊，請參閱???。

此影片示範如何根據最低權限的最佳實務，撰寫和建立客戶受管許可的關聯。如需詳細資訊，請參閱???。

的優勢 AWS RAM

為什麼要使用 AWS RAM？ 它提供下列優點：

- 降低您的營運開銷 – 建立資源一次，然後使用 AWS RAM 與其他帳戶共用該資源。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 資源的帳戶中， 可 AWS RAM 簡化授予該帳戶中每個角色和使用者的存取權，而不必使用身分型許可政策。

- 提供安全性和一致性 – 使用一組政策和許可，簡化共用資源的安全管理。如果您改為在所有不同的帳戶中建立重複的資源，您將有實作相同政策和許可的任務，然後必須在所有這些帳戶中保持相同。相反地， AWS RAM 資源共享的所有使用者都由一組政策和許可管理。 AWS RAM 提供一致的體驗，以共享不同類型的 AWS 資源。
- 提供可見性和可稽核性 – 透過 AWS RAM 與 Amazon CloudWatch 和 的整合來檢視共用資源的使用詳細資訊 AWS CloudTrail。 AWS RAM 提供共用資源和帳戶的全面可見性。

使用資源型政策進行跨帳戶存取會如何？

您可以透過在 外部 AWS 帳戶 連接識別 AWS Identity and Access Management (IAM) 委託人 AWS (IAM 角色和使用者） 的資源型政策，與其他 共用某些類型的資源 AWS 帳戶。不過，透過連接政策來共用資源並不會利用 AWS RAM 提供的額外好處。透過使用 AWS RAM ，您可獲得下列功能：

- 您可以與組織或組織單位 (OU) 共用，而不必列舉每個 AWS 帳戶 IDs。
- 使用者可以在原始 AWS 服務 主控台和 API 操作中直接看到與其共用的資源，就像這些資源直接在使用者帳戶中一樣。例如，如果您使用 與其他帳戶 AWS RAM 共用 Amazon VPC 子網路，則該帳戶中的使用者可以在 Amazon VPC 主控台中查看子網路，並在該帳戶中執行的 Amazon VPC API 操作結果中查看子網路。透過連接以資源為基礎的政策所共享的資源不會以這種方式顯示；反之，您必須依其 Amazon Resource Name (ARN) 探索並明確參考資源。
- 資源的擁有者可以查看哪些主體可以存取他們共用的每個個別資源。
- 如果您與不屬於您組織的 帳戶共用資源，則 會 AWS RAM 啟動邀請程序。收件人必須先接受邀請，該主體才能存取共用資源。在您開啟在組織內共用的功能之後，與組織中的帳戶共用不需要邀請。

如果您有使用以資源為基礎的許可政策來共用的資源，您可以執行下列任一動作，將這些資源提升為完全 AWS RAM 受管的資源：

- 使用 PromoteResourceShareCreatedFromPolicy API 操作。
- 使用 API 操作的同等項目，即 AWS Command Line Interface (AWS CLI) promote-resource-share-created-from-policy命令。

資源共用的運作方式

當您在擁有帳戶中與另一個耗 AWS 帳戶用帳戶共用資源時，您會將耗用帳戶中的主體存取權授予共用資源。套用至耗用帳戶中角色和使用者的任何政策和許可，也適用於共用資源。共用中的資源看起來像是 AWS 帳戶 您共用資源的 中的原生資源。

您可以共用全域和區域資源。如需詳細資訊，請參閱與全域資源相比，共用區域資源。

共用您的 資源

您可以使用 AWS RAM建立資源共享，以共享您擁有的資源。若要建立資源共享，請指定下列項目：

- 您要在 AWS 區域 其中建立資源共用的 。在 主控台中，您可以從主控台右上角的區域下拉式功能表中進行選擇。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同 AWS 區域 之區域資源。
  - 只有在資源共用位於指定之 全球資源主區域，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`。
- 資源共用的名稱。
- 您想要在此資源共享中授予存取權的資源清單。
- 您授予資源共享存取權的主體。委託人可以是個人 AWS 帳戶、組織中的帳戶或 中的組織單位 (OU) AWS Organizations，或個人 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。

- 與您在資源共享中包含的每個資源類型建立關聯的受管許可。受管許可決定其他帳戶中的主體可以對資源共享中的資源執行哪些操作。

  許可的行為取決於委託人類型：

  - 如果主體位於與擁有資源的主體不同的帳戶中，則附加到資源共享的許可是授予這些帳戶中角色和使用者的最大許可。然後，這些帳戶的管理員必須透過 IAM 身分型政策授予個別角色和使用者對共用資源的存取權。這些政策中授予的許可不能超過附加至資源共享之許可中定義的許可。

擁有帳戶的資源會保留其共用資源的完整所有權。

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，就像您的帳戶擁有該資源一樣。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。您帳戶中的主體可執行的 API 操作會因資源類型而異，並且由 AWS RAM 附加至資源共享的許可指定。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，這可讓您在安全和控管控制中利用現有的投資。

當您使用該資源的服務存取共用資源時，您具有與擁有該資源 AWS 帳戶 的 相同的功能和限制。

- 如果資源是區域性資源，則您只能從其存在於擁有帳戶中的 AWS 區域 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 存取它。您只能在指定的主區域美國東部（維吉尼亞北部）中檢視和管理 AWS RAM 主控台和工具中的資源共享及其全域資源。 `us-east-1`

存取 AWS RAM

您可以透過下列 AWS RAM 任何方式使用 ：

AWS RAM 主控台

AWS RAM 提供以 Web 為基礎的使用者介面 AWS RAM 主控台。如果您已註冊 AWS 帳戶，您可以登入 AWS Management Console 並從 AWS RAM 主控台首頁選擇 AWS RAM 來存取 主控台。

您也可以在瀏覽器中直接導覽至AWS RAM 主控台。如果您尚未登入，則在主控台出現之前，系統會要求您這麼做。

AWS CLI 和 Tools for Windows PowerShell

AWS CLI 和 AWS Tools for PowerShell 可直接存取 AWS RAM 公有 API 操作。 AWS 支援 Windows、 macOS和 上的這些工具Linux。如需入門的詳細資訊，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AWS CLI 命令參考或 AWS Tools for Windows PowerShell Cmdlet 參考。

AWS SDKs

AWS 為廣泛的程式設計語言提供 API 命令。如需入門的詳細資訊，請參閱AWS SDKs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。使用 AWS RAM API，您可以直接向 服務發出 HTTPS 請求。使用 AWS RAM API 時，您必須包含程式碼，才能使用您的憑證以數位方式簽署請求。如需詳細資訊，請參閱 AWS RAM API 參考。

的定價 AWS RAM

使用 AWS RAM 或 建立資源共用和跨帳戶共用資源，無需額外費用。資源用量會隨資源類型而異。如需如何 AWS 計費可共用資源的詳細資訊，請參閱資源擁有服務的文件。

合規和國際標準

PCI DSS

AWS RAM 支援由商家或服務供應商處理、儲存和傳輸信用卡資料，並已驗證為符合支付卡產業 (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 在下列內容中授權為 FedRAMP Moderate AWS 區域：美國東部（維吉尼亞北部）、美國東部（俄亥俄）、美國西部（加利佛尼亞北部）和美國西部（奧勒岡）。

AWS RAM 在下列 中授權為 FedRAMP High 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 合規的詳細資訊，請參閱 FedRAMP。

SOC 和 ISO

AWS RAM 可用於受 Service Organization Control (SOC) 合規和國際標準化組織 (ISO) ISO 9001、ISO 27001、ISO 27017、ISO 27018 和 ISO 27701 標準的工作負載。財務、醫療保健和其他受監管產業的客戶可以深入了解保護客戶資料的安全程序和控制，這些資料可在 的 SOC 報告和 AWS ISO 和 CSA STAR 憑證中找到AWS Artifact。

如需 SOC 合規的詳細資訊，請參閱 SOC。

如需 ISO 合規的詳細資訊，請參閱 ISO 9001、ISO 27001、ISO 27017、ISO 27018 和 ISO 27701。

入門 AWS RAM

您可以使用 AWS Resource Access Manager與其他個人共用您擁有的資源 AWS 帳戶。如果您的帳戶是由 管理 AWS Organizations，您也可以與組織中的其他帳戶共用資源。您也可以使用其他 與您共用的資源 AWS 帳戶。

如果您未啟用內部共用 AWS Organizations，則無法與組織或組織中的組織單位 (OU) 共用資源。不過，您仍然可以與 AWS 帳戶 組織中的個人共用資源。對於支援的資源類型，您也可以與組織中的個別 AWS Identity and Access Management (IAM) 角色或使用者共用資源。在這種情況下，這些委託人會被視為外部帳戶，而不是組織的一部分。他們會收到加入資源共用的邀請，而且必須接受邀請才能存取共用資源。

目錄

- 的術語和概念 AWS RAM
- 共用您的 AWS 資源
- 使用共用 AWS 資源

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。資源共享具有下列三個元素：

- 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。
- 您在共用中包含之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 建立資源共享之後，資源共享中指定的主體可以獲得共享資源的存取權。

- 如果您開啟與 AWS RAM 共用 AWS Organizations，且與 共用的主體位於共用帳戶相同的組織中，則只要這些主體的帳戶管理員授予他們使用 資源的許可，即可取得存取權 AWS Identity and Access Management 。

- 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，他們必須先接受邀請，才能讓資源共享中指定的主體存取共用資源。
- 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，他們必須先接受邀請，才能讓資源共享中指定的主體存取共用資源。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，而 AWS RAM 管理員會在其中使用 建立 AWS 資源共用 AWS RAM。

AWS RAM 管理員是具有在 中建立和設定資源共用許可的 IAM 主體 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享中的資源， AWS RAM 管理員也必須具有許可，才能 AWS 服務 針對資源共享中包含的每個資源類型，在 中呼叫 `PutResourcePolicy`操作。

取用主體

耗用帳戶是共用資源 AWS 帳戶 的 。資源共用可以將整個帳戶指定為主體，或指定為帳戶中的某些資源類型、個別角色或使用者。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享的取用者。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。這些指定可授予耗用帳戶中主體的最大許可。
- IAM 身分型政策由耗用帳戶中的 IAM 管理員連接到個別角色或使用者。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 ARN 指定此委託人類型。
  - 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`

  為了降低代理人混淆的風險，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的 OU IDs 共用。依組織或 OU 的 ARN 在組織中指定帳戶。

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

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

  - 組織單位中的所有帳戶 – 以下是 OU ID 的範例 ARN：

    ```
    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都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 連接至共用中每個資源的資源型政策使用 `"Principal": "*"`。如需詳細資訊，請參閱在資源型政策"Principal": "*"中使用 的含意。
> 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。這些政策必須授予對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。

以資源為基礎政策

資源型政策是實作 IAM 政策語言的 JSON 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，您會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 IAM 身分型政策，以及 AWS Organizations 可能適用於 的服務控制政策 (SCPs) AWS 帳戶。所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 透過提供easy-to-use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，請考慮您使用共用的 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享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，僅將 SageMaker AI 執行許可授予單一帳戶。 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。您可以透過呼叫 GetResourcePolicy操作來檢視此基礎資源政策。 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，如果您與另一個帳戶共用 AWS CodeBuild 專案，耗用帳戶中的使用者可以在 CodeBuild 主控台和執行的 CodeBuild API 操作結果中查看專案。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，您必須探索並明確地參考其 ARN 的資源。
- 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 API 中檢查個別資源的政策，才能查看耗用帳戶。
- 效率 – 如果您使用 共用資源 AWS RAM，則可以共用多個資源，並以一個單位管理它們。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 ready-to-use AWS 受管許可，您可以從中選擇連接到資源共用。

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 – 客戶擁有的 IPv4 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 Image Builder 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 中的 IAM 角色或使用者共用 EC2 Image Builder 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 Image Builder 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"`元素來限制與指定 相符的身分的許可`PrincipalOrgID`。如需詳細資訊，請參閱在資源型政策"Principal": "*"中使用 的含意。

```
{
    "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"
                }
            }
        }
    ]
}
```

在資源型政策"Principal": "*"中使用 的含意

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被此類資源型政策授予存取 動作的委託人。

如果您的案例不想要此行為，則可以將明確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，來限制此行為。

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個受管許可。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。

您只能為資源共享中的每個資源類型連接一個受管許可。您無法建立資源共享，其中特定類型的部分資源使用一個受管許可，而相同類型的其他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享，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 受管許可由 建立和維護 AWS ，並授予常見客戶案例的許可。 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 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，僅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。客戶受管許可為區域特定。

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。所有新的資源共享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。此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 受管許可更新至較新版本。

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 外部的委託人共用資源，並不會變更套用至建立資源之帳戶中資源的許可或配額。
> - AWS RAM 是區域性服務。您共用的委託人只能在建立資源的 AWS 區域 中存取資源共用。
> - 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，使用者都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。組織中的委託人可以存取共用資源，而無需交換邀請。

當您在組織內啟用資源共用時， 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`。

> **Note**
>
> AWS Organizations 啟用與 共用時，組織內的任何資源共用僅限於同一組織內的消費者。這表示如果消費者離開組織，他們將無法存取資源共享中的資源。當資源與 OU、整個組織或組織中的個別帳戶共用時，這是如此。

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

最低許可

若要執行下列程序，您必須以具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 來啟用 的受信任存取，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

在您的組織內啟用資源共用

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

在您的組織內啟用資源共用

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 會建立受管許可 AWS ，以涵蓋標準使用案例。
   - 客戶受管許可可讓您量身打造自己的受管許可，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. 指定您想要存取資源的主體。

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）中檢視這類資源共用及其全域資源和工具。 `us-east-1`如需 AWS RAM 和 全域資源的詳細資訊，請參閱 與全域資源相比，共用區域資源。
- 如果您共用的 帳戶是 中組織的一部分， AWS Organizations 且已啟用組織內的共用，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。您在組織內容之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的 IAM 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無法存取透過該資源共用存取的資源。

> **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都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，請參閱在資源型政策"Principal": "*"中使用 的含意。
> 其他取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 ARNsAllow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和該組織的 OUs 新增至資源共享。您無法將來自自己組織外部OUs 或組織以主體身分新增至資源共享。不過，您可以新增個別 ， AWS 帳戶 或針對支援的服務，將來自組織外部的 IAM 角色和使用者新增為資源共用的主體。

> **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享。如果您在邀請過期之前不接受邀請，則會自動拒絕邀請。

> **Important**
>
> 對於不在下列清單上的共用資源類型，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 – 客戶擁有的 IPv4 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

建立資源共享

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，您必須將 AWS 區域 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 與全域資源相比，共用區域資源。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. 在名稱中，輸入資源共享的描述性名稱。
   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，選取您要共用之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 IDs 。
   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，請參閱受管許可的類型。

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。如需更多資訊，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. 選擇下一步。
8. 在步驟 3：授予主體存取權中，執行下列動作：

   a. 根據預設，會選取允許與任何人共用，這表示對於支援它的資源類型，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您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) AWS 帳戶 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都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，請參閱在資源型政策"Principal": "*"中使用 的含意。
> 其他取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

ARNsAllow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 OUs AWS 帳戶 中的所有主體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 ARN 指定委託人，包括組織外部的委託人，請為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，請輸入角色的 ARN。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 角色的唯一 ARN，請在 IAM 主控台中檢視角色清單、使用 get-role AWS CLI 命令或 GetRole API 動作。

- IAM 使用者 – 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 IAM 使用者的唯一 ARN，請在 IAM 主控台中檢視使用者清單、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，請選擇對應至您要返回之步驟的連結，並進行必要的變更。
11. 檢閱完資源共享後，選擇建立資源共享。

    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。您可以針對支援超過預設受管許可的類型，變更資源共用中包含之資源類型的受管許可。當您不想再共用資源時，可以刪除資源共用。如需詳細資訊，請參閱共用您擁有 AWS 的資源。

AWS CLI

建立資源共享

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**
>
> 如果您想要在此資源共享中使用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。記下客戶受管許可的 ARN，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

若要開始使用與您的帳戶共用的資源 AWS Resource Access Manager，請完成下列任務。

任務

- 回應資源共享邀請
- 使用與您共用的資源

回應資源共享邀請

如果您收到加入資源共享的邀請，您必須接受該邀請才能存取共用資源。

邀請不會用於下列案例：

- 如果您是 中組織的一部分， AWS Organizations 並在組織中共用已啟用，則組織中的主體會自動存取共用資源，而無需邀請。
- 如果您與 AWS 帳戶 擁有該資源的 共用，則該帳戶中的主體會自動存取共用資源，而無需邀請。

Console

回應邀請

1. 在 主控台中 AWS RAM 開啟與我共用 ： 資源共用頁面。

   > **Note**
   >
   > 只有建立資源共享 AWS 區域 的 中才會顯示該資源共享。如果預期資源共享未出現在主控台中，您可能需要 AWS 區域 使用右上角的下拉式清單控制項切換到不同的資源共享。

2. 檢閱已授予您存取權的資源共用清單。

   狀態欄指出資源共享的目前參與狀態。`Pending` 狀態表示您已新增至資源共享，但您尚未接受或拒絕邀請。

3. 若要回應資源共享邀請，請選取資源共享 ID，然後選擇接受資源共享以接受邀請，或拒絕資源共享以拒絕邀請。如果您拒絕邀請，您將無法存取 資源。如果您接受邀請，即可存取 資源。

AWS CLI

若要開始，請取得可供您使用的資源共享邀請清單。下列範例命令已在 `us-west-2` 區域中執行，並顯示 `PENDING` 狀態中有一個可用的資源共享。

```
$ 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"
        }
    ]
}
```

您可以使用上一個命令邀請的 Amazon Resource Name (ARN) 做為下一個命令中的參數，以接受該邀請。

```
$ 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`。包含在該資源共享中的資源現在可供接受帳戶中的主體使用。

使用與您共用的資源

接受加入資源共享的邀請後，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 操作中使用。如果資源是區域性資源，則必須在服務主控台或 API/CLI 命令 AWS 區域 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`若要在 中檢視資源 AWS RAM，您必須開啟 AWS RAM 主控台，使其成為建立資源共用 AWS 區域 的 。

使用共用 AWS 資源

您可以使用 AWS Resource Access Manager (AWS RAM) 來共用您擁有 AWS 的資源，並存取 AWS 與您共用的資源。

內容

- 與全域資源相比，共用區域資源
  - 區域資源和全球資源有何不同？
  - 資源共用及其區域
- 共用您擁有 AWS 的資源
  - 檢視您在 中建立的資源共用 AWS RAM
  - 在 中建立資源共享 AWS RAM
  - 在 中更新資源共用 AWS RAM
  - 在 中檢視您的共用資源 AWS RAM
  - 檢視您在 中與 共用資源的主體 AWS RAM
  - 在 中刪除資源共享 AWS RAM
- 存取與您共用 AWS 的資源
  - 接受和拒絕資源共用邀請
  - 檢視與您共用的資源共用
  - 檢視與您共用的資源
  - 檢視與您共用的委託人
  - 離開資源共享
    - 離開資源共用的先決條件
    - 如何保留資源共享
- AWS 資源的可用區域 IDs

與全域資源相比，共用區域資源

本主題討論 AWS Resource Access Manager (AWS RAM) 如何與區域和全球資源搭配使用的差異。

資源可以是區域或全域。您可以使用 Amazon Resource Name (ARN) 中的第四個欄位來識別資源是區域性還是全域。區域資源會顯示 AWS 區域。如果為空白，則資源為全域。

區域資源和全球資源有何不同？

區域資源

您可以共用的大多數資源 AWS RAM 都是區域性資源。您在指定的 AWS 區域中建立區域資源後，這些資源就會存在於該區域中。若要查看這些資源或與其互動，您必須將操作導向至該區域。例如，若要使用 建立 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體 AWS Management Console，您可以選擇要在 AWS 區域其中建立執行個體的 。如果您使用 AWS Command Line Interface (AWS CLI) 來建立執行個體，則會包含 `--region` 參數。每個 AWS SDKs 都有自己的同等機制，以指定操作使用的 區域。

使用區域資源的原因有幾個。其中一個好原因就是確保資源和您用來存取資源的服務端點盡可能接近客戶。這可將延遲降至最低來提高效能。另一個原因是要提供隔離界限。這可讓您在多個區域中建立獨立的資源副本，以分發負載並改善可擴展性。同時，其可將資源彼此隔離以提高可用性。

如果您在 AWS 區域 主控台或 AWS CLI 命令中指定不同的 ，則您無法再看到或與上一個區域中可以看到的資源互動。

當您查看區域資源的《Amazon Resource Name (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 執行個體是區域資源。這類資源的 ARNs 看起來與 `us-east-1`區域中存在的 VPC 的下列範例類似。

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

全域資源

有些 AWS 服務支援您可以全域存取的資源，這表示您可以從任何地方使用該資源。您不會在全域服務的主控台 AWS 區域 中指定 。若要存取全域資源，使用 服務和 AWS CLI SDK AWS 操作時，您不會指定 `--region` 參數。

全域資源支援一次只能存在一個特定資源執行個體至關重要的情況。在這種情況下，不同區域中複本之間的複寫或同步還不夠。必須存取單一全域端點 (但可能會增加延遲) 是可接受的考量，以確保資源的消費者可立即看到任何變更。例如，當您建立 AWS Cloud WAN 核心網路做為全域資源時，它與所有使用者一致。它顯示為跨所有區域的單一連續全球網路。

全域資源的《Amazon Resource Name (ARN)》不包含區域。這類 ARN 的第四個欄位是空的，例如下列適用於 Cloud WAN 核心網路的範例 ARN。

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

資源共用及其區域

AWS RAM 是區域性服務，資源共享是區域性服務。因此，資源共享可以包含與資源共享 AWS 區域相同的資源，以及任何支援的全域資源。您建立資源共享的區域是資源共享的主區域。

> **Important**
>
> 目前，您只能在指定的主區域美國東部（維吉尼亞北部）區域 中建立與全球資源的資源共享。 `us-east-1`雖然您只能在該單一主區域中建立資源共用，但當在該服務的主控台或 CLI 和 SDK 操作中檢視時，任何共用的全域資源都會顯示為標準全域資源。主區域的限制僅適用於資源共享，而不是其中包含的資源。

若要共用您在 `us-west-2`區域中建立的區域資源，您必須設定 AWS RAM 主控台來使用 ，`us-west-2`並在其中建立資源共用。您無法建立包含不同 區域資源的資源共享 AWS 區域。這表示若要從 `us-west-2`和 共用資源`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享。

若要在 AWS RAM 主控台中共用全域資源，您必須設定 AWS RAM 主控台以使用指定的主區域：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享。您只能將資源共享中的全域資源與`us-east-1`區域的資源混合。

即使全域資源只能檢視指定主區域中 AWS RAM 的資源共用中，但在您共用後仍然是全域資源。您可以從原始 中可存取它的任何區域， AWS 帳戶 在共用的 中存取它 AWS 帳戶。

考量事項

- 若要在 AWS RAM 主控台中建立資源共享，您必須使用包含您要共享之資源的區域。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享，您必須使用包含資源共享的區域。同樣地， AWS RAM AWS CLI 和 SDK 操作可讓您僅與您在操作中指定的區域中的資源共用互動。若要檢視或修改包含全球資源的資源共享，您必須使用指定的主區域，美國東部（維吉尼亞北部），`us-east-1`。
- 若要在 AWS RAM 主控台中檢視區域資源以將其包含在資源共享中，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包含在資源共享中，您必須使用指定的主區域：美國東部（維吉尼亞北部）`us-east-1`。

- 您只能在指定的主區域美國東部（維吉尼亞北部）中，使用區域和全球資源建立資源共享。 `us-east-1`

共用您擁有 AWS 的資源

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

主題

- 檢視您在 中建立的資源共用 AWS RAM
- 在 中建立資源共享 AWS RAM
- 在 中更新資源共用 AWS RAM
- 在 中檢視您的共用資源 AWS RAM
- 檢視您在 中與 共用資源的主體 AWS RAM
- 在 中刪除資源共享 AWS RAM

檢視您在 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。您可以查看您要共用的資源，以及與其共用的主體。

Console

檢視您的資源共用

1. 在 主控台中 AWS RAM 開啟由我共用 ： 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享，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，請參閱與全域資源相比，共用區域資源。
3. 如果資源共用在結果中使用的任何受管許可具有指定為預設值的受管許可新版本，則頁面會顯示橫幅來提醒您。您可以選擇在頁面頂端檢閱並更新所有 ，以選擇一次更新所有受管許可版本。

   或者，對於具有一或多個新受管許可版本的個別資源共用，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許可版本，並讓您將它們指派為該資源共享中相關資源類型的版本。

4. （選用）套用篩選條件以尋找特定資源共享。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的屬性欄位下拉式清單。選擇一個之後，您可以從該欄位的可用值清單中選擇。您可以新增其他屬性或關鍵字，直到您找到所需的資源為止。
5. 選擇要檢閱的資源共用名稱。主控台會顯示資源共用的下列資訊：
   - 摘要 – 列出資源共用名稱、ID、擁有者、Amazon Resource Name (ARN)、建立日期、是否允許與外部帳戶共用，以及其目前狀態。
   - 受管許可 – 列出連接到此資源共享的受管許可。資源共用中包含的每個資源類型最多可以有一個受管許可。每個受管許可會顯示與資源共用相關聯的受管許可版本。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，則您有機會更新資源共享以使用預設版本。
   - 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，在原生服務的主控台中檢視資源。
   - 共用主體 – 列出與之共用資源的主體。
   - 標籤 – 列出連接至資源共用本身的標籤鍵值對；這些不是連接至資源共用中包含之個別資源的標籤。

AWS CLI

檢視您的資源共用

您可以使用 get-resource-shares 命令，並將 參數`--resource-owner`設定為 `SELF`，以顯示在 中建立之資源共享的詳細資訊 AWS 帳戶。

下列範例顯示在目前 AWS 區域 (`us-east-1`) 中針對呼叫共用的資源共用 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享，您必須指定美國東部（維吉尼亞北部）`us-east-1`區域。

```
$  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），在主控台和工具中檢視此類資源共享及其全域資源。 `us-east-1`如需 AWS RAM 和 全域資源的詳細資訊，請參閱 與全域資源相比，共用區域資源。
- 如果您共用的 帳戶是 中組織的一部分， AWS Organizations 且已啟用組織內的共用，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。您在組織內容之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，而且只有在他們接受邀請之後，才會被授予共用資源的存取權。
- 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的 IAM 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都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 連接至共用中每個資源的資源型政策使用 `"Principal": "*"`。如需詳細資訊，請參閱在資源型政策"Principal": "*"中使用 的含意。
> 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。這些政策必須授予對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。

- 您只能將帳戶所屬的組織和該組織的 OUs 新增至資源共享。您無法將來自自己組織外部OUs 或組織新增至資源共享，做為主體。不過，您可以新增個別 ， AWS 帳戶 或針對支援的服務，將 IAM 角色和組織外部的使用者新增為資源共用的主體。

> **Note**
>
> 並非所有資源類型都可與 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享。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 – 客戶擁有的 IPv4 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

建立資源共享

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享，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，請參閱與全域資源相

比，共用區域資源。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，請從我的共用：資源共用頁面選擇建立資源共用。 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享的資源，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中的相對位置。如需詳細資訊，請參閱AWS 資源的可用區域 IDs 。
   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，請參閱受管許可的類型。

   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：授予主體存取權中，執行下列動作：

   a. 根據預設，會選取允許與任何人共用，這表示對於支援它的那些資源類型，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都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 連接至共用中每個資源的資源型政策使用 `"Principal": "*"`。如需詳細資訊，請參閱在資源型政策"Principal": "*"中使用 的含意。
        > 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。這些政策必須授予對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 OUs AWS 帳戶 中的所有主體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 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輸入 ID 或 ARN。

- 若要依 ID 或 ARN 指定委託人，包括組織外的委託人，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。可用的委託人類型和 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
    ```

  - Organization – 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，請輸入角色的 ARN。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 角色的唯一 ARN，請在 IAM 主控台中檢視角色清單、使用 get-role AWS CLI 命令或 GetRole API 動作。

  - IAM 使用者 – 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 IAM 使用者的唯一 ARN，請在 IAM 主控台中檢視使用者清單、使用 get-user AWS CLI 命令或 GetUser API 動作。

- 服務主體 – 若要新增服務主體，請從選取主體類型下拉式清單中選擇服務主體。 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，請選擇對應至您要返回之步驟的連結，並進行必要的變更。
11. 檢閱完資源共享後，請選擇建立資源共享。

    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，請參閱共用您擁有 AWS 的資源。

AWS CLI

建立資源共享

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**
>
> 如果您想要在此資源共享中使用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。記下客戶受管許可的 ARN，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享。
- 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權。如果您撤銷存取權，主體就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留下資源共用。如果資源共用包含不支援離開的資源類型，則會顯示訊息，通知主體他們必須聯絡共用擁有者。在此情況下，身為資源共享擁有者的您必須從資源共享中移除主體。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

更新資源共享

1. 導覽至 主控台中的 AWS RAM 「由我共用」：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 。若要查看包含全球資源的資源共享，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，請參閱與全域資源相比，共用區域資源。
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，請在選取的資源下找到資源，然後選擇資源 ID 旁的 X。
   d. （選用）若要將標籤新增至資源共享，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，請參閱受管許可的類型。

   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。完成此程序後，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**
>
> 在最終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的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委託人 AWS Organizations，請選擇僅允許與組織中的委託人共用。

   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都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 連接至共用中每個資源的資源型政策使用 `"Principal": "*"`。如需詳細資訊，請參閱在資源型政策"Principal": "*"中使用 的含意。
>
> 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。這些政策必須授予對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 已啟用與 共享，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 IAM 角色或使用者。反之，您必須輸入這些主體的識別符來新增這些主體，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，然後輸入主體的 ID 或 ARN。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）– 讓其他 帳戶可使用資源。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享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享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，檢閱資源共享的組態詳細資訊。
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，藉此有另一個解決的機會。
13. 當您完成變更時，請選擇更新資源共享。

AWS CLI

更新資源共享

您可以使用下列 AWS CLI 命令來修改資源共享：

- 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 AWS 區域 包含資源共享的 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享，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。您可以在資源共用中為每個資源類型指派一個受管許可。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 Amazon Elastic Compute Cloud (Amazon EC2) 子網路可用的受管許可 ARNs，然後使用其中一個 ARNs 來取代指定資源共享中該資源類型目前指派的 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指定 ARN 的 Amazon 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具有 金鑰的標籤。

```
$ 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。

在 中檢視您的共用資源 AWS RAM

您可以檢視您已在所有資源共用中共用的個別資源清單。此清單可協助您判斷目前共用的資源、資源共用的數目，以及可存取這些資源的主體數目。

Console

檢視您目前正在共用的資源

1. 在 主控台中開啟由我共用 ： 共用資源頁面。 AWS RAM
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享，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，請參閱與全域資源相比，共用區域資源。
3. 針對每項共用的資源，下列資訊可供使用：
   - 資源 ID – 資源的 ID。選擇資源的 ID 以開啟新的瀏覽器索引標籤，在原生服務主控台中檢視資源。
   - 資源類型 – 資源的類型。
   - 上次共用日期 – 資源上次共用的日期。
   - 資源共用 – 包含資源的資源共用數目。若要查看資源共用的清單，請選擇號碼。
   - 主體 – 可存取資源的主體數量。選擇值以檢視主體。

AWS CLI

檢視您目前正在共用的資源

您可以使用 list-resources 命令，並將 參數`--resource-owner`設定為 `SELF`，以顯示您目前共用資源的詳細資訊。

下列範例顯示 AWS 區域 (`us-east-1`) 中包含於資源共用中的資源，用於呼叫 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 中與 共用資源的主體 AWS RAM

您可以檢視所有資源共用中與之共用資源的主體。檢視此委託人清單可協助您判斷誰可以存取您的共用資源。

Console

檢視您要與 共用資源的主體

1. 導覽至 主控台中的 AWS RAM 共用：主體頁面。
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享，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，請參閱與全域資源相比，共用區域資源。
3. 套用篩選條件以尋找特定主體。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的屬性欄位下拉式清單。選擇一個之後，您可以從該欄位的可用值清單中選擇。您可以新增其他屬性或關鍵字，直到您找到所需的資源為止。
4. 對於清單中的每個主體，主控台會顯示下列資訊：
    - 主體 ID – 主體的 ID。選擇 ID 以開啟新的瀏覽器索引標籤，在原生主控台中檢視主體。

- 資源共用 – 您與指定委託人共用的資源共用數目。選擇號碼以檢視資源共享清單。
- 資源 – 您與委託人共用的資源數量。選擇號碼以檢視共用資源的清單。

AWS CLI

檢視您要與 共用資源的主體

您可以使用 list-principals 命令來取得您在目前 AWS 區域 為呼叫帳戶建立的資源共用中參考的委託人清單。

下列範例列出有權存取在預設區域中為呼叫帳戶建立的共用的委託人。在此範例中，委託人是呼叫帳戶的組織，並且是獨立的 AWS 帳戶，作為兩個不同資源共享的一部分。您必須針對 AWS 區域 包含資源共享的 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
        }
    ]
}
```

在 中刪除資源共享 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體都會失去共用資源的存取權。刪除資源共用不會刪除共用的資源。

> **刪除 AWS 資源**
>
> 如果您需要刪除包含在資源共用中的 AWS 資源， AWS 建議您先確定從包含資源共用中移除資源，或刪除資源共用。

刪除的資源共享在刪除後會在 AWS RAM 主控台中短暫顯示，但其狀態會變更為 `Deleted`。

Console

刪除資源共用

1. 在 主控台中 AWS RAM 開啟由我共用 ： 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享，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，請參閱與全域資源相比，共用區域資源。
3. 選取您要刪除的資源共用。

   > **Warning**
   >
   > 請務必選取正確的資源共享。刪除資源共享後，您無法復原該資源共享。

4. 選擇刪除，然後在確認訊息中，選擇刪除。
5. 刪除的資源共享會在兩小時後消失。在此之前，它會在主控台中保持可見狀態為已刪除。

AWS CLI

刪除資源共用

您可以使用 delete-resource-share 命令來刪除不再需要的資源共用。

下列範例會先使用 get-resource-shares 命令來取得您要刪除之資源共享的 Amazon Resource Name (ARN)。然後，它會使用 delete-resource-share 來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 AWS 的資源

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

目錄

- 接受和拒絕資源共用邀請
- 檢視與您共用的資源共用
- 檢視與您共用的資源
- 檢視與您共用的委託人
- 離開資源共享

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體。擁有者可以將下列任何項目新增為資源共用的委託人。

- 您帳戶為成員的組織
- 包含您帳戶的組織單位 (OU)
- 您的個別帳戶
- 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 中組織 AWS 帳戶 成員的 新增至資源共用 AWS Organizations，且啟用組織內的共用，則會自動存取共用資源，而不必接受邀請。服務主體也可以自動存取共用資源，而無需接受邀請。如果稍後從組織移除您透過其取得存取權的帳戶，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。

如果您被下列其中一項新增至資源共享，您會收到加入資源共享的邀請：

- 中的組織外部帳戶 AWS Organizations
- AWS Organizations 未啟用與 共用時，組織內的帳戶

如果您收到加入資源共享的邀請，您必須接受該邀請才能存取其共用資源。如果您拒絕邀請，則無法存取共用資源。

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享。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 – 客戶擁有的 IPv4 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

回應資源共享的邀請

1. 導覽至 AWS RAM 主控台中的與我共用：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享，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，請參閱與全域資源相比，共用區域資源。
3. 檢閱您已新增的資源共享清單。

   狀態欄指出資源共享的目前參與狀態。`Pending` 狀態表示您已新增至資源共享，但您尚未接受或拒絕邀請。
4. 若要回應資源共享邀請，請選取資源共享 ID，然後選擇接受資源共享以接受邀請，或拒絕資源共享以拒絕邀請。如果您拒絕邀請，您將無法存取 資源。如果您接受邀請，即可存取 資源。

AWS CLI

回應資源共享的邀請

您可以使用下列命令來接受或拒絕資源共享的邀請：

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

1. 下列範例一開始使用 get-resource-share-invitations 命令來擷取使用者 可用的所有邀請清單 AWS 帳戶。 AWS CLI `query` 參數可讓您將輸出限制為僅那些`status`設定為 的邀請`PENDING`。此範例顯示來自帳戶 `111111111111` 的一個邀請，目前`PENDING`適用於指定`123456789012`中的目前帳戶 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. 找到您要接受的邀請後，請在輸出`resourceShareInvitationArn`中記下要在下一個命令中使用的 ，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 變更為 `PENDING` `ACCEPTED`。

如果您改為拒絕邀請，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

您可以檢視您有權存取的資源共用。您可以查看哪些主體與您共用資源，以及他們共用哪些資源。

Console

檢視資源共用

1. 導覽至 主控台中的 AWS RAM 與我共用 ： 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享，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，請參閱與全域資源相比，共用區域資源。
3. （選用）套用篩選條件以尋找特定資源共享。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的屬性欄位下拉式清單。選擇一個之後，您可以從該欄位的可用值清單中選擇。您可以新增其他屬性或關鍵字，直到您找到所需的資源為止。
4. AWS RAM 主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 以檢視資源共享的詳細資訊頁面。

- 擁有者 – AWS 帳戶 建立資源共用的 ID。
- 狀態 - 資源共用的目前狀態。可能的值包括：
  - `Active` – 資源共享處於作用中狀態，可供使用。
  - `Deleted` – 資源共享已刪除，不再可供使用。
  - `Pending` – 接受資源共享的邀請正在等待回應。

AWS CLI

檢視資源共用

使用 get-resource-shares 命令，並將 `--resource-owner` 參數設定為 `OTHER-ACCOUNTS`。

下列範例顯示其他 AWS 區域 與呼叫帳戶所指定 中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。您可以查看哪些主體與您共用資源，以及哪些資源共用包含資源。

Console

檢視與您共用的資源

1. 導覽至 主控台中的 AWS RAM 與我共用 ： 共用資源頁面。
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 。若要查看包含全球資源的資源共享，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，請參閱與全域資源相比，共用區域資源。
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：
   - 資源 ID – 資源的 ID。選擇要在該服務主控台中檢視的資源 ID。
   - 資源類型 – 資源的類型。
   - 上次共用日期：與您共用資源的日期。
   - 資源共用 – 包含資源的資源共用數目。選擇值以檢視資源共用。
   - 擁有者 ID – 擁有資源的主體 ID。

AWS CLI

檢視與您共用的資源

您可以使用 list-resources 命令來檢視與您共用的資源。

下列範例命令會顯示從 AWS 區域 另一個 指定的 中，透過資源共用存取資源的詳細資訊 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"
        }
    ]
}
```

檢視與您共用的委託人

您可以檢視與您共用資源的所有委託人清單。您可以查看他們與您共用的資源和資源。

Console

檢視與您共用資源的主體

1. 在 https：//https://console.aws.amazon.com/ram/home 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，您必須將 AWS 區域 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 與全域資源相比，共用區域資源。
3. 在導覽窗格中，選擇 Shared with me (與我共用)、Principals (委託人)。
4. （選用）您可以套用篩選條件來尋找特定委託人。您可以套用多個篩選條件，藉此縮小搜尋範圍。
5. 主控台會顯示下列資訊：
   - 委託人 ID – 與您共用的委託人 ID。
   - 資源共用 – 委託人已新增您的資源共用數量。選擇號碼以檢視資源共享清單。
   - 資源 – 委託人與您共用的資源數量。選擇值以檢視資源清單。

AWS CLI

檢視與您共用資源的主體

您可以使用 list-principals 命令來擷取與 共用資源的委託人清單 AWS 帳戶。

下列範例命令會顯示與用來呼叫指定 中 操作的帳戶共用資源 AWS 帳戶 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
        }
    ]
}
```

離開資源共享

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，您會失去共用資源的存取權。

離開資源共用的先決條件

- 只有當資源共用是以個人身分共用 AWS 帳戶 ，而不是在組織內容中共用時，您才能保留資源共用。如果您是由 AWS 帳戶 組織內的 新增至資源共用，且 AWS Organizations 已啟用與 共用，則無法離開資源共用。會自動存取組織內的資源共用。
- 若要保留資源共用，請確認資源共用是空的，或是只包含支援保留共用的資源類型。

  以下是唯一支援離開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`

如何保留資源共享

Console

保留資源共用

1. 導覽至主控台中的 AWS RAM 與我共用：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 。若要查看包含全球資源的資源共享，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，請參閱與全域資源相比，共用區域資源。
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保留。

AWS CLI

保留資源共用

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

下列範例命令會導致 AWS 帳戶 呼叫 命令的 失去 ARN 所指定資源共享所共用資源的存取權。您必須將請求導向 中的 AWS 區域 服務端點，其中包含您要離開的資源共用。

1. 首先，擷取資源共享清單，以擷取您要離開的資源共享 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，您可以執行 命令來保留該資源共享。請注意，您也必須指定帳戶 ID 123456789012作為與指定資源共享取消關聯的委託人，該共用由帳戶 共用111111111111。

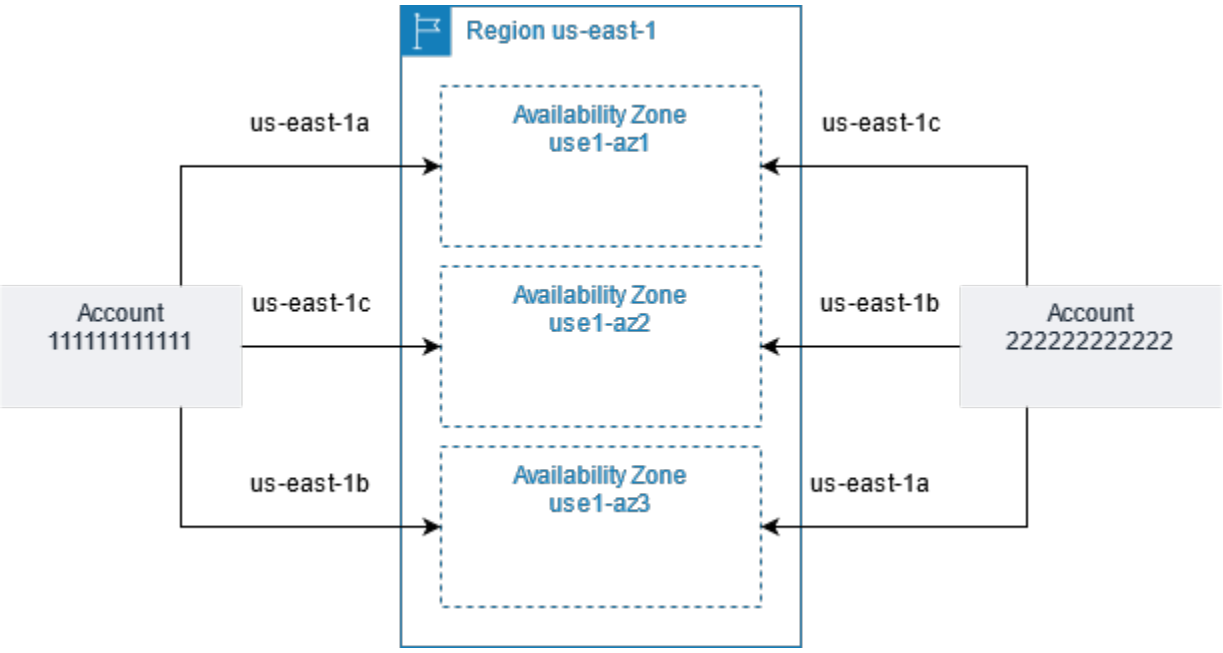
```
$ aws ram disassociate-resource-share \
```

```
    --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 IDs

AWS 會將實體可用區域隨機對應至每個 的可用區域名稱 AWS 帳戶。此方法有助於在 中的可用區域分配資源 AWS 區域，而不是將資源集中在每個區域的可用區域「a」中。因此，`us-east-1a`您 AWS 帳戶的可用區域可能不會代表與`us-east-1a`不同 AWS 帳戶相同的實體位置。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的區域與可用區域。

下圖顯示每個帳戶的可用區域IDs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 AWS 區域，還必須識別可用區域。例如，Amazon VPC 子網路。在單一帳戶中，可用區域與特定名稱的映射並不重要。但是，當您使用 與其他人 AWS RAM 共用此類資源時 AWS 帳戶，映射很重要。此隨機映射會讓存取共用資源的帳戶功能複雜化，以了解要參考哪個可用區域。為了協助解決此問題，這類資源也可讓您使用 AZ ID 來識別資源相對於您帳戶的實際位置。AZ ID 是所有可用區域的唯一且一致的識別符 AWS 帳戶。例如， `use1-az1` 是 `us-east-1` 區域中可用區域的 AZ ID，代表每個 AWS 帳戶中相同的實體位置。

您可以使用 AZ IDs 來判斷一個帳戶中資源相對於另一個帳戶中資源的位置。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。每個子網路的 AZ ID 會顯示在 Amazon VPC 主控台中，並且可以使用 進行查詢 AWS CLI。

Console

檢視您帳戶中可用區域的 AZ ID

1. 導覽至AWS RAM 主控台中的 AWS RAM 主控台頁面。
2. 您可以在您的 AZ IDs AWS 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 IDs，以及它們如何對應至呼叫 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。有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 AWS 服務的資源類型分組依據 AWS RAM。資料表中的資料欄指定每個資源類型支援哪些功能：

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。	是
	– 您只能與 帳戶共用此類型的資源。	否
可以與其組織外部的帳戶共用	– 您只能與其組織內外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。	是
	– 您只能與相同組織的成員帳戶共用此類型的資源。	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，但此欄中的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。 – 此類型的資源不支援使用客戶受管許可。	是 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。 – 您無法與 共用此類型的資源 AWS 服務。	是 否

AWS App Mesh

您可以使用 來共用下列 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	是	是 可以與任何 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
	App Mesh 《使用者指南》中的使用共用網格。		AWS 帳戶。		

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 API 的一部分，該 API 可從相同區域中不同帳戶間的多個子結構描述 APIs存取資料。如需詳細資訊，請參閱《 AWS AppSync 開發人員指南》中的合併 APIs。	是	是 可以與任何 共用 AWS 帳戶。	是	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。這可讓多個帳戶調用映射至私有 APIs網域名稱。如需詳細資訊，請參閱《Amazon APIs Gateway 開發人員指南》中的 API Gateway 中私有 API 的自訂網域名稱。 Amazon API Gateway	否	是 可以與任何 共用 AWS 帳戶。	否	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-c`	集中建立和管理 ARC 叢集，並與其他 AWS 帳戶 或您的組織共用。這可讓多個帳戶在單一共用叢集中建立控制面	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
`ontrol:Cluster`	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 Application Recovery Controller (ARC) 開發人員指南》中的跨帳戶共用叢集。		可以與任何 共用 AWS 帳戶。		

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、集中管理的資料庫叢集。如需詳細資訊，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。	否	是 可以與任何 共用 AWS 帳戶。	否	否

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，並與其他 AWS 帳戶 或您的組織共用。此選項可讓多個（多個）帳戶從保存庫存取和還原備份。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 可以與任何 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	是	否 只能在自己的組織中與 AWS	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《Amazon Bedrock 使用者指南》中的為另一個帳戶共用模型。		帳戶 共用。		

AWS Billing 檢視服務

您可以使用 來共用下列 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 的支出。如需詳細資訊，請參閱AWS Cost Management 《 使用者指南》中的使用 Billing View 控制成本管理資料存取。	否	否 只能在自己的組織中與 AWS 帳戶 共用。	是	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。	是	是	是	否

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	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
	《使用者指南》中的使用共用專案。				
報告群組 `codebuild:ReportGroup`	建立報告群組，並在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。報告可以在建立後檢視 30 天，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。	是	是 可以與任何 共用 AWS 帳戶。	是	否

AWS CodeConnections

您可以使用 來共用下列 CodeConnections 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
程式碼連線	管理在多個帳戶中重複使用程式碼連線。換句話說，共用程式碼連線可減少管理員負擔，並	否	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
`codeconnections:Connection`	需要在每個需要程式碼連線的帳戶中存取管理員。如需詳細資訊，請參閱《 開發人員工具主控台使用者指南》中的與 共用連線 AWS 帳戶。		可以與任何 共用 AWS 帳戶。		

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 DataZone 使用者指南》中的什麼是 Amazon DataZone。	否	是 可以與任何 共用 AWS 帳戶。	否	否

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 或您的組織共用預留容量。這可讓多個 將其 Amazon EC2 執行個體 AWS 帳戶 啟動到集中管理的預留容量。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。 **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，則會以可累積較高成本的隨需執行個體的形式啟動。建議您嘗試在 Amazon EC2 主控台中檢視共用容量保留，以確認您可以存取共	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
	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。				
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 在 上將其 Amazon EC2 執行個體 AWS 帳戶 啟動至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》中的使用共用的專用主機。	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
置放群組 `ec2:PlacementGroup`	在組織內部和外部 AWS 帳戶共用您擁有的置放群組。您可以從您共用的任何帳戶啟動 Amazon EC2 執行個體至共用置放群組。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 可以與任何 共用 AWS 帳戶。	否	否

EC2 Image Builder

您可以使用 來共用下列 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 Image Builder 使用者指南中的共用 EC2 Image Builder 資源。	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
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 Image Builder 使用者指南中的共用 EC2 Image Builder 資源。	是	是 可以與任何 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 EC2 Image Builder 建立的映像。如需詳細資訊，請參閱 EC2 Image Builder 使用者指南中的共用 EC2 Image Builder 資源。	是	是 可以與任何 共用 AWS 帳戶。	是	否
映像配方 `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 Image Builder 使用者指南中的共用 EC2 Image Builder 資源。	是	是 可以與任何 共用 AWS 帳戶。	是	否

Elastic Load Balancing

您可以使用 共用下列 Elastic Load Balancing 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
信任存放區 `elasticloadbalancing:TrustStore`	集中建立和管理 Elastic Load Balancing 信任存放區，並與其他 AWS 帳戶 或您的組織共用。安全管理員可以維護單一或較少數量的信任存放區，並跨 Application Load Balancer 啟用互斥 TLS 組態。如需詳細資訊，請參閱《Application Load Balancer 使用者指南》中的共用 Application Load Balancer 的 Elastic Load Balancing 信任存放區。	是	是	否	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
選擇不接收清單 `sms-voice:OptOutList`	建立選擇退出清單，並與組織中 AWS 帳戶 的其他 共用。您可以共用選擇退出清單，讓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 也可以檢查使用者電話號碼的狀態。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 可以與任何 共用 AWS 帳戶。	是	否
電話號碼 `sms-voice:PhoneNumber`	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 可以與任何 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	否	是 可以與任何 共用	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
	Messaging SMS 《使用者指南》中的使用共用資源。		AWS 帳戶。		
寄件者 ID `sms-voice:SenderId`	建立和管理寄件者 IDs，並將其分享給其他 AWS 帳戶 或您的組織。這可讓多個 使用共用寄件者 ID 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 可以與任何 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 for 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 FSx APIs `CreateVolume` 或在共用磁碟區下使用	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
	OpenZfs 快照執行資料複寫`CopySnapshotAndUpdateVolume` 。如需詳細資訊，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 來共用下列 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
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。	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
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有關 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。這可讓使用者執行查詢和 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。	否	是 可以與任何 共用 AWS 帳戶。	否	否

AWS License Manager

您可以使用 來共用下列 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:Li`	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多	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
`censeConfiguration`	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。		可以與任何 共用 AWS 帳戶。		

AWS Marketplace

您可以使用 來共用下列 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`	在 AWS 帳戶 組織中建立、管理和共用實體 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 可以與任何 共用 AWS 帳戶。	否	否

AWS Migration Hub Refactor Spaces

您可以使用 來共用下列 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`	建立重構空間環境，並使用它來包含您的重構空間應用程式。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 和使用者檢視環境和其中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 共用重構空間環境 AWS RAM。	是	是 可以與任何 共用 AWS 帳戶。	是	否

多方核准

您可以使用 來共用下列多方核准資源 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
核准團隊 `mpa:ApprovalTeam`	建立和管理核准團隊，並將其分享給其他 AWS 帳戶 或您的組織。這可讓其他 AWS 帳戶 使用與受保護操作相關聯的核准團隊。受保護的操作是預先定義的操作清	是	是 可以與任何 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
	單，需要團隊核准才能執行。如需詳細資訊，請參閱《多方核准使用者指南》中的術語和概念。		AWS 帳戶。		

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 `network-firewall:Firewall`	集中建立和管理防火牆，並與其他防火牆共用， AWS 帳戶 以便它們可以建立防火牆端點。這可讓多個帳戶使用單一防火牆的保護。如需詳細資訊，請參閱《 AWS Network Firewall 開發人員指南》中的共用 AWS Network Firewall 資源。	是	是 可以與任何 共用 AWS 帳戶。	否	否
防火牆政策 `network-firewall:F`	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	是	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
`irewallPolicy`	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 AWS Network Firewall 資源。		可以與任何 共用 AWS 帳戶。		

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 AWS Network Firewall 資源。	是	是
			
			可以與任何 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 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 Private Certificate Authority

您可以使用 來共用下列 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`	為組織的內部公有金鑰基礎設施 (CAs)，並與其他 AWS 帳戶 或您的組織共用這些 CAs。這可讓其他帳戶中 AWS Certificate Manager 的使用者發行由您共用 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 可以與任何 共用 AWS 帳戶。	否	是

AWS 資源總管

您可以使用 來共用下列 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 搜尋和探索可透過 檢視存取的資源。如需詳細資訊，	否	否 只能在自己的組織中與 AWS	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
	請參閱AWS 資源總管《使用者指南》中的共用 Resource Explorer 檢視。		帳戶 共用。		

AWS Resource Groups

您可以使用 來共用下列 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 License Manager 《使用者指南》中的在中託管資源群組 AWS License Manager。	否	是 可以與任何 共用 AWS 帳戶。	否	否

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 Resolver 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 Resolver 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
Route 53 Profiles `route53profiles:Profile`	Profiles 集中建立和管理 Route 53，並與其他 AWS 帳戶 或您的組織共用。這可讓多個帳戶將 Route 53 中指定的 DNS 組態套用至 Profiles多個 VPCs。如需詳細資訊，請參閱《Amazon Route 53 Profiles 開發人員指南》中的 Amazon Route 53。	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
解析程式規則 `route53resolver:ResolverRule`	集中建立和管理 Resolver 規則，並將其與其他 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、集中管理的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
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 VPCs DNS 查詢記錄到集中管理的查詢日誌。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 可以與任何 共用 AWS 帳戶。	是	否

Amazon Simple Storage Service

您可以使用 來共用下列 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
存取授權 `s3:AccessGrants`	集中建立和管理 S3 Access Grants 執行個體，並將其與其他 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 可以與任何 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`	為了可探索性 – 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。一旦授予存取權，這些帳戶的使用者可以從 目錄檢視已與其共用的功能群組。如需詳細資訊，請參閱	否	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
	《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。				
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，以用於選取特徵群組資源。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。	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
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 共用。如需詳細資訊，請參閱《Amazon SageMaker AI JumpStart 開發人員指南》中的使用私有策劃中樞控制基礎模型存取。 Amazon SageMaker	是	是 可以與任何 共用 AWS 帳戶。	是	否
歷程群組 `sagemaker:LineageGroup`	Amazon SageMaker AI 可讓您建立管道中繼資料的歷程群組，深入了解其歷史記錄和關係。與組織中的其他 AWS 帳戶 或帳戶共用歷程群組。這可讓多個 AWS 帳戶 和 使用者檢視有關歷程群組的資訊，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》中的跨帳戶歷程追蹤。	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
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，以簡化控管和報告。與組織中的其他 AWS 帳戶 或帳戶共用模型卡，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 SageMaker AI 模型卡。Amazon SageMaker	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
SageMaker AI 模型登錄檔模型套件群組 `sagemaker:model-package-group`	使用 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 SageMaker AI 模型登錄檔。 Amazon SageMaker	是	是	是	否
SageMaker AI 合作夥伴應用程式 `sagemaker:PartnerApp`	使用 SageMaker AI 合作夥伴 AI 應用程式，您可以集中建立和管理 SageMaker AI 合作夥伴 AI 應用程式，並與其他共用其存取權 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
SageMaker AI 管道 `sagemaker:Pipeline`	透過 Amazon SageMaker AI 模型建置管道，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 SageMaker AI 管道的跨帳戶支援。 Amazon SageMaker	是	是 可以與任何 共用 AWS 帳戶。	是	否

AWS Service Catalog AppRegistry

您可以使用 來共用下列 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:Applications`	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聯資源的相關資訊。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:AttributeGroups`	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。 **Note** 目前，不支援將另一個帳戶共用的聯絡人新增至事件回應計劃。 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 可以與任何 共用 AWS 帳戶。	是	否
回應計畫 `ssm-incidents:ResponsePlan`	集中建立和管理回應計畫，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 連線至回應計劃，並在偵測到事件時自動建立事件。事件也	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
	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。				

AWS Systems Manager

您可以使用 來共用下列 AWS Systems 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
拒絕存取政策 `ssm:Document`	使用 Systems Manager 建立just-in-time節點存取的核准政策。拒絕存取政策明確防止自動核准對您指定節點的存取請求。與其他 AWS 帳戶 或您的組織共用拒絕存取政策。這可確保即時just-in-time節點存取的拒絕存取政策適用於組織中的所有帳戶。如需詳細資訊，請參閱 AWS Systems Manager《使用者指南》中的使	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
	用 Systems Manager Just-in-time節點存取。				
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這些資料。與其他 AWS 帳戶或您的組織共用 參數。這可讓多個 AWS 帳戶和 使用者檢視字串的相關資訊，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 可以與任何 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
客戶擁有的 IPv4 地址 `ec2:CoipPool`	在 AWS Outposts 安裝過程中，會根據您提供的現場部署網路相關資訊，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，為 Outposts 子網路中的資源提供本機或外部連線。您可以使用彈性 IP 地址或使用自動指派客戶擁有 IP 地址的子網路設定，將這些地址指派給 Outpost 上的資源，例如 EC2 執行個體。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`	與其他 AWS 帳戶 IAM 角色或使用者或整個組織或組織單位 (OU) 集中共用 Amazon VPC IPAM 集區 AWS Organizations。這可讓這些委託人將 CIDRs 從集區配置到各自帳戶中 AWS 的資源，例如 VPCs。如需詳細資訊，	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
	請參閱《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 VPC IPAM 元件，可讓 IPAM 管理和監控屬於擁有帳戶的資源。如需詳細資訊，請參閱《Amazon VPC IPAM 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
子網路 `ec2:Subnet`	集中建立和管理子網路，並與 AWS 帳戶 組織內的子網路共用。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	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的集中受管流量鏡像目標。如需詳細資訊，請參閱《流量鏡射指南》中的跨帳戶流量鏡射目標。	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
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。這可讓其 VPCs與內部部署網路之間透過共用、集中管理的傳輸閘道進行多個 AWS 帳戶 路由流量。如需詳細資訊，請參閱 Amazon VPC Transit Gateways 中的共用傳輸閘道。 **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
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，並與其他 AWS 帳戶 或您的組織共用它們。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 可以與任何 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 可以與任何 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 資源組態 `vpc-lattice:ResourceConfiguration`	在 Amazon VPC Lattice 中建立資源組態，以在帳戶和 VCPs 資源。在資源組態中，您可以識別誰可以存取該資源，並指定您要共用資源的資源閘道。消費者可以透過在其中建立的資源 VPC 端點存取 VPC 資源 AWS PrivateLink。如需詳細資訊，請參閱《VPC Lattice 使用者指南》中的透過 存取 AWS PrivateLink VPC 資源，以及《VPC Lattice 使用者指南》中的 VPC 資源的資源組態。 AWS PrivateLink	否	是 可以與任何 共用 AWS 帳戶。	是	否
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
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 可以與任何 共用 AWS 帳戶。	是	否

AWS 雲端 WAN

您可以使用 共用下列 AWS Cloud 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
Cloud WAN 核心網路 `networkmanager:CoreNetwork`	集中建立和管理 Cloud WAN 核心網路，並與其他網路共用 AWS 帳戶。這可讓單一 Cloud WAN 核心網路上有多個 AWS 帳戶 存取和佈建主機。如需詳細資訊，請參閱《AWS Cloud	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
	WAN 使用者指南》中的共用核心網路。				

在 中管理許可 AWS RAM

在 中 AWS RAM，有兩種類型的受管許可、 AWS 受管許可和客戶受管許可。

受管許可定義取用者如何對資源共享中的資源採取行動。當您建立資源共享時，您必須指定要針對資源共享中包含的每個資源類型使用哪個受管許可。受管許可中的政策範本包含資源型政策所需的一切，委託人和資源除外。資源的 Amazon Resource Name (ARN) 和與資源共享相關聯的委託人 ARN 會完成資源型政策的元素。 AWS RAM 然後， 會撰寫資源型政策，將其連接到該資源共享中的所有資源。

每個受管許可可以有一或多個版本。一個版本指定為該受管許可的預設版本。偶爾， 會透過建立新版本並將該新版本指定為預設值，來 AWS 更新資源類型的 AWS 受管許可。您也可以建立新的版本，以更新客戶受管許可。已連接至資源共享的受管許可不會自動更新。 AWS RAM 主控台會指出何時有新的預設版本可用，而且您可以檢閱新預設版本相較於前一個版本的變更。

> **Note**
>
> 建議您盡快更新到 AWS 受管許可的新版本。這些更新通常會新增對可使用 AWS 服務 共用其他資源類型的新增或更新的支援 AWS RAM。新的預設版本也可以解決和修正安全漏洞。

> **Important**
>
> 您只能將受管許可的預設版本連接至新的資源共享。

您可以隨時擷取可用受管許可的清單。如需詳細資訊，請參閱檢視受管許可。

主題

- 檢視受管許可
- 在 中建立和使用客戶受管許可 AWS RAM
- 將 AWS 受管許可更新至較新版本
- 在 中使用客戶受管許可的考量 AWS RAM
- 受管許可的運作方式
- 受管許可的類型

檢視受管許可

您可以檢視可指派給資源共享中資源類型的受管許可詳細資訊。您可以識別指派給資源共享的受管許可。若要查看這些詳細資訊，請使用 主控台中的 AWS RAM 受管許可程式庫。

Console

檢視 中可用受管許可的詳細資訊 AWS RAM

1. 導覽至 AWS RAM 主控台中的受管許可程式庫頁面。
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享，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，請參閱與全域資源相比，共用區域資源。雖然所有區域共用相同的可用 AWS 受管許可，但這會影響 中每個受管許可顯示的相關聯資源共用數量Step 5。客戶受管許可只能在其建立所在的區域中使用。
3. 在受管許可清單中，選擇您要檢視其詳細資訊的受管許可。您可以使用搜尋方塊來篩選受管許可清單，方法是輸入部分名稱或資源類型，或從下拉式清單中選擇受管許可類型。
4. （選用）若要變更顯示偏好設定，請選擇受管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。
   - 包裝線 – 是否要在資料表列中包裝線。
   - 資料欄 – 是否顯示或隱藏資源類型和相關聯共享的相關資訊。

   完成設定顯示偏好設定後，請選擇確認。
5. 針對每個受管許可，清單會顯示下列資訊：
   - 受管許可名稱 – 受管許可的名稱。
   - 資源類型 – 與受管許可相關聯的資源類型。
   - 受管許可類型 – 受管許可是 AWS 受管許可還是客戶受管許可。
   - 關聯的共用 – 與受管許可相關聯的資源共用數目。如果出現數字，則您可以選擇數字，以顯示具有以下資訊的資源共享資料表：
     - 資源共用名稱 – 與受管許可相關聯的資源共用名稱。
     - 受管許可版本 – 連接到此資源共享的受管許可版本。
     - 擁有者 – AWS 帳戶 資源共用擁有者的數目。

  - 允許外部主體 – 資源共用是否允許與組織外部的主體共用 AWS Organizations。
  - 狀態 – 資源共用與受管許可之間的關聯目前狀態。
- 狀態 – 描述受管許可是否為：
  - 可連接 – 您可以將受管許可連接到資源共用。
  - 不可連接 – 您無法將受管許可連接到資源共用。
  - 刪除 – 受管許可不再有效，即將刪除。
  - 已刪除 – 已刪除受管許可。在從受管許可程式庫消失之前，它會保持可見狀態兩個小時。

您可以選擇受管許可的名稱，以顯示該受管許可的詳細資訊。受管許可的詳細資訊頁面會顯示下列資訊：

- 資源類型 – 此受管許可適用的資源類型 AWS 。
- 版本數量 – 您最多可以有五個版本的客戶受管許可。
- 預設版本 – 指定哪個版本是預設版本，因此會自動指派給使用此受管許可的所有新資源共用。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ARNs 使用以下格式：

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

  子字串 *[DefaultPermission]*（在實際 ARN 中沒有括號） 僅存在於指定預設值之資源類型的一個受管許可的名稱中。
- 受管許可版本 – 您可以選擇要在此下拉式清單下的索引標籤中顯示哪個版本的資訊。
  - 詳細資訊索引標籤：
    - 建立時間 – 建立此受管許可版本的日期和時間。
    - 上次更新時間 – 上次更新此版本的受管許可的日期和時間。
  - 政策範本索引標籤 – 服務動作和條件的清單，如果適用，此版本的受管許可允許主體對相關聯的資源類型執行。
  - 關聯的資源共用 – 使用此版本的受管許可的資源共用清單。

AWS CLI

檢視 中可用受管許可的詳細資訊 AWS RAM

您可以使用 list-permissions命令來取得可用於呼叫帳戶目前 中資源共用 AWS 區域 的受管許可清單。

```
$ 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許可的 ARN。下列範例會篩選輸出，使其僅包含符合指定名稱之`permissions`陣列結果中的元素。我們也指定只查看結果中的 ARN 欄位，並以純文字格式顯示，而不是預設的 JSON。

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

在您找到您感興趣的特定受管許可的 ARN 之後，您可以執行命令 來擷取其詳細資訊，包括其 JSON 政策文字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許可 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 受管許可。不過，這些受管許可可能不會為您的共用使用案例提供最低權限存取。當其中一個提供的 AWS 受管許可無法運作時，您可以建立自己的客戶受管許可。

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 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，僅授予對共用資源執行任務所需的許可。

此外，您可以視需要更新或刪除客戶受管許可。

主題

- 建立客戶受管許可
- 建立新的客戶受管許可版本
- 選擇不同的版本做為客戶受管許可的預設值
- 刪除客戶受管許可版本
- 刪除客戶受管許可

建立客戶受管許可

客戶受管許可專屬於 AWS 區域。請確定您在適當的區域中建立此客戶受管許可。

Console

建立客戶受管許可

1. 執行以下任意一項：
   - 導覽至受管許可程式庫，然後選擇建立客戶受管許可。
   - 直接導覽至主控台中的建立客戶受管許可頁面。
2. 針對客戶受管許可詳細資訊，輸入客戶受管許可名稱。
3. 選擇此受管許可適用的資源類型。
4. 對於政策範本，您可以定義允許在此資源類型上執行的操作。
   - 您可以選擇匯入受管許可，以使用現有受管許可中的動作。
   - 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. （選用）若要將標籤連接至受管許可，請針對標籤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。
6. 完成後，請選擇建立客戶受管許可。

AWS CLI

建立客戶受管許可

- 執行命令 create-permission，並指定名稱、客戶受管許可適用的資源類型，以及政策範本內文文字。

  下列範例命令會為 `imagebuilder:Component` 資源類型建立受管許可。

```
$ 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
    }
}
```

建立新的客戶受管許可版本

如果您的客戶受管許可的使用案例變更，您可以建立新的受管許可版本。這不會影響您現有的資源共享，只有未來使用此客戶受管許可的新資源共享。

每個受管許可最多可以有五個版本，但您只能關聯預設版本。

Console

建立新的客戶受管許可版本

1. 導覽至受管許可程式庫。
2. 依客戶受管許可篩選受管許可清單，或搜尋您要變更的客戶受管許可名稱。
3. 在受管許可詳細資訊頁面的受管許可版本區段下，選擇建立版本。
4. 對於政策範本，您可以使用視覺化編輯器或 JSON 編輯器來新增或移除動作和條件。

   您也可以選擇匯入受管許可，以使用現有的政策範本。
5. 完成後，請選擇頁面底部的建立版本。

AWS CLI

建立新的客戶受管許可版本

1. 尋找您要為其建立新版本的受管許可的 Amazon Resource Name (ARN)。使用 `--permission-type CUSTOMER_MANAGED` 參數呼叫 list-permissions 以僅包含客戶受管許可，藉此執行此操作。

```
$ 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. 在您擁有 ARN 之後，您可以呼叫 create-permission-version 操作並提供更新的政策範本。

```
$ 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
    }
}
```

輸出包含新版本的版本編號。

選擇不同的版本做為客戶受管許可的預設值

您可以將另一個客戶受管許可版本設定為新的預設版本。

Console

為客戶受管許可設定新的預設版本

1. 導覽至受管許可程式庫。
2. 依客戶受管篩選受管許可清單，或搜尋您要變更的客戶受管許可名稱。
3. 在客戶受管許可詳細資訊頁面的受管許可版本區段下，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，請確認您希望使用此客戶受管許可的所有新資源共用的預設值為此版本。若您同意，請選擇設為預設版本。

AWS CLI

為客戶受管許可設定新的預設版本

1. 呼叫 list-permission-versions，尋找您要設定為預設版本的版本編號。

   下列範例命令會擷取指定受管許可的目前版本。

```
$ 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. 將版本號碼設定為預設之後，您可以呼叫 set-default-permission-version 操作。

```
$ 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。您可以再次執行 list-permission-versions，並確認所選版本的 `defaultVersion` 欄位現在已設定為 `true`。

刪除客戶受管許可版本

每個客戶受管許可最多可以有五個版本。當不再需要 版本且未使用時，您可以將其刪除。您無法刪除客戶受管許可的預設版本。刪除的版本在完全移除之前，會在主控台中最多顯示兩個小時，狀態為已刪除。

Console

刪除客戶受管許可版本

1. 導覽至受管許可程式庫。
2. 依客戶受管篩選受管許可清單，或使用您要刪除的版本搜尋客戶受管許可的名稱。
3. 請確定您要刪除的版本目前不是預設值。
4. 針對頁面的版本區段，選擇關聯的資源共享索引標籤，以查看是否有任何共享使用此版本。

   如果有任何關聯的共用，您必須先變更客戶受管許可版本，才能刪除此版本。
5. 選擇版本區段右側的刪除版本。

6. 在確認對話方塊中，選取刪除以確認您想要刪除此版本的客戶受管許可。

   如果您不想刪除此版本的客戶受管許可，請選擇取消。

AWS CLI

刪除客戶受管許可的一個版本

1. 呼叫 list-permission-versions 操作以擷取可用的版本編號。
2. 取得版本編號後，請提供它做為 delete-permission-version 的參數。

```
$ 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。您可以再次執行 list-permission-versions，並確認版本不再包含在輸出中。

刪除客戶受管許可

如果不再需要客戶受管許可，且未使用，您可以將其刪除。您無法刪除與資源共享相關聯的客戶受管許可。刪除的客戶受管許可會在兩小時後消失。在此之前，它會在已刪除狀態的受管許可程式庫中保持可見。

Console

刪除客戶受管許可

1. 導覽至受管許可程式庫。
2. 依客戶受管許可篩選受管許可清單，或搜尋您要刪除的客戶受管許可名稱。
3. 在選取客戶受管許可之前，請確認受管許可清單中有 0 個相關聯的共用。

   如果仍有與受管許可相關聯的資源共用，您必須先將所有受管許可指派給所有資源共用，才能繼續。
4. 在客戶受管許可詳細資訊頁面的右上角，選擇刪除受管許可。
5. 當確認對話方塊出現時，選擇刪除以刪除受管許可。

AWS CLI

刪除客戶受管許可

1. 透過呼叫具有 `--permission-type CUSTOMER_MANAGED` 參數的 list-permissions 來尋找您要刪除的受管許可 ARN，以僅包含客戶受管許可。

```
$ 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. 在您擁有要刪除之受管許可的 ARN 之後，請提供它做為刪除許可的參數。

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

將 AWS 受管許可更新至較新版本

偶爾 AWS 會更新可連接到特定資源類型的資源共用的 AWS 受管許可。 AWS 執行此操作時，它會建立新的 AWS 受管許可版本。包含指定資源類型的資源共用不會自動更新為使用最新版本的受管許可。您必須明確更新每個資源共享的受管許可。此額外步驟是必要的，因此您可以在將變更套用至資源共享之前進行評估。

Console

每當主控台顯示列出與資源共用相關聯的許可的頁面，且一或多個這些許可使用 許可預設以外的版本時，主控台會在主控台頁面頂端顯示橫幅。橫幅表示您的資源共享正在使用預設版本以外的版本。

此外，當該版本不是預設版本時，個別許可可以在目前版本編號旁顯示更新至預設版本按鈕。

選擇該按鈕會啟動更新資源共享精靈。在精靈的步驟 2 中，您可以更新任何非預設許可的版本，以使用其預設版本。

在您完成精靈之前，不會儲存變更，方法是在精靈的最後一頁選擇提交。

> **Note**
>
> 您只能連接預設版本，且無法還原至其他版本。
> 對於客戶受管許可，在您將許可更新為預設版本之後，除非您先將該其他版本設定為預設版本，否則無法將另一個版本套用至資源共用。例如，如果您將許可更新為預設版本，然後發現要復原的錯誤，您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，然後將該版本指定為預設值。執行其中一個選項之後，您會更新資源共用，以使用現在的預設版本。

AWS CLI

更新 AWS 受管許可的版本

1. get-resource-shares 使用 `--permission-arn` 參數執行 命令，以指定您要更新的受管許可的 Amazon Resource Name (ARN)。這會導致命令只傳回使用該受管許可的資源共用。

   例如，下列範例命令會傳回每個資源共用的詳細資訊，這些資源共用使用 Amazon EC2 容量保留的預設 AWS 受管許可。

   ```
   $ 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，其中至少有一個資源的存取是由該受管許可所控制。

2. 針對上一個命令中指定的每個資源共享，執行命令 associate-resource-share-permission。包含 `--resource-share-arn` 以指定要更新的資源共用、 `--permission-arn`以指定您要更新的 AWS 受管許可，以及 `--replace` 參數以指定您要更新共用以使用該受管許可的最新版本。您不需要指定版本編號；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`ResourceShareArn`您在步驟 1 中從命令收到結果的每個 ，重複上一個步驟中的命令。

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：

- 用於比對委託人屬性的條件索引鍵：
  - `aws:PrincipalOrgId`
  - `aws:PrincipalOrgPaths`
  - `aws:PrincipalAccount`

- 用於限制服務主體存取的條件索引鍵：
  - `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`aws:SourceAccount`值。

受管許可的運作方式

如需快速概觀，請觀看下列影片，示範 受管許可如何讓您將 AWS 最低權限存取的最佳實務套用至 資源。

此影片示範如何根據最低權限的最佳實務，撰寫和建立客戶受管許可的關聯。如需詳細資訊，請參閱 ???。

當您建立資源共用時，您可以將受 AWS 管許可與您要共用的每個資源類型建立關聯。如果受管許可具有多個版本，則新資源共享一律會使用指定為預設的版本。

在您建立資源共用之後， AWS RAM 會使用受管許可來產生連接至每個共用資源的資源型政策。

受管許可中的政策範本會指定下列項目：

Effect

指示 是 `Allow`還是`Deny`主體許可，以對共用資源執行 操作。對於受管許可，效果一律為 `Allow`。如需詳細資訊，請參閱《IAM 使用者指南》中的效果。

動作

授予委託人執行許可的操作清單。這可以是 中的動作 AWS Management Console ，也可以是 AWS Command Line Interface (AWS CLI) 或 AWS API 中的 操作。動作由 許可定義 AWS 。如需詳細資訊，請參閱《IAM 使用者指南》中的動作。

條件

委託人與資源共享中資源互動的時間和方式。條件會將額外的安全層新增至共用資源。使用它們來限制對共用資源敏感動作的存取。例如，您可以包含要求動作源自特定公司 IP 地址範圍的條件，或者必須由使用多重要素身分驗證的使用者執行動作。如需條件的詳細資訊，請參閱《IAM 使用者指

南》中的AWS 全域條件內容金鑰。如需服務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、資源和條件索引鍵。

> **Note**
>
> 條件適用於客戶受管許可，以及 AWS 受管許可支援的 資源類型。
> 如需排除與客戶受管許可搭配使用的條件資訊，請參閱 在 中使用客戶受管許可的考量 AWS RAM。

受管許可的類型

當您建立資源共用時，您可以選擇受管許可，以與資源共用中包含的每個資源類型建立關聯。受 AWS 管許可由 AWS 資源擁有服務定義並由 管理 AWS RAM。您撰寫和維護自己的客戶受管許可。

- AWS 受管許可 – 每個支援的資源類型都有一個預設的 AWS RAM 受管許可。預設受管許可是用於資源類型的許可，除非您明確選擇其他受管許可之一。預設受管許可旨在支援共用指定類型資源的最常見客戶案例。預設受管許可允許主體執行由 服務為 資源類型定義的特定動作。例如，對於 Amazon VPC `ec2:Subnet` 資源類型，預設受管許可允許主體執行下列動作：
  - `ec2:RunInstances`
  - `ec2:CreateNetworkInterface`
  - `ec2:DescribeSubnets`

  預設 AWS 受管許可的名稱使用以下格式：`AWSRAMDefaultPermission`*`ShareableResourceType`*。例如，對於`ec2:Subnet`資源類型，預設 AWS 受管許可的名稱為 `AWSRAMDefaultPermissionSubnet`。

> **Note**
>
> 預設受管許可與受管許可的預設版本不同。所有受管許可，無論是預設或某些資源類型支援的其他受管許可之一，都是獨立的完整許可，具有不同的效果和動作，支援不同的共用案例，例如讀寫和唯讀存取。任何受管許可，無論是 AWS 還是 客戶受管，都可以有多個版本，其中一個版本是該許可的預設版本。

例如，當您共用同時支援完整存取 (`Read` 和 `Write`) 受管許可和唯讀受管許可的資源類型時，您可以為具有完整存取受管許可的管理員建立一個資源共用。然後，您可以使用唯讀受管許可來為其他開發人員建立單獨的資源共享，以遵循授予最低權限的做法。

> **Note**
>
> 使用 的所有 AWS 服務都 AWS RAM 支援至少一個預設受管許可。您可以在 AWS 服務 受管許可程式庫頁面上檢視每個 的可用許可。此頁面提供有關每個可用受管許可的詳細資訊，包括目前與該許可相關聯的任何資源共用，以及是否允許與外部主體共用，如果適用的話。如需詳細資訊，請參閱檢視受管許可。
> 對於不支援其他受管許可的服務，當您建立資源共用時， AWS RAM 會自動套用您所選資源類型定義的預設許可。如果支援，您也可以選擇在關聯受管許可頁面上建立客戶受管許可。

- 客戶受管許可 – 客戶受管許可是您編寫和維護的受管許可，透過精確指定可在哪些條件下使用 共用資源來執行哪些動作 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 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，僅授予對共用資源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。身為 AWS 客戶，您可以從資料中心和網路架構中受益，該架構旨在滿足最安全敏感組織的需求。

安全是 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 也為您提供可安全使用的服務。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 – 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其他 AWS 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 中記錄和監控 AWS RAM
- 中的彈性 AWS RAM
- 中的基礎設施安全性 AWS RAM
- AWS Resource Access Manager 使用介面端點 (AWS PrivateLink) 存取

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

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

- 每個帳戶均要使用多重要素驗證 (MFA)。
- 使用 SSL/TLS 與 AWS 資源通訊。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 使用 設定 API 和使用者活動記錄 AWS CloudTrail。如需有關使用 CloudTrail 追蹤擷取 AWS 活動的資訊，請參閱AWS CloudTrail 《 使用者指南》中的使用 CloudTrail 追蹤。
- 使用 AWS 加密解決方案，以及其中的所有預設安全控制 AWS 服務。
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Amazon S3 的敏感資料。
- 如果您在 AWS 透過命令列界面或 API 存取 時需要 FIPS 140-3 驗證的密碼編譯模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的更多相關資訊，請參閱聯邦資訊處理標準 (FIPS) 140-3。

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

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。IAM 控制項中的管理員，誰可以驗證 （ 登入 ） 和授權 （ 具有許可 ） 來使用 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。您可以控制這些委託人使用 AWS 資源執行任務的許可。您可以免費使用 IAM。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 的 受管政策 AWS RAM
- 使用 AWS RAM的服務連結角色
- 的範例 IAM 政策 AWS RAM
- AWS Organizations 和 的服務控制政策範例 AWS RAM
- 使用 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。
- 透過身分提供者在 IAM 中管理的使用者：

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

AWS RAM 提供數個您可以使用的 AWS 受管政策，可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 的 受管政策 AWS RAM。

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

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
  - Effect
  - 動作
  - 資源
  - 條件

政策結構

IAM 許可政策是 JSON 文件，其中包含下列陳述式：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

動作陳述式指定政策允許或拒絕許可的 AWS RAM API 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

條件陳述式是選用的。它們可用來進一步精簡政策適用的條件。 AWS RAM 支援下列條件索引鍵：

- `aws:RequestTag/${TagKey}` – 測試服務請求是否包含具有指定標籤索引鍵的標籤，並具有指定的值。
- `aws:ResourceTag/${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。外部委託人是您組織 AWS 帳戶 外部的 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` – 測試服務請求中指定的許可 ARN 是否符合您在政策中指定的 ARN 字串。
- `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` – 測試服務請求中指定的委託人的 ARN 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` – 測試服務請求所處理之資源的 ARN 是否符合您在政策中指定的 ARN。
- `ram:ResourceShareName` – 測試服務請求所處理的資源共享名稱是否符合您在政策中指定的字串。
- `ram:ShareOwnerAccountId` – 測試由服務請求所處理之資源共享的帳戶 ID 號碼，符合您在政策中指定的字串。

AWS 的 受管政策 AWS RAM

AWS Resource Access Manager 目前提供數個 AWS RAM 受管政策，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 RAM 受 AWS 管政策的更新

在上述清單中，您可以將前三個政策連接至您的 IAM 角色、群組和使用者，以授予許可。清單中的最後一個政策會保留給 AWS RAM 服務的 服務連結角色。

AWS 受管政策是由 AWS AWS 受管政策建立和管理的獨立政策旨在為許多常見使用案例提供許可，以便您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予特定使用案例的最低權限許可，因為這些許可可供所有 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。

您無法變更 AWS 受管政策中定義的許可。如果 AWS 更新受管政策中 AWS 定義的許可，則更新會影響政策連接的所有主體身分（使用者、群組和角色）。 AWS 服務 當新的 啟動或新的 API 操作可用於現有 服務時， AWS 最有可能更新受 AWS 管政策。

如需詳細資訊，請參閱《IAM 使用者指南》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。

此政策為 擁有的資源共用提供唯讀許可 AWS 帳戶。

它透過授予執行任何 `Get*`或 `List*`操作的許可來執行此操作。它不提供修改任何資源共用的任何功能。

許可詳細資訊

此政策包含以下許可。

- `ram` – 允許主體檢視帳戶所擁有資源共享的詳細資訊。

```
{
    "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。

此政策提供完整的管理存取權，以檢視或修改您擁有的資源共用 AWS 帳戶。

它透過授予執行任何`ram`操作的許可來執行此操作。

許可詳細資訊

此政策包含以下許可。

- `ram` – 允許主體檢視或修改 所擁有資源共享的任何資訊 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。

此政策可讓主體接受或拒絕與此共用的資源共用 AWS 帳戶，以及檢視這些資源共用的詳細資訊。它不提供修改這些資源共用的任何功能。

它透過授予執行某些ram操作的許可來執行此操作。

許可詳細資訊

此政策包含以下許可。

- ram – 允許主體接受或拒絕資源共用邀請，並檢視與帳戶共用的資源共用詳細資訊。

```
{
    "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

AWS 受管政策只能與 的服務連結角色AWSResourceAccessManagerServiceRolePolicy搭配使用 AWS RAM。您無法連接、分離、修改或刪除此政策。

此政策 AWS RAM 可讓您唯讀存取組織的結構。當您啟用 AWS RAM 和 之間的整合時 AWS Organizations， AWS RAM 會自動建立名為 AWSServiceRoleForResourceAccessManager 的服務連結角色，當服務需要查詢組織及其帳戶的相關資訊時，例如，當您在 AWS RAM 主控台中檢視組織結構時，該角色即會擔任該角色。

它透過授予唯讀許可來執行提供組織結構organizations:Describe和帳戶詳細資訊的 和 organizations:List操作來執行此操作。

許可詳細資訊

此政策包含以下許可。

- `organizations` – 允許主體檢視組織結構的相關資訊，包括組織單位及其 AWS 帳戶 所包含的 。

```
{
    "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 RAM 受 AWS 管政策的更新

檢視自此服務開始追蹤這些變更 AWS RAM 以來， AWS 受管政策更新的詳細資訊。如需此頁面變更的自動提醒，請訂閱 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 已記錄其現有的 受管政策並開始追蹤變更。	2021 年 9 月 16 日

使用 AWS RAM的服務連結角色

AWS Resource Access Manager use AWS Identity and Access Management (IAM) 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 AWS 代表您呼叫其他服務 AWS RAM 所需的所有許可。

服務連結角色可讓您更 AWS RAM 輕鬆地設定，因為您不必手動新增必要的許可。 AWS RAM 會定義其服務連結角色的許可，除非另有定義，否則 AWS RAM 只能擔任其服務連結角色。定義的許可包括信任政策和許可政策，該許可政策無法連接到任何其他 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。

的服務連結角色許可 AWS RAM

AWS RAM 當您啟用與 共用`AWSServiceRoleForResourceAccessManager`時， 會使用名為 的服務連結角色 AWS Organizations。此角色授予 AWS RAM 服務檢視組織詳細資訊的許可，例如成員帳戶清單，以及每個帳戶所在的組織單位。

此服務連結角色信任下列服務擔任該角色：

- `ram.amazonaws.com`

名為 AWSResourceAccessManagerServiceRolePolicy 的角色許可政策會連接到此服務連結角色，並允許 對指定的資源 AWS RAM 完成下列動作：

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

若要讓委託人在您的組織中開啟 AWS RAM 共用，該委託人（例如使用者、群組或角色的 IAM 實體）必須具有建立服務連結角色的許可。如需詳細資訊，請參閱《IAM 使用者指南》中的服務連結角色許可。

為 建立服務連結角色 AWS RAM

您不需要手動建立一個服務連結角色。當您在 中開啟 AWS RAM 組織內的共用 AWS Management Console，或使用 AWS CLI 或 AWS API 在帳戶中執行 EnableSharingWithAwsOrganization 時， 會為您 AWS RAM 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訊的許可。

編輯 的服務連結角色 AWS RAM

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。如需更多資訊，請參閱 IAM 使用者指南中的編輯服務連結角色。

刪除 的服務連結角色 AWS RAM

您可以使用 IAM 主控台、 AWS CLI 或 AWS API 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。

的範例 IAM 政策 AWS RAM

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

IAM 政策範例

- 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：限制與外部共享 AWS 帳戶

範例 1：允許共用特定資源

您可以使用 IAM 許可政策來限制主體僅將特定資源與資源共享建立關聯。

例如，下列政策限制主體只能與指定的 Amazon Resource Name (ARN) 共用解析程式規則。如果請求不包含 `ResourceArn` 參數，或者如果該請求包含該參數，則運算子`StringEqualsIfExists`允許請求，則其值完全符合指定的 ARN。

如需何時及為何使用`...IfExists`運算子的詳細資訊，請參閱 ...IAM 使用者指南中的 IfExists 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 政策來限制主體僅將特定資源類型與資源共用建立關聯。

動作 `AssociateResourceShare`和 `CreateResourceShare`可接受主體 和 `resourceArns`做為獨立輸入參數。因此， 會獨立 AWS RAM 授權每個委託人和資源，因此可能會有多個請求內容。這表示當主體與 AWS RAM 資源共享相關聯時，`ram:RequestedResourceType`條件索引鍵不存在於請求內容中。同樣地，當資源與 AWS RAM 資源共享相關聯時，`ram:Principal`條件索引鍵不會出現在請求內容中。因此，若要允許 `AssociateResourceShare`和 將主體與 AWS RAM 資源共享建立關聯`CreateResourceShare`時，您可以使用 `Null`條件運算子。

例如，下列政策限制主體僅共用 Amazon Route 53 解析程式規則，並允許他們將任何主體與該共用建立關聯。

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [{
        "Sid": "AllowOnlySpecificResourceType",
        "Effect": "Allow",
        "Action": ["ram:CreateResourceShare", "ram:AssociateResourceShare"],
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "ram:RequestedResourceType": "route53resolver:ResolverRule"
            }
        }
    },
    {
    "Sid": "AllowAssociatingPrincipals",
     "Effect": "Allow",
        "Action": ["ram:CreateResourceShare", "ram:AssociateResourceShare"],
        "Resource": "*",
        "Condition": {
            "Null": {
                "ram:Principal": "false"
             }
        }
    }
  ]
}
```

範例 3：限制與外部共享 AWS 帳戶

您可以使用 IAM 政策來防止主體與其 AWS 組織外部 AWS 帳戶 的 共用資源。

例如，下列 IAM 政策可防止主體 AWS 帳戶 將外部新增至資源共用。

```
{
    "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)。SCP 是您附加至組織中元素的政策，藉此管理該組織內的許可。SCP 會套用至 AWS 帳戶 您連接 SCP 的 元素下。SCP 可集中控制組織中所有帳戶可用的許可上限。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。

先決條件

若要使用 SCP，您必須執行下列動作：

- 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 SCP 以便於您的組織內使用。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
- 建立您需要的 SCP。如需建立 SCPs的詳細資訊，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

- 範例 1：防止外部共用
- 範例 2：防止使用者接受來自組織外部帳戶的資源共享邀請
- 範例 3：允許特定帳戶共用特定資源類型
- 範例 4：防止與整個組織或組織單位共用
- 範例 5：僅允許與特定委託人共用

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 可防止使用者建立允許與共用使用者組織外部主體共用的資源共用。

AWS RAM 會分別針對通話中列出的每個委託人和資源授權 APIs。

```
{
```

```
    "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享邀請

下列 SCP 會阻止受影響帳戶中的任何主體接受使用資源共享的邀請。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 SCP 影響。

```
{
    "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。

AWS RAM 會分別針對通話中列出的每個委託人和資源授權 APIs。

如果請求不包含資源類型參數，或者如果該請求包含該參數，則運算子`StringEqualsIfExists`允許請求，其值完全符合指定的資源類型。如果您要包含委託人，您必須擁有 `...IfExists`。

如需何時及為何使用`...IfExists`運算子的詳細資訊，請參閱 ...IAM 使用者指南中的 IfExists 條件運算子。

```
{
    "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 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，或與 IAM 角色或使用者共用。

AWS RAM 會分別針對通話中列出的每個委託人和資源授權 APIs。

```
{
    "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：僅允許與特定委託人共用

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

如果您使用具有 否定條件運算子的 `"Effect": "Deny"`元素，例如 `StringNotEqualsIfExists`，即使條件索引鍵不存在，請求仍會遭到拒絕。使用 `Null` 條件運算子檢查授權時是否沒有條件索引鍵。

AWS RAM 會分別針對通話中列出的每個委託人和資源授權 APIs。

```
{
  "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"
        }
      }
    }
  ]
}
```

使用 停用資源共用 AWS Organizations

如果您先前已啟用與 共用， AWS Organizations 而且不再需要與整個組織或組織單位 OUs) 共用資源，則可以停用共用。當您停用與 共用時 AWS Organizations，所有組織或 OUs都會從您建立的資源共用中移除，而且會失去共用資源的存取權。外部帳戶（透過邀請新增至資源共享的帳戶）不會受到影響，且將繼續與資源共享建立關聯。

停用與 共用 AWS Organizations

1. AWS Organizations 使用 AWS Organizations disable-aws-service-access AWS CLI 命令停用對的信任存取。

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

   > **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，並失去對這些共用資源的存取。

2. 使用 IAM 主控台 AWS CLI、 或 IAM API 操作來刪除 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 中記錄和監控 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，以便在發生多點失敗時更輕鬆地偵錯。 AWS 提供數種工具來監控您的 AWS RAM 資源並回應潛在事件：

Amazon EventBridge

提供near-real-time的系統事件串流，描述 AWS 資源的變更。EventBridge 啟用自動的事件驅動運算，因為您可以在這些事件發生時，編寫監看特定事件與在其他 AWS 服務內觸發自動化動作的規則。如需詳細資訊，請參閱AWS RAM 使用 EventBridge 監控。

AWS CloudTrail

擷取 API 呼叫和由 或 代您發出的相關事件， AWS 帳戶 並將日誌檔案交付至您指定的 Amazon S3 儲存貯體。您可以識別呼叫哪些使用者和帳戶 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 記錄 AWS RAM API 呼叫 AWS CloudTrail。

AWS RAM 使用 EventBridge 監控

使用 Amazon EventBridge，您可以設定特定事件的自動通知 AWS RAM。來自 的事件 AWS RAM 會以近乎即時的方式交付至 EventBridge。您可以設定 EventBridge 來監控事件並叫用目標，以回應指出資源共享變更的事件。資源共用擁有者以及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，服務會再嘗試數次。不過，它可能會逾時，並導致該特定事件遺失。

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

考慮您希望與組織中其他帳戶共用 Amazon EC2 容量保留的案例。這樣做是降低成本的好方法。

不過，如果您不符合共用容量保留的所有先決條件，則可能會無提示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 EC2 會如同容量保留已滿一樣，改為以隨需執行個體的形式啟動執行個體。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 SNS 的詳細資訊，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，選擇您要發佈通知的 SNS 主題。此主題必須已存在。
10. 選擇下一步，然後再次選擇下一步，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 的資源共享都會對您發佈主題的收件人產生 SNS 警示。

您也可以嘗試從這些帳戶在 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 記錄 AWS RAM API 呼叫 AWS CloudTrail

AWS RAM 已與 整合 AWS CloudTrail，此服務提供使用者、角色或服務在 AWS 中採取之動作的記錄 AWS RAM。CloudTrail 會將 AWS RAM 的所有 API 呼叫擷取為事件。擷取的呼叫包括從 AWS RAM

主控台呼叫，以及對 AWS RAM API 操作的程式碼呼叫。如果您建立線索，您可以啟用 CloudTrail 事件持續交付至您指定的 Amazon S3 儲存貯體，包括 的事件 AWS RAM。即使您未設定追蹤，依然可以透過 CloudTrail 主控台中的事件歷史記錄檢視最新事件。使用 CloudTrail 所收集的資訊，來判斷對提出的請求 AWS RAM、請求 IP 地址、請求者、提出的時間，以及其他詳細資訊。

如需有關 CloudTrail 的相關資訊，請參閱 AWS CloudTrail 使用者指南。

AWS RAM CloudTrail 中的資訊

建立帳戶 AWS 帳戶 時，您的 上會啟用 CloudTrail。當活動在 中發生時 AWS RAM，該活動會記錄在 CloudTrail 事件中，以及事件歷史記錄中的其他服務 AWS 事件。您可以在 中檢視、搜尋和下載最近的事件 AWS 帳戶。如需詳細資訊，請參閱《使用 CloudTrail 事件歷史記錄檢視事件》https://docs.aws.amazon.com/awscloudtrail/latest/userguide/view-cloudtrail-events.html。

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。線索能讓 CloudTrail 將日誌檔案交付至 Amazon S3 儲存貯體。根據預設，當您在主控台中建立追蹤時，追蹤會套用至所有 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 CloudTrail 日誌中收集的事件資料並對其採取行動。如需詳細資訊，請參閱下列內容：

- 為您的 建立追蹤 AWS 帳戶
- AWS 服務 與 CloudTrail 日誌的整合
- 設定 CloudTrail 的 Amazon SNS 通知
- 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

CloudTrail 會記錄所有 AWS RAM 動作，並記錄在 AWS RAM API 參考中。例如，對 `CreateResourceShare`、`AssociateResourceShare` 以及 `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 根憑證
- 來自 AWS Identity and Access Management (IAM) 角色或聯合身分使用者的臨時安全登入資料。
- IAM 使用者提供的長期安全憑證。
- 另一項 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到您指定的 Amazon S3 儲存貯體。CloudTrail 日誌檔案包含一或多個日誌專案。一個事件為任何來源提出的單一請求，並包含請求動作、請求的日期和時間、請求參數等資訊。CloudTrail 日誌檔並非依公有 API 呼叫的堆疊追蹤排序，因此不會以任何特定順序出現。

以下範例顯示 `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"
```

```
}
```

中的彈性 AWS RAM

AWS 全域基礎設施是以 AWS 區域 和 可用區域為基礎建置。 AWS 區域 提供多個實體分隔和隔離的可用區域，這些區域與低延遲、高輸送量和高度冗餘聯網連接。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 和 可用區域的詳細資訊，請參閱AWS 全球基礎設施。

中的基礎設施安全性 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 AWS 安全服務及如何 AWS 保護基礎設施的相關資訊，請參閱AWS 雲端安全。若要使用基礎設施安全的最佳實務設計您的 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 並建議使用 TLS 1.3。
- 具備完美轉送私密(PFS)的密碼套件，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，請求必須使用存取金鑰 ID 和與 IAM 主體相關聯的私密存取金鑰來簽署。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。

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

您可以使用 在 VPC 和 之間 AWS PrivateLink 建立私有連線 AWS Resource Access Manager。您可以 AWS RAM 像在 VPC 中一樣存取 ，無需使用網際網路閘道、NAT 裝置、VPN 連線或 AWS Direct Connect 連線。VPC 中的執行個體不需要公有 IP 地址即可存取 AWS RAM。

您可以建立由 AWS PrivateLink提供支援的介面端點來建立此私有連線。我們會在您為介面端點啟用的每個子網中建立端點網路介面。這些是請求者管理的網路介面，可作為目的地為 AWS RAM之流量的進入點。

如需詳細資訊，請參閱「AWS PrivateLink 指南」中的透過 AWS PrivateLink存取 AWS 服務。

的考量事項 AWS RAM

在您設定 的介面端點之前 AWS RAM，請檢閱 AWS PrivateLink 指南中的考量事項。

AWS RAM 支援透過介面端點呼叫其所有 API 動作。

支援 VPC 端點政策 AWS RAM。根據預設， AWS RAM 允許透過介面端點完整存取 。

建立 的介面端點 AWS RAM

您可以使用 Amazon VPC AWS RAM 主控台或 AWS Command Line Interface () 建立 的介面端點 AWS CLI。如需詳細資訊，請參閱《AWS PrivateLink 指南》中的建立介面端點。

AWS RAM 使用下列服務名稱建立 的介面端點：

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

如果您為介面端點啟用私有 DNS，您可以使用 AWS RAM 其預設的區域 DNS 名稱向 提出 API 請求。例如：`ram.us-east-1.amazonaws.com`。

為您的介面端點建立端點政策

端點政策為 IAM 資源，您可將其連接至介面端點。預設端點政策允許 AWS RAM 透過介面端點完整存取 。若要控制 AWS RAM VPC 允許存取的 ，請將自訂端點政策連接至介面端點。

端點政策會指定以下資訊：

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

如需詳細資訊，請參閱「AWS PrivateLink 指南」中的使用端點政策控制對服務的存取。

範例： AWS RAM 動作的 VPC 端點政策

以下是自訂端點政策的範例。當您將此政策連接至介面端點時，它會授予所有資源上所有主體的所列 AWS RAM 動作的存取權。

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

對 的問題進行故障診斷 AWS RAM

使用本指南本節中的資訊，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」
- 錯誤：「AccessDeniedException」
- 錯誤：「UnknownResourceException」
- 嘗試與組織外部帳戶共用時發生錯誤
- 在目的地帳戶中看不到共用資源
- 錯誤：超過限制
- 我組織中的另一個帳戶從未收到邀請
- 您無法共用 VPC 子網路

錯誤：「您的帳戶 ID 不存在於 AWS 組織中」

案例

當嘗試與組織中的帳戶或組織單位 (OU) 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，未成功建立服務連結角色 AWSServiceRoleForResourceAccessManager，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，並失去對這些共用資源的存取。

1. 使用具有管理許可的 IAM 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。

您現在應該可以使用 AWS RAM 與組織中的帳戶和 OUs 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 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 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。
- 透過身分提供者在 IAM 中管理的使用者：

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

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 SCPs 不得封鎖許可。

若要建立資源共享，您需要下列兩個許可：

- `ram:CreateResourceShare`
- `ram:AssociateResourceShare`

若要檢視資源共享，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：找不到 OrganizationalUnit ou-*xxxx*」
- 「CannotUpdateResourceShare： UnknownResourceException：找不到 OrganizationalUnit ou-*xxxx*」。

原因

如果您使用 Organizations AWS Organizations 主控台或 Organizations EnableAWSServiceAccess API 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。EnableAWSServiceAccess 當您使用 Organizations 主控台或 API 啟用整合時，服務不會在您的帳戶中建立`AWSServiceRoleForResourceAccessManager`角色。需要該角色才能存取您組織的相關資訊。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

若要解決問題，請關閉 AWS RAM 和 之間的整合 AWS Organizations。然後，透過呼叫 AWS RAM EnableSharingWithAwsOrganization API 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，並失去對這些共用資源的存取。

1. 使用具有管理許可的 IAM 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。

您現在應該可以使用 AWS RAM 與組織中的帳戶和 OUs 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

某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 EC2) 一部分的虛擬私有連線 (VPCs)。

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`，未成功建立服務連結角色，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，並失去對這些共用資源的存取。

1. 使用具有管理許可的 IAM 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，並失去對這些共用資源的存取。

1. 使用具有管理許可的 IAM 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。

資源共享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已列為主體。如果不是，則更新共享，將帳戶新增為委託人。

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 中的資源分享至另一個帳戶 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 中需要存取資源的 IAM 角色和使用者。例如，以下政策顯示如何授予 B 帳戶中的 角色和使用者的唯讀存取權，以從帳戶 A 取得資源。此政策會依其 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

當您嘗試共用資源時，會收到「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. 如果此配額可用，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。

開啟此選項，並與組織中的另一個帳戶共用時，不會傳送邀請，也不需要接受。您在資源共享中參考為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，即使他們位於同一個 AWS 組織中，它們也會被視為獨立帳戶。邀請會傳送，而且必須先接受，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 AWS RAM 與其他帳戶共用 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項限制，其中一些限制也能夠有效地防止共用 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 RAM 的資源共享建立關聯，以偵測變更。

的服務配額 AWS RAM

您的 AWS 帳戶 具有與 AWS Resource Access Manager (AWS RAM) 相關的下列限制。您可以對一部分限制請求提高限制。聯絡 支援 以請求增加限制。

> **Note**
>
> 下列定義適用於以下配額中的描述：
>
> - 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。資源共享中參考的每個資源都會計入此配額。如果您在三個不同的資源共享中共用相同的資源，則此配額的計數會增加三個。
> - 資源共用 – AWS RAM 建立的容器，可用來共用資源。每個資源共享，無論其包含多少資源，都會計入您的配額。
> - 共用主體 – 您已與資源共用相關聯的識別符。這可以是 AWS Identity and Access Management (IAM) 角色或使用者、 AWS 帳戶 識別符、組織單位或整個組織。您在資源共享中參考的每個共用主體都會新增一個配額使用。如果您透過參考整個組織的 ID 與整個組織共用，則它只會計入此配額的 ID。
> - 客戶受管許可 – 您使用最低權限存取來管理共用資源的使用方式，來解決特定使用案例的受管許可。

資源	預設值限制
每個資源共用的數量上限 AWS 區域	25,000
每個資源共享的資源關聯數目上限	5,000
每個資源共享的主體關聯數目上限	5,000
客戶受管許可的數量上限	1,500
每種資源類型的客戶受管許可數量上限	10
每個客戶受管許可的版本數量上限	5
中所有資源共用的資源關聯數目上限 AWS 區域	25,000

資源	預設值限制
Note 資源共享中包含的每個資源都會計入此限制。如果資源包含在 10 個不同的資源共享中，則會根據限制計算 10 個資源。	
中所有資源共用的主體關聯數目上限 AWS 區域 Note 資源共享中包含的每個主體都會計入此限制。如果委託人包含在 10 個不同的資源共享中，則會根據限制計算 10 個。	25,000
每個共用帳戶的待處理邀請數量上限 • 此配額僅適用於傳送與不屬於相同 的帳戶共用的帳戶 AWS Organizations。 • 沒有配額可限制接收帳戶可以擁有的待處理邀請數量。 • 在屬於相同 且 AWS Organizations 您已在 中開啟資源共用的帳戶之間共用時，不會使用邀請 AWS Organizations。	250

AWS RAM 搭配 AWS SDK 使用

AWS 軟體開發套件 SDKs) 適用於許多熱門的程式設計語言。每個 SDK 都提供 API、程式碼範例和文件，協助開發人員以偏好的語言建置應用程式。

SDK 文件	代碼範例
適用於 C++ 的 AWS SDK	適用於 C++ 的 AWS SDK 程式碼範例
適用於 Go 的 AWS SDK	適用於 Go 的 AWS SDK 程式碼範例
適用於 Java 的 AWS SDK	適用於 Java 的 AWS SDK 程式碼範例
適用於 JavaScript 的 AWS SDK	適用於 JavaScript 的 AWS SDK 程式碼範例
適用於 .NET 的 AWS SDK	適用於 .NET 的 AWS SDK 程式碼範例
適用於 PHP 的 AWS SDK	適用於 PHP 的 AWS SDK 程式碼範例
適用於 Python (Boto3) 的 AWS SDK	適用於 Python (Boto3) 的 AWS SDK 程式碼範例
適用於 Ruby 的 AWS SDK	適用於 Ruby 的 AWS SDK 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。我們也會更新文件，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 RSS AWS RAM 摘要。

變更	描述	日期
新增共享多方核准資源的支援	您現在可以與其他 AWS 帳戶或組織內的 共享多方核准核准團隊。	2025 年 6 月 17 日
新增共用 Amazon SageMaker AI 資源的支援	您現在可以使用 AWS RAM 與其他 AWS 帳戶 和您的組織共用 Amazon SageMaker AI 合作夥伴應用程式。	2025 年 6 月 6 日
新增共享 AWS Network Firewall 資源的支援	您現在可以使用 AWS RAM 與其他 AWS 帳戶 和您的組織共用 AWS Network Firewall 防火牆。	2025 年 5 月 28 日
新增共享 AWS Systems Manager 資源的支援	您可以與其他 AWS 帳戶 或您的組織共用 AWS Systems Manager 拒絕存取政策 AWS RAM。	2025 年 4 月 30 日
新增共享 AWS CodeConnections 資源的支援	您現在可以與組織中的其他 AWS 帳戶 或 共用 AWS CodeConnections 程式碼連線。	2025 年 3 月 5 日
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

新增共享 Amazon VPC Lattice 資源組態的支援	您現在可以與其他 共用 Amazon VPC Lattice 資源組態 AWS 帳戶。	2024 年 12 月 1 日
新增共享 Amazon API Gateway 資源的支援	您現在可以與其他 AWS 帳戶或組織內的 共用 API Gateway 網域名稱。	2024 年 11 月 21 日
新增共用 Amazon VPC 資源的支援	您現在可以與其他 AWS 帳戶或組織內的 共用 Amazon VPC 安全群組。	2024 年 10 月 30 日
新增共享 AWS End User Messaging SMS 資源的支援	您可以與其他 AWS 帳戶 或組織共用 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 (VPC) 中的介面端點直接連線至 RAM。	2024 年 9 月 9 日
新增共享的支援 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
新增共享 Elastic Load Balancing 資源的支援	您可以跨組織 AWS 帳戶 或在組織內共用 Elastic Load Balancing 信任存放區。	2024 年 8 月 5 日
新增共享 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 共用 Amazon Bedrock 自訂模型。	2024 年 8 月 1 日
新增共享 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

新增共享 Amazon SageMaker AI Model Registry 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 6 月 27 日
新增共享 Amazon SageMaker AI JumpStart 的支援	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 與 AWS 帳戶 組織內的其他 共用 Amazon Route 53 Resolver Profiles。	2024 年 4 月 22 日
新增共享 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
新增共用 Amazon FSx for OpenZFS 快照的支援	您現在可以與 AWS 帳戶 組織內的其他 共用 Amazon FSx for OpenZFS 快照。	2023 年 12 月 19 日
新增共享 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
新增共享 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

新增共享 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 Model Card 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 作為可共用資源的支援	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 APIs做為可共用資源的支援	您現在可以使用 AWS 帳戶與其他 共用 AWS AppSync GraphQL APIs AWS RAM。	2023 年 5 月 24 日
新增 AWS Verified Access 對群組做為可共用資源的支援	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 目錄實體做為可共用資源的支援	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	更新了指南以符合 IAM 最佳實務。如需更多詳細資訊，請參閱 IAM 中的安全最佳實務。	2023 年 1 月 3 日
新增對 Amazon EC2 置放群組做為可共用資源的支援	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
新增兩個有關 的介紹影片連結 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
新增支援 AWS Service Catalog AppRegistry 應用程式和屬性群組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 獲得 SOC 和 ISO 認證	AWS RAM 已驗證為符合服務組織控制 (SOC) 和國際標準化組織 (ISO) ISO 9001、ISO 27001、ISO 27017、ISO 27018 和 ISO 27701 標準。	2022 年 5 月 31 日
AWS Resource Access Manager 收到 FedRAMP 認證	AWS RAM 已驗證為符合美國聯邦風險與授權管理計劃 (FedRAMP)。	2022 年 4 月 8 日
AWS Resource Access Manager 獲得 PCI DSS 認證	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 Cloud 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 Cloud 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 VPC IPAM 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 歷程群組。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
新增受管 AWS RAMAWS 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，並連接到 中的 IAM 主體 AWS 帳戶。	2021 年 9 月 16 日
新增共用 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 主體共用資源的支援	對於支援的資源類型，您可以選擇其他 AWS RAM 受管許可，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
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

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
新增對共用 Outpost 和本機閘道路由表的支援	您現在可以使用 與其他 AWS RAM 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
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 共用 Glue 資料目錄、資料庫和資料表 AWS 帳戶。	2020 年 7 月 7 日
新增共享 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
新增支援共用 AWS Outposts 客戶擁有的 IPv4 地址	您現在可以使用 與其他 共用 AWS Outposts 客戶擁有 AWS RAM 的 IPv4 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 共用隨需容量保留 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
新增了共用流量鏡射目標的支援	您現在可以使用 與其他 AWS RAM 共用流量鏡射目標 AWS 帳戶。	2019 年 6 月 25 日
新增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 傳輸閘道 AWS 帳戶。	2018 年 11 月 26 日
新增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。