使用者指南

AWS Resource Groups

AWS Resource Groups: 使用者指南

Table of Contents

什麼是資源群組？

您可以使用資源群組來組織資 AWS 源。 AWS Resource Groups 是一項服務，可讓您一次管理和自動執行大量資源上的任務。本指南說明如何在 AWS Resource Groups中建立和管理資源群組。您可以在資源上執行的工作視您使用的 AWS 服務而有所不同。如需支援的服務清單，以 AWS Resource Groups 及每個服務允許您使用資源群組的簡短描述，請參閱AWS 與之合作的服務 AWS Resource Groups。

您可以透過下列任一進入點存取 Resource Groups。

- 在頂端導覽列中，選擇「服務」。AWS Management Console然後，在 [管理與控管] 下，選擇 [Resource Groups 與標籤編輯器]。

  直接鏈接：AWS Resource Groups 控制台
- 透過使用 Resource GroupsAPI，使用 AWS CLI 命令或 AWS SDK程式設計語言。如需詳細資訊，請 AWS Resource Groups API參閱參考資料。

若要使用 AWS Management Console 首頁上的資源群組

1. 登入 AWS Management Console。
2. 在導覽列上選擇 Services (服務)。
3. 在 [管理與控管] 下，選擇 [Resource Groups 與標籤編輯器]。
4. 在左側的導覽窗格中，選擇 [儲存的 Resource Groups] 以使用現有群組，或選擇 [建立群組] 建立新群組。

資源及其群組類型

在中 AWS，資源是您可以使用的實體。範例包括 Amazon EC2 執行個體、 AWS CloudFormation 堆疊或 Amazon S3 儲存貯體。如果您使用多個資源，您可能會發現將它們作為一個群組進行管理，而不是針對每個任務從一個 AWS 服務移動到另一個服務很有用。如果您管理大量相關資源 (例如組成應用程式層的執行個EC2體)，您可能需要一次對這些資源執行批次處理動作。大量動作的範例包括：

- 套用更新或安全性修補程式。
- 升級應用程式。
- 開啟或關閉網路流量的連接埠。

- 從您的執行個體機群收集特定日誌並監控資料。

資源群組是資 AWS 源的集合，這些資源都處於相同狀態 AWS 區域，且符合群組查詢中指定的準則。在 Resource Groups 中，您可以使用兩種類型的查詢來建立群組。這兩個查詢類型包括以格式 `AWS::service::resource` 指定的資源。

- 以標籤為基礎

  以標籤為基礎的資源群組以查詢為基礎，該查詢會指定資源類型和標籤清單。標籤為索引鍵，可幫助識別和排序組織內的資源。標籤選擇性地包含索引鍵的值。

  > **Important**
  >
  > 請勿在標籤中儲存個人識別資訊 (PII) 或其他機密或敏感資訊。我們使用標籤為您提供帳單和管理服務。標籤不適用於私人或敏感資料。

- AWS CloudFormation 基於堆棧

  以堆 AWS CloudFormation 疊為基礎的資源群組會以查詢為基礎，該查詢會在目前區域的帳戶中指定 AWS CloudFormation 堆疊。您可以選擇性地選擇要在群組中的堆疊中的資源類型。您只能以一個 AWS CloudFormation 堆疊為基礎查詢。

服務連結資源群組

某些資源群組 AWS 服務 定義了您只能使用該服務的主控台和來建立和管理的資源群組APIs。您可以在 Resource Groups 主控台中對這些群組執行的動作受到限制。如需詳細資訊，請參閱《AWS Resource Groups API參考指南》中的資源群組的服務組態。

資源群組可以是巢狀；資源群組可包含在同一區域的現有資源群組。

資源群組的使用案例

依預設，會 AWS Management Console 依 AWS 服務組織。但是透過 Resource Groups，您可以建立自訂主控台，根據標籤中指定的條件或堆疊中的資源來組織和合併資訊。 AWS CloudFormation 以下清單說明資源群組可以協助組織您資源的一些案例。

- 應用程式有不同的階段，例如開發、預備和生產。
- 專案由多個部門或個人管理。
- 您一起用於一般專案的一組 AWS 資源，或者您想要以群組形式管理或監視的資源集。

- 在特定平台 (例如 Android 或 iOS) 上執行之應用程式相關的一組資源。

例如，您要開發 Web 應用程式，而且要對 alpha、beta 和發行階段維護單獨的資源集。每個版本都在 Amazon 上運行，EC2並帶有一個 Amazon 彈性區塊存儲存區 您可以使用 Elastic Load Balancing 來管理流量，使用 Route 53 來管理您的網域。如果沒有 Resource Groups，您可能需要存取多個主控台，只是為了檢查服務的狀態或修改某個應用程式版本的設定。

透過 Resource Groups，您可以使用單一頁面來檢視和管理資源。例如，假設您使用此工具為應用程式的每個版本 (Alpha、beta 版和發行版) 建立資源群組。若要檢查您的應用程式 alpha 版本的資源，請開啟您的資源群組。然後在您的資源群組頁面上檢視彙總的資訊。若要修改特定資源，請在您的資源群組頁面上選擇資源的連結，以存取您所需設定的服務主控台。

AWS Resource Groups 和權限

Resource Groups 功能權限位於帳號層級。只要共用您帳戶的IAM主參與者 (例如角色和使用者) 具有正確的IAM權限，他們就可以使用您建立的資源群組。

標籤為資源的屬性，使得它們會在您的整個帳戶之間共用。部門或專業群組中的使用者可以透過通用的詞彙 (標籤) 來描繪，以建立對其角色與責任有意義的資源群組。擁有通用的標籤也表示當使用者共用資源群組時，不需擔心標籤資訊遺失或發生衝突。

AWS Resource Groups 資源

在 Resource Groups 中，唯一可用的資源是群組。群組具有與其相關聯的唯一 Amazon 資源名稱 (ARNs)。如需有關 Amazon 詳細資 AWS 訊ARNs，請參閱. ARN Amazon Web Services 一般參考

資源類型	ARN格式
Resource Group (資源群組)	`arn:aws:resource-groups:` *`region`*`:`*`account`*`:group/`*`group-name`*

標記的運作方式

標籤是索引鍵和值配對，可做為組織資 AWS 源的中繼資料。對於大多數 AWS 資源，您可以在建立資源時選擇新增標籤，無論是 Amazon EC2 執行個體、Amazon S3 儲存貯體還是其他資源。不過，您也

可以使用標籤編輯器，一次將標籤新增至多個支援的資源。您可以為各種類型的資源建立查詢，然後在搜尋結果中新增、移除或取代資源的標籤。標籤式查詢會將 AND 運算子指派至標籤，因此，查詢會傳回符合指定資源類型和所有指定標籤的任何資源。

> **Important**
>
> 請勿在標籤中儲存個人識別資訊 (PII) 或其他機密或敏感資訊。我們使用標籤為您提供帳單和管理服務。標籤不適用於私人或敏感資料。

若要取得有關標籤的更多資訊，請參閱《標籤編輯器使用指南 您可以使用標籤編輯器來為支援的資源加標籤，以及在您在其中建立和管理資源的服務主控台中使用加標籤功能，為一些額外的資源加標籤。

開始使用 AWS Resource Groups

在中 AWS，資源是您可以使用的實體。範例包括 Amazon EC2 執行個體、Amazon S3 儲存貯體或亞馬遜路線 53 託管區域。如果您使用多個資源，您可能會發現將它們作為一個群組進行管理，而不是針對每個任務從一個 AWS 服務移動到另一個服務很有用。

本節說明如何開始使用 AWS Resource Groups。首先，透過在標籤編輯器中標記 AWS 資源來組織資源。然後在 Resource Groups 中建立查詢，其中包含您想要在群組中的資源類型，以及已套用至資源的標籤。

在 Resource Groups 中建立資源群組後，請使用諸如自動化之類的 AWS Systems Manager 工具來簡化資源群組的管理工作。

若要取得有關開始使用 AWS Systems Manager 功能和工具的更多資訊，請參閱《AWS Systems Manager 使用指南》。

主題

使用的先決條件 AWS Resource Groups

開始使用資源群組之前，請確定您有一個作用中的 AWS 使用現有資源和適當權限來標記資源和建立群組。

主題

註冊成為 AWS

如果您沒有 AWS 帳戶，請完成下列步驟來建立。

若要註冊成為 AWS 帳戶

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

   部分註冊程序需接收來電，並在電話鍵盤輸入驗證碼。

   當您註冊一個 AWS 帳戶，一個 AWS 帳戶根使用者已建立。根使用者可以存取所有 AWS 服務 和帳戶中的資源。作為安全最佳實務，請將管理存取權指派給使用者，並且僅使用根使用者來執行需要根使用者存取權的任務。

建立 資源

您可以建立空的資源群組，但在群組中有資源之前，無法對資源群組成員執行任何工作。如需支援資源類型的詳細資訊，請參閱可與標籤編輯器搭配使用 AWS Resource Groups 的資源類型。

設定許可

為了完整利用資源群組和標籤編輯器，您可能需要額外的許可，來為資源加上標籤或查看資源的標籤索引鍵和值。這些許可分為以下類別：

- 個別服務的許可，使得您可以為來自那些服務的資源加上標籤，並將它們包含在資源群組中。
- 使用標籤編輯器主控台所需的權限
- 使用所需的權限 AWS Resource Groups 控制台和API。

如果您是系統管理員，您可以透過 AWS Identity and Access Management (IAM) 服務。您先建立主參與者 (例如IAM角色或使用者)，或將外部識別與您的 AWS 環境使用類似的服務 AWS IAM Identity

Center。 然後，您可以使用您的使用者需要的權限來套用原則。如需有關建立和附加IAM原則的資訊，請參閱使用原則。

個別服務的權限

> **Important**
>
> 本節說明如果您想要標記來自其他服務主控台的資源APIs，並將這些資源新增至資源群組時，所需的權限。

如資源及其群組類型中所述，每個資源群組代表共用一或多個標籤索引鍵或值之指定類型的資源集合。若要將標籤新增到資源，您需要資源所屬服務所需的許可。例如，若要標記 Amazon EC2 執行個體，您必須擁有該服務中標記動作的許可API，例如 Amazon EC2 使用者指南中列出的動作。

為了完整利用資源群組功能，您需要其他許可，以允許您存取服務的主控台並與該處的資源互動。如需 Amazon 這類政策的範例EC2，請參閱 Amazon EC2使用者指南中的 Amazon EC2 主控台中的範例政策。

Resource Groups 和標籤編輯器的必要權限

若要使用 Resource Groups 和標籤編輯器，必須將下列權限新增至中的使用者政策陳述式IAM。您可以添加 AWS-由維護和保存 up-to-date 的管理策略 AWS，或者您可以建立和維護自己的自訂原則。

使用 AWS Resource Groups 和標籤編輯器權限的受管策略

AWS Resource Groups 和標籤編輯器支持以下內容 AWS 受管理的策略，您可以用來提供一組預先定義的權限給您的使用者。您可以將這些受管理的政策附加到任何使用者、角色或群組，就像您建立的任何其他原則一樣。

ResourceGroupsandTagEditorReadOnlyAccess

此原則會授與附加的IAM角色或使用者權限，以呼叫 Resource Groups 和標籤編輯器的唯讀作業。若要讀取資源的標籤，您還必須透過個別原則擁有該資源的權限 (請參閱下列重要注意事項)。

ResourceGroupsandTagEditorFullAccess

此原則會授與附加的IAM角色或使用者權限，以便在標籤編輯器中呼叫任何 Resource Groups 作業以及讀取和寫入標籤作業。若要讀取或寫入資源的標籤，您還必須透過個別原則擁有該資源的權限 (請參閱下列重要注意事項)。

Important

先前的兩個原則會授與呼叫 Resource Groups 和標籤編輯器作業以及使用這些主控台的權限。對於 Resource Groups 作業，這些策略就足夠了，並授與使用 Resource Groups 主控台中任何資源所需的所有權限。
不過，對於標記作業和標籤編輯器主控台，權限會更加精細。您不僅必須具有調用操作的權限，還必須具有對您嘗試訪問其標籤的特定資源的適當權限。若要授與該標籤存取權，您還必須附加下列其中一個原則：

- 所以此 AWS-託管策略ReadOnlyAccess授予對每個服務資源的只讀操作的權限。 AWS 自動保持此政策與新的最新狀態 AWS 服務，因為他們變得可用。
- 許多服務提供服務特定的唯讀 AWS-受管理的政策，您可以用來限制只存取該服務所提供的資源。例如，Amazon EC2 提供 Amazon EC2ReadOnlyAccess。
- 您可以建立自己的原則，針對您希望使用者存取的少數服務和資源，僅授與非常特定的唯讀作業的存取權。此原則使用「允許清單」策略或拒絕清單策略。

  允許清單策略會利用預設拒絕存取的事實，直到您在原則中明確允許存取為止。因此，您可以使用如下示例所示的策略：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [ "resource-groups:*" ],
            "Resource": "arn:aws:resource-groups:*:123456789012:group/*"
        }
    ]
}
```

  或者，您可以使用「拒絕清單」策略，允許存取您明確封鎖的資源以外的所有資源。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
             "Action": [ "resource-groups:*" ],
            "Resource": "arn:aws:resource-groups:*:123456789012:group/*"
        }
```

```
    ]
}
```

手動新增 Resource Groups 和標籤編輯器權限

- `resource-groups:*`(此權限允許所有 Resource Groups 動作。 如果您想要限制使用者可使用的動作，可以使用特定的 Resource Groups 動作取代星號，或以逗號分隔的動作清單取代星號)
- `cloudformation:DescribeStacks`
- `cloudformation:ListStackResources`
- `tag:GetResources`
- `tag:TagResources`
- `tag:UntagResources`
- `tag:getTagKeys`
- `tag:getTagValues`
- `resource-explorer:*`

> **Note**
>
> 該`resource-groups:SearchResources`權限允許標籤編輯器在您使用標籤鍵或值篩選搜尋時列出資源。
> 此`resource-explorer:ListResources`權限允許「標籤編輯器」在您搜尋資源時列出資源，而不定義搜尋標籤。

若要在主控台中使用 Resource Groups 和標籤編輯器，您還需要執行`resource-groups:ListGroupResources`動作的權限。此權限對於列出目前區域中的可用資源類型是必要的。目前不支援將原則條件與搭配`resource-groups:ListGroupResources`使用。

授與使用權限 AWS Resource Groups 和標籤編輯器

若要新增原則以使用 AWS Resource Groups 和標籤編輯器對用戶，執行以下操作。

1. 開啟主IAM控台。
2. 在導覽窗格中，選擇使用者 。

3. 尋找您要授予的使用者 AWS Resource Groups 和標籤編輯器權限。選擇使用者的名稱來開啟使用者屬性頁面。
4. 選擇新增許可。
5. 選擇直接連接現有政策。
6. 選擇 建立政策。
7. 在JSON索引標籤上，貼上下列原則陳述式。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "resource-groups:*",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "tag:GetResources",
        "tag:TagResources",
        "tag:UntagResources",
        "tag:getTagKeys",
        "tag:getTagValues",
        "resource-explorer:*"
      ],
      "Resource": "*"
    }
  ]
}
```

> **Note**
>
> 此範例原則陳述式僅授與權限 AWS Resource Groups 和「標籤編輯器」動作。它不允許訪問 AWS Systems Manager 「」中的工作 AWS Resource Groups 控制台。例如，此原則不會授與您使用 Systems Manager 自動化指令的權限。若要對資源群組執行「Systems Manager」工作，您必須將「Systems Manager」權限附加至您的原則 (例如`ssm:*`)。如需有關授與 Systems Manager 存取權的詳細資訊，請參閱〈設定 Systems Manager 的存取權限〉AWS Systems Manager 用戶指南。

8. 選擇檢閱政策。
9. 為新政策提供名稱和描述 (例如，`AWSResourceGroupsQueryAPIAccess`)。

10. 選擇 建立政策。
11. 現在已儲存原則IAM，您可以將其附加到其他使用者。如需有關如何將策略新增至使用者的詳細資訊，請參閱《使用指南》中的〈透過將策略直接附加至使用者來新增權限〉。IAM

進一步了解 AWS Resource Groups 授權和存取控制

Resource Groups 支援下列項目。

- 以動作為基礎的政策。例如，您可以建立允許使用者執行ListGroups作業，但不允許其他原則執行作業。
- 資源層級權限。Resource Groups 支援使用ARNs來指定策略中的個別資源。
- 基於標籤的授權。Resource Groups 支援在策略的情況下使用資源標籤。例如，您可以建立一個策略，允許 Resource Groups 使用者完全存取您已標記的群組。
- 暫時性登入資料。使用者可以扮演具有允許 AWS Resource Groups 作業之策略的角色。

Resource Groups 不支援以資源為基礎的政策。

如需有關 Resource Groups 和標籤編輯器如何與 AWS Identity and Access Management (IAM) 整合的詳細資訊，請參閱《AWS Identity and Access Management 使用指南》中的以下主題。

- AWS 與之合作的服務 IAM
- 下列項目的動作、資源和條件索引鍵 AWS Resource Groups
- 使用原則控制存取

AWS 與之合作的服務 AWS Resource Groups

您可以在一起使用以下 AWS 服務 AWS Resource Groups。

AWS 服務	搭配 Resource Groups 使用
AWS CloudFormation— 使用堆疊範本在中 AWS CloudFormation 建立資源群組。	在同一時間佈建和組織 AWS 資源。按標籤組織資源。從另一個堆棧組織資源。使用 Amazon 收集資 AWS 源群組中資源的深入解析， CloudWatch 或使用採取操作動作 AWS Systems Manager。

AWS 服務	搭配 Resource Groups 使用
	如需詳細資訊，請參閱《AWS CloudFormation 使用指南》中的ResourceGroups資源類型參考。
CloudTrail— 使用擷取所有資源群組動作 AWS CloudTrail。	擷取在資源群組上執行之動作的相關資訊，包括執行動作者 (IAM 主體，例如角色、使用者或 AWS 服務)、動作執行時間、動作發生位置 (來源 IP 位址) 等詳細資訊。然後，這些記錄可用於分析或觸發後續行動。 如需詳細資訊，請參閱使用 CloudTrail 事件歷程記錄檢視事件。
Amazon CloudWatch — 啟用即時監控您的 AWS 資源和執行的應用程式 AWS。	聚焦檢視以顯示來自單一資源群組的指標和警示。 如需詳細資訊，請參閱 Amazon CloudWatch 使用者指南中的專注於資源群組中的指標和警示。
Amazon CloudWatch 應用程式深入解析 — 偵測 .NET 和 SQL 伺服器應用程式的常見問題。	監視屬於資源群組的 .NET 和 SQL Server 應用程式資源。 如需詳細資訊，請參閱 Amazon CloudWatch 使用者指南中的支援應用程式元件。
Amazon DynamoDB 表格群組 — 將 DynamoDB 表格組織成邏輯分組，讓您可以更輕鬆地管理資源。	從 DynamoDB 動作功能表中建立、編輯和刪除 DynamoDB 表格群組。 如需詳細資訊，請參閱 Amazon DynamoDB 開發人員指南。
Amazon EC2 專用主機 — 使用現有的每個插槽、每核心或虛擬機器軟體授權，包括視窗伺服器、Microsoft SQL 伺服器、SUSE 和 Linux 企業伺服器。	將 Amazon EC2 執行個體啟動到主機資源群組，以協助您最大化專用主機的使用率。 如需詳細資訊，請參閱 Amazon EC2 使用者指南中的使用專用主機。

AWS 服務	搭配 Resource Groups 使用
Amazon EC2 容量保留 — 為您的 Amazon EC2 執行個體預留容量，以便在需要時使用。您可以指定容量保留的屬性，使其僅適用於以相符屬性啟動的 Amazon EC2 執行個體。	將 Amazon EC2 執行個體啟動到包含一或多個容量保留的資源群組中。如果群組沒有具有相符屬性和已請求執行個體的可用容量的容量保留，則執行個體會以隨需執行個體的形式執行。如果您稍後將相符的容量保留新增至目標群組，則執行個體會自動與該執行個體進行比對並移入保留容量中。 如需詳細資訊，請參閱 Amazon EC2 使用者指南中的使用容量保留群組。
AWS License Manager— 簡化將軟體供應商授權帶入雲端的程序。	設定主機資源群組，以啟用 License Manager 來管理您的專用主機。 如需詳細資訊，請參閱 License Manager 使用指南中的 License Manager 中的主機 Resource Groups 。
AWS 彈性中樞 — 準備並保護您的應用程式免受中斷的影響。	探索使用 Resource Groups 定義的應用程式。 如需詳細資訊，請參閱AWS 新聞部落格中的使用 AWS 彈性中樞測量和提升應用程式復原能力。
AWS Resource Access Manager— 與其他帳號共用您擁有的指定 AWS 資源。	使用共用主機資源群組 AWS RAM。 如需詳細資訊，請參閱《AWS RAM 使用指南》中的可共用資源。

AWS 服務	搭配 Resource Groups 使用
AWS Service Catalog AppRegistry— 定義和管理您的應用程式及其中繼資料。	當您在中建立應用程式時 AppRegistry，該服務會自動為該應用程式建立資源群組。應用程式資源群組是應用程式中所有資源的集合。此服務也會為與應用程式相關聯的每個堆 AWS CloudFormation 疊建立以堆疊為基礎的資源群組。 如需詳細資訊，請參閱《AWS Service Catalog 管理指南》 AppRegistry中的〈使用〉。
AWS Systems Manager— 啟用 AWS 資源的可見性和控制權。	收集營運見解，並針對以資源群組為基礎的應用程式採取大量動作。在 AWS Systems Manager 主控台中，[應用程式管理員：自訂應用程式] 頁面會自動匯入並顯示以資源群組為基礎的應用程式的作業資料。您可以使用「應用程式管理員」中的資訊來協助您判斷應用程式中哪些資源符合標準並正常運作，以及哪些資源需要採取動作。 若要取得更多資訊，請參閱《使用指南》中的〈應用程式管理員〉中的〈AWS Systems Manager 使
Amazon VPC 網路存取分析器 — 識別不需要的網路存取您的資源。 AWS	您可以使用指定網路存取需求的來源和目的地 AWS Resource Groups。這可讓您控管整個 AWS 環境的網路存取，而不受您設定網路的方式影響。 如需詳細資訊，請參閱 Amazon Virtual Private Cloud 使用者指南中的將 Resource Groups 與網路存取範圍搭配使用。

資源群組的服務組態

資源群組可讓您以單位形式管理 AWS 資源集合。一些 AWS 服務通過對該組的所有成員執行請求的操作來支持這一點。這類服務可以將要套用至群組成員的設定儲存為附加至群組的JSON資料結構形式的組態。

本主題說明支援 AWS 服務的可用組態設定。

主題

- 如何存取附加至資源群組的服務組態
- JSON服務配置的語法
- 支援的組態類型和參數

如何存取附加至資源群組的服務組態

支援服務連結群組的服務通常會在您使用該服務所提供的工具 (例如該服務的管理主控台或其 AWS CLI 與 AWS SDK作業) 時，為您設定組態。有些服務會完全管理其服務連結群組，除非主控台或擁有 AWS 服務提供的命令允許，否則您無法以任何方式修改這些服務。不過，在某些情況下，您可以使用 AWS SDKs或其 AWS CLI 對等項目中的下列API作業與服務組態互動：

- 當您使用CreateGroup作業建立群組時，您可以將自己的組態附加至群組。
- 您可以使用此作業來修改連結至群組的目前組PutGroupConfiguration態。
- 您可以呼叫GetGroupConfiguration作業來檢視資源群組的目前配置。

JSON服務配置的語法

資源群組可以包含定義服務特定設定的組態，這些設定可套用至屬於該群組成員的資源。

配置表示為一個JSON對象。在最頂層，配置是組配置項的數組。每個群組組態項目都包含兩個元素：一個Type用於組態，以及由該類型Parameters定義的一組。每個參數都包含一個或多個Name和一個或多個數組的數組Values。下面的例子 *placeholders* 顯示單一範例資源類型之組態的基本語法。此範例顯示具有兩個參數的型別，每個參數都有兩個值。下一節將討論實際的有效類型、參數和值。

```
[
    {
        "Type": "configuration-type",
        "Parameters": [
```

```
            {
                "Name": "parameter1-name",
                "Values": [
                    "value1",
                    "value2"
                ]
            },
            {
                "Name": "parameter2-name",
                "Values": [
                    "value3",
                    "value4"
                ]
            }
        ]
    }
]
```

支援的組態類型和參數

Resource Groups 支援使用下列組態類型。每個組態類型都有一組對該類型有效的參數。

主題

- AWS::ResourceGroups::Generic
- AWS::AppRegistry::Application
- AWS::CloudFormation::Stack
- AWS::EC2::CapacityReservationPool
- AWS::EC2::HostManagement
- AWS::NetworkFirewall::RuleGroup

AWS::ResourceGroups::Generic

此組態類型會指定對資源群組強制執行成員資格需求的設定，而不是為 AWS 服務配置特定資源類型的行為。此組態類型會由需要的服務連結群組 (例如`AWS::EC2::CapacityReservationPool`和`AWS::EC2::HostManagment`類型) 自動新增。

下列項`Parameters`目對`AWS::ResourceGroups::Generic`服務連結群組`Type`有效。

- **allowed-resource-types**

此參數指定資源群組只能包含指定類型的資源。

值的資料類型：字串

允許的值：

- AWS::EC2::Host— 當服務組態也包含 of 類型時，需要Configuration具有此參數和值Configuration的 A AWS::EC2::HostManagement。這可確保群HostManagement組只能包含 Amazon EC2 專用主機。
- AWS::EC2::CapacityReservation— 當服務組態也包含類型的Configuration項目時，需要Configuration具有此參數和值的 A AWS::EC2::CapacityReservationPool。這可確保群CapacityReservation組只能包含 Amazon EC2 容量保留容量。

必要：以附加至資源群組的其他Configuration元素為基礎的條件式。請參閱上一個項目以瞭解允許的值。

下列範例將群組成員限制為僅 Amazon EC2 主機執行個體。

```
[
    {
        "Type": "AWS::ResourceGroups::Generic",
        "Parameters": [
            {
                "Name": "allowed-resource-types",
                "Values": ["AWS::EC2::Host"]
            }
        ]
    }
]
```

- **deletion-protection**

此參數指定除非資源群組不包含任何成員，否則無法刪除該資源群組。如需詳細資訊，請參閱《License Manager 使用指南》中的〈刪除主機資源群組〉

值的數據類型：字符串數組

允許的值：唯一允許的值是["UNLESS_EMPTY"]（值必須為大寫）。

必要：以附加至資源群組的其他Configuration元素為基礎的條件式。只有當資源群組也具有的另一個Configuration元素時，才需要此參Type數AWS::EC2::HostManagement。

下列範例會啟用群組的刪除保護，除非群組沒有成員。

```
[
    {
        "Type": "AWS::ResourceGroups::Generic",
        "Parameters": [
            {
                "Name": "deletion-protection",
                "Values": [ "UNLESS_EMPTY" ]
            }
        ]
    }
]
```

AWS::AppRegistry::Application

此Configuration類型指定資源群組代表由建立的應用程式 AWS Service Catalog AppRegistry。

此類型的資源群組由 AppRegistry 服務完全管理，除了使用提供的工具以外，使用者無法建立、更新或刪除 AppRegistry。

> **Note**
>
> 由於此類型的資源群組是由使用者自動建立 AWS 和維護，而不是由使用者管理，因此這些資源群組不會計入您可在中建立的資源群組數目上限的配額限制 AWS 帳戶。

如需詳細資訊，請參閱 Service Catalog 使用指南 AppRegistry中的使用。

AppRegistry 建立此類型的服務連結資源群組時，也會自動為與應用程式相關聯的每個 AWS CloudFormation 堆疊建立個別的額外AWS CloudFormation 服務連結群組。

AppRegistry 自動為此類型所建立的服務連結群組命名，AWS_AppRegistry_Application-後面加上應用程式名稱的前置詞：AWS_AppRegistry_Application-*MyAppName*

AWS::AppRegistry::Application服務連結群組類型支援下列參數。

- **Name**

  此參數指定使用者在中建立應用程式時所指派的易記名稱 AppRegistry。

值的資料類型：字串

允許的值： AppRegistry 服務允許用於應用程式名稱的任何文字字串。

必要：是

- **`Arn`**

  此參數指定由指派之應用程式的 Amazon 資源名稱 (ARN) 路徑 AppRegistry。

  值的資料類型：字串

  允許的值：一個有效的ARN。

  必要：是

> **Note**
>
> 若要變更任何這些元素，您必須使用 AppRegistry 主控台或該服務的 AWS SDK和 AWS CLI 作業來修改應用程式。

此應用程式資源群組會自動將針對與 AppRegistry 應用程式相關聯之 AWS CloudFormation 堆疊所建立的資源群組納入為群組成員。您可以使用此ListGroupResources作業來查看這些子群組。

下列範例顯示`AWS::AppRegistry::Application`服務連結群組的設定區段。

```
[
    {
        "Type": "AWS::AppRegistry::Application",
        "Parameters":[
            {
                "Name": "Name",
                "Values": [
                    "MyApplication"
                ]
            },
            {
                "Name": "Arn",
                "Values": [
```

```
                    "arn:aws:servicecatalog:us-east-1:123456789012:/
applications/<application-id>"
                ]
            }
        ]
    }
]
```

AWS::CloudFormation::Stack

此Configuration類型指定該組表示 AWS CloudFormation 堆棧，其成員是該堆棧創建的 AWS 資源。

當您將 AWS CloudFormation 堆疊與 AppRegistry 服務產生關聯時，系統會自動為您建立此類型的資源群組。除非使用提供的工具，否則您無法建立、更新或刪除這些群組 AppRegistry。

AppRegistry 自動為此類型所建立的服務連結群組命名，AWS_CloudFormation_Stack-後面加上堆疊名稱的前置詞：AWS_CloudFormation_Stack-*MyStackName*

> **Note**
>
> 由於此類型的資源群組是由使用者自動建立 AWS 和維護，而不是由使用者管理，因此這些資源群組不會計入您可在中建立的資源群組數目上限的配額限制 AWS 帳戶。

如需詳細資訊，請參閱 Service Catalog 使用指南 AppRegistry中的使用。

AppRegistry 會針對您與 AppRegistry 應用程式相關聯的每個 AWS CloudFormation 堆疊，自動建立此類型的服務連結資源群組。這些資源群組會成為 AppRegistry應用程式之父項資源群組的子項成員。

此 AWS CloudFormation 資源群組的成員是建立為堆疊一部分的 AWS 資源。

AWS::CloudFormation::Stack服務連結群組類型支援下列參數。

- **Name**

  此參數指定使用者在建立 AWS CloudFormation 堆疊時所指派之堆疊的易記名稱。

  值的資料類型：字串

  允許的值： AWS CloudFormation 服務允許用於堆疊名稱的任何文字字串。

必要：是

- **`Arn`**

  此參數指定中附加至應用程式之 AWS CloudFormation 堆疊的 Amazon 資源名稱 (ARN) 路徑 AppRegistry。

  值的資料類型：字串

  允許的值：一個有效的ARN。

  必要：是

> **Note**
>
> 若要變更任何這些元素，您必須使用 AppRegistry 主控台或對等的 AWS SDK和 AWS CLI 作業來修改應用程式。

下列範例顯示`AWS::CloudFormation::Stack`服務連結群組的組態區段的外觀。

```
[
    {
        "Type": "AWS::CloudFormation::Stack",
        "Parameters":[
            {
                "Name": "Name",
                "Values": [
                    "MyStack"
                ]
            },
            {
                "Name": "Arn",
                "Values": [
                    "arn:aws:cloudformation:us-
east-1:123456789012:stack/MyStack/<stack-id>"
                ]
            }
        ]
    }
```

```
]
```

AWS::EC2::CapacityReservationPool

此Configuration類型指定資源群組代表群組成員所提供的一般容量集區。此資源群組的成員必須是 Amazon EC2 容量保留。資源群組可包含您在帳戶中擁有的產能保留，以及使用從其他帳號與您共用的產能保留 AWS Resource Access Manager。這可讓您使用此資源群組作為容量保留參數的值來啟動 Amazon EC2 執行個體。執行此操作時，執行個體會使用群組中的可用保留容量。如果資源群組沒有可用容量，則執行個體會以集區外的獨立隨需執行個體的形式啟動。如需詳細資訊，請參閱 Amazon EC2 使用者指南中的使用容量保留群組。

如果您使用此類型的Configuration項目設定服務連結資源群組，則也必須使用下列值指定個別Configuration項目：

- 具有一個參數的AWS::ResourceGroups::Generic類型：
  - 參數allowed-resource-types和的單一值AWS::EC2::CapacityReservation。這可確保只有 Amazon EC2 容量保留可以成為資源群組的成員。

群組設定中的AWS::EC2::CapacityReservationPool項目不支援任何參數。

下面的例子顯示了這樣的組的Configuration部分是什麼樣子。

```
[
    {
        "Type": "AWS::EC2::CapacityReservationPool"
    },
    {
        "Type": "AWS::ResourceGroups::Generic",
        "Parameters": [
            {
                "Name": "allowed-resource-types",
                "Values": [ "AWS::EC2::CapacityReservation" ]
            }
        ]
    }
]
```

AWS::EC2::HostManagement

此識別碼指定 Amazon EC2 主機管理的設定 AWS License Manager ，並針對群組的成員強制執行。如需詳細資訊，請參閱中的主機資源群組 AWS License Manager。

如果您使用此類型的Configuration項目設定服務連結資源群組，則也必須使用下列值指定個別Configuration項目：

- 具有參數allowed-resource-types且單一值為的AWS::ResourceGroups::Generic類型AWS::EC2::Host。這可確保只有 Amazon EC2 專用主機可以成為群組的成員。
- 具有參數deletion-protection且單一值為的AWS::ResourceGroups::Generic類型UNLESS_EMPTY。如此可確保除非群組為空，否則無法刪除群組。

AWS::EC2::HostManagement服務連結群組類型支援下列參數。

- **auto-allocate-host**

  此參數指定執行處理是啟動到特定專用主機，還是啟動到具有相符組態的任何可用主機上。如需詳細資訊，請參閱 Amazon EC2 使用者指南中的了解自動放置和親和性。

  值的資料類型：布林

  允許的值：「真」或「假」（必須是小寫）。

  必要：否

```
[
    {
        "Type": "AWS::EC2::HostManagement",
        "Parameters": [
            {
                "Name": "auto-allocate-host",
                "Values": [ "true" ]
            },
            {
                "Name": "any-host-based-license-configuration",
                "Values": ["true"]
            }
        ]
    },
    {
```

```
        "Type": "AWS::ResourceGroups::Generic",
        "Parameters": [
            {
                "Name": "allowed-resource-types",
                "Values": [ "AWS::EC2::Host" ]
            },
            {
                "Name": "deletion-protection",
                "Values": [ "UNLESS_EMPTY" ]
            }
        ]
    }
]
```

- **auto-release-host**

  此參數指定群組中的專用主機是否在其上次執行的執行個體終止後自動釋放。如需詳細資訊，請參閱 Amazon EC2 使用者指南中的釋放專用主機。

  值的資料類型：布林

  允許的值：「真」或「假」（必須是小寫）。

  必要：否

```
[
    {
        "Type": "AWS::EC2::HostManagement",
        "Parameters": [
            {
                "Name": "auto-release-host",
                "Values": [ "false" ]
            },
            {
                "Name": "any-host-based-license-configuration",
                "Values": ["true"]
            }
        ]
    },
    {
        "Type": "AWS::ResourceGroups::Generic",
        "Parameters": [
            {
```

```
                "Name": "allowed-resource-types",
                "Values": [ "AWS::EC2::Host" ]
            },
            {
                "Name": "deletion-protection",
                "Values": [ "UNLESS_EMPTY" ]
            }
        ]
    }
]
```

- **allowed-host-families**

  此參數指定做為此群組成員的例證可使用哪些例證類型族群。

  值的數據類型：字符串數組。

  允許的值：每個都必須是有效的 Amazon EC2 執行個體類型系列識別碼C4，例如M5P3dn、、或R5d。

  必要：否

  下列範例組態項目指定啟動的執行個體只能是 C5 或 M5 執行個體類型系列的成員。

```
[
    {
        "Type": "AWS::EC2::HostManagement",
        "Parameters": [
            {
                "Name": "allowed-host-families",
                "Values": ["c5", "m5"]
            },
            {
                "Name": "any-host-based-license-configuration",
                "Values": ["true"]
            }
        ]
    },
    {
        "Type": "AWS::ResourceGroups::Generic",
        "Parameters": [
            {
                "Name": "allowed-resource-types",
```

```
                "Values": ["AWS::EC2::Host"]
            },
            {
                "Name": "deletion-protection",
                "Values": ["UNLESS_EMPTY"]
            }
        ]
    }
]
```

- **allowed-host-based-license-configurations**

  此參數指定您要套用至群組成員的一或多個以核心/通訊端為基礎的授權組態的 Amazon 資源名稱 (ARN) 路徑。

  值的資料類型：陣列ARNs。

  允許的值：每個都必須是有效的 L icense Manager 組態ARN。

  必要：有條件限制。您必須指定此參數或any-host-based-license-configuration，但不能同時指定兩者。它們是相互排斥的。

  下列範例組態項目指定群組成員可以使用兩個指定的 License Manager 組態。

```
[
    {
        "Type": "AWS::EC2::HostManagement",
        "Parameters": [
            {
                "Name": "allowed-host-based-license-configurations",
                "Values": [
                    "arn:aws:license-manager:us-west-2:123456789012:license-
configuration:lic-6eb6586f508a786a2ba41EXAMPLE1111",
                    "arn:aws:license-manager:us-west-2:123456789012:license-
configuration:lic-8a786a26f50ba416eb658EXAMPLE2222"
                ]
            }
        ]
    },
    {
        "Type": "AWS::ResourceGroups::Generic",
        "Parameters": [
            {
```

```
                "Name": "allowed-resource-types",
                "Values": [ "AWS::EC2::Host" ]
            },
            {
                "Name": "deletion-protection",
                "Values": [ "UNLESS_EMPTY" ]
            }
        ]
    }
]
```

- **any-host-based-license-configuration**

  此參數指定您不想將特定授權組態與群組相關聯。在這種情況下，所有基於核心/通訊端的授權配置都可供您的主機資源群組的成員使用。如果您擁有無限數量的授權，並且想要針對主機使用率進行最佳化，請使用此設定。

  值的資料類型：布林

  允許的值：「真」或「假」（必須是小寫）。

  必要：有條件限制。您必須指定此參數或allowed-host-based-license-configurations，但不能同時指定兩者。它們是相互排斥的。

  下列範例組態項目指定群組成員可以使用任何以核心/通訊端為基礎的授權組態。

```
[
    {
        "Type": "AWS::EC2::HostManagement",
        "Parameters": [
            {
                "Name": "any-host-based-license-configuration",
                "Values": ["true"]
            }
        ]
    },
    {
        "Type": "AWS::ResourceGroups::Generic",
        "Parameters": [
            {
                "Name": "allowed-resource-types",
                "Values": ["AWS::EC2::Host"]
            },
```

```
            {
                "Name": "deletion-protection",
                "Values": ["UNLESS_EMPTY"]
            }
        ]
    }
]
```

下列範例說明如何將所有主機管理設定併入單一組態中。

```
[
    {
        "Type": "AWS::EC2::HostManagement",
        "Parameters": [
            {
                "Name": "auto-allocate-host",
                "Values": ["true"]
            },
            {
                "Name": "auto-release-host",
                "Values": ["false"]
            },
            {
                "Name": "allowed-host-families",
                "Values": ["c5", "m5"]
            },
            {
                "Name": "allowed-host-based-license-configurations",
                "Values": [
                    "arn:aws:license-manager:us-west-2:123456789012:license-
configuration:lic-6eb6586f508a786a2ba41EXAMPLE1111",
                    "arn:aws:license-manager:us-west-2:123456789012:license-
configuration:lic-8a786a26f50ba416eb658EXAMPLE2222"
                ]
            }
        ]
    },
    {
        "Type": "AWS::ResourceGroups::Generic",
        "Parameters": [
            {
                "Name": "allowed-resource-types",
```

```
                "Values": ["AWS::EC2::Host"]
            },
            {
                "Name": "deletion-protection",
                "Values": ["UNLESS_EMPTY"]
            }
        ]
    }
]
```

AWS::NetworkFirewall::RuleGroup

此識別碼會指定為群組成員強制執行的 AWS Network Firewall 規則群組設定。防火牆管理員可以指定此類型ARN的資源群組，以針對防火牆規則自動解析群組成員的 IP 位址，而不必手動列出每個位址。如需詳細資訊，請參閱中 AWS Network Firewall使用以標籤為基礎的資源群組。

您可以使用 Network Firewall 主控台或執行 AWS CLI 命令或 AWS SDK作業來建立此組態類型的資源群組。

此配置類型的資源群組具有下列限制：

- 群組的成員僅包含 Network Firewall 支援的類型資源。
- 群組必須包含以標籤為基礎的查詢，才能管理群組的成員資格；任何支援類型且標籤符合查詢的資源都會自動成為群組的成員。
- 此組態類型不`Parameters`受支援。
- 若要刪除此組態類型的資源群組，任何 Network Firewall 規則群組都無法參考該群組。

下列範例說明此類型之群組的`Configuration`和`ResourceQuery`區段。

```
{
    "Configuration": [
        {
            "Type": "AWS::NetworkFirewall::RuleGroup",
            "Parameters": []
        }
    ],
    "ResourceQuery": {
        "Query": "{\"ResourceTypeFilters\":[\"AWS::EC2::Instance\"],\"TagFilters\":
[{\"Key\":\"environment\",\"Values\":[\"production\"]}]}",
        "Type": "TAG_FILTERS_1_0"
```

```
    }
}
```

下列範例 AWS CLI 命令會使用先前的設定和查詢建立資源群組。

```
$ aws resource-groups create-group \
    --name test-group \
    --resource-query '{"Type": "TAG_FILTERS_1_0", "Query": "{\"ResourceTypeFilters\":
 [\"AWS::EC2::Instance\"], \"TagFilters\": [{\"Key\": \"environment\", \"Values\":
 [\"production\"]}]}"}' \
    --configuration '[{"Type": "AWS::NetworkFirewall::RuleGroup", "Parameters": []}]'
{
    "Group":{
        "GroupArn":"arn:aws:resource-groups:us-west-2:123456789012:group/test-group",
        "Name":"test-group",
        "OwnerId":"123456789012"
    },
    "Configuration": [
        {
            "Type": "AWS::NetworkFirewall::RuleGroup",
            "Parameters": []
        }
    ],
    "ResourceQuery": {
        "Query": "{\"ResourceTypeFilters\":[\"AWS::EC2::Instance\"],\"TagFilters\":
[{\"Key\":\"environment\",\"Values\":[\"production\"]}]}",
        "Type": "TAG_FILTERS_1_0"
    }
}
```

建立以查詢為基礎的群組 AWS Resource Groups

資源群組查詢的類型

在中 AWS Resource Groups，查詢是以查詢為基礎的群組的基礎。您可以讓資源群組以以下兩個類型查詢中的一個為基礎。

以標籤為基礎

以標籤為基礎的查詢包括以下列格AWS::*service*::*resource*式指定的資源類型清單和標籤。標籤為索引鍵，可幫助識別和排序組織中的資源。標籤選擇性地包含索引鍵的值。

針對以標籤為基礎的查詢，您也可以指定您要其成為群組成員的資源所共用的標籤。例如，如果您想要建立一個資源群組，其中包含您用來EC2執行應用程式測試階段的所有 Amazon 執行個體和 Amazon S3 儲存貯體，並且擁有以此方式標記的執行個體AWS::EC2::Instance和值區，請從下拉式清單中選擇和AWS::S3::Bucket資源類型，然後指定標籤值的標籤金鑰**StageTest**。

以標籤為基礎的資源群組的ResourceQuery參數語法包含下列元素：

- Type

  此元素會指出定義此資源群組的查詢類型。若要建立以標籤為基礎的資源群組，請指定值TAG_FILTERS_1_0，如下所示：

  ```
  "Type": "TAG_FILTERS_1_0"
  ```

- Query

  這個元素會定義用來比對資源的實際查詢。它包含具有以下元素的JSON結構的字符串表示：

  - ResourceTypeFilters

    此元素將結果限制為僅符合篩選條件的資源類型。您可以指定下列值：

    - "AWS::AllSupported"— 指定結果可包含符合查詢且 Resource Groups 服務目前支援之任何類型的資源。
    - "AWS::*service-id*::*resource-type*— 以逗號分隔的資源類型規格字串清單，其格式為：，例如。"AWS::EC2::Instance"

  - TagFilters

此元素指定與附加到資源的標籤進行比較的鍵/值字符串對。那些具有標籤鍵和符合篩選條件的值會包含在群組中。每個過濾器都由以下元素組成：

- "Key"— 具有金鑰名稱的字串。只有具有符合索引鍵名稱之標籤的資源才符合篩選器，而且是群組的成員。
- "Values"— 以逗號分隔的指定索引鍵值清單的字串。只有具有相符標籤鍵和符合此清單中一個值的資源才會是群組的成員。

所有這些JSON元素都必須組合成JSON結構的單行字符串表示。例如，考慮一個Query具有以下示例JSON結構。此查詢旨在僅比對具有標籤「Stage」且值為「Test」的 Amazon EC2 執行個體。

```
{
    "ResourceTypeFilters": [ "AWS::EC2::Instance" ],
    "TagFilters": [
        {
            "Key": "Stage",
            "Values": [ "Test" ]
        }
    ]
}
```

可JSON以表示為以下單行字符串，並用作Query元素的值。因為JSON結構的值必須是雙引號字串，因此您必須在每個字元前加上反斜線，以逸出任何內嵌的雙引號字元或正斜線字元，如下所示：

```
"Query":"{\"ResourceTypeFilters\":[\"AWS::AllSupported\"],\"TagFilters\":[{\"Key\":
\"Stage\",\"Values\":[\"Test\"]}]}"
```

然後將完整的ResourceQuery字串表示為CLI指令參數，如下所示：

```
--resource-query '{"Type":"TAG_FILTERS_1_0","Query":"{\"ResourceTypeFilters\":
[\"AWS::AllSupported\"],\"TagFilters\":[{\"Key\":\"Stage\",\"Values\":[\"Test
\"]}]}"}'
```

AWS CloudFormation 基於堆棧

在以 AWS CloudFormation 堆 AWS CloudFormation 疊為基礎的查詢中，您可以在目前區域的帳戶中選擇一個堆疊，然後在堆疊中選擇要加入群組的資源類型。您只能以一個 AWS CloudFormation 堆疊為基礎查詢。

> **Note**
>
> AWS CloudFormation 堆棧可以包含其他 AWS CloudFormation 「子」堆棧。但是，基於「父」堆棧的資源組不會將所有子堆棧的資源作為組成員獲取。資源群組會將子堆疊新增至父系堆疊的資源群組，做為單一群組成員，而不會展開它們。

Resource Groups 支援根據具有下列其中一種狀態的 AWS CloudFormation 堆疊進行查詢。

- `CREATE_COMPLETE`
- `CREATE_IN_PROGRESS`
- `DELETE_FAILED`
- `DELETE_IN_PROGRESS`
- `REVIEW_IN_PROGRESS`

> **Important**
>
> 只有直接建立為查詢堆疊一部分的資源才會包含在資源群組中。之後由 AWS CloudFormation 堆疊成員建立的資源不會成為群組的成員。例如，如果自動調整資源群組是 AWS CloudFormation 由堆疊的一部分建立，則該 auto-scaling 群組就是群組的成員。不過，由該 auto-scaling 群組建立的 Amazon EC2 執行個體做為其作業的一部分，並不是 AWS CloudFormation 堆疊型資源群組的成員。

如果您根據 AWS CloudFormation 堆疊建立群組，而堆疊的狀態會變更為不再支援做為群組查詢的基礎 (例如`DELETE_COMPLETE`，資源群組仍然存在，但沒有成員資源)。

建立資源群組後，您可以對群組中的資源執行工作。

CloudFormation 堆疊型資源群組的`ResourceQuery`參數語法包含下列元素：

- `Type`

  此元素會指出定義此資源群組的查詢類型。

  若要建立 AWS CloudFormation 以堆疊為基礎的資源群組，請指定值`CLOUDFORMATION_STACK_1_0`，如下所示：

```
"Type": "CLOUDFORMATION_STACK_1_0"
```

- `Query`

  這個元素會定義用來比對資源的實際查詢。它包含具有以下元素的JSON結構的字符串表示：

  - `ResourceTypeFilters`

    此元素將結果限制為僅符合篩選條件的資源類型。您可以指定下列值：

    - `"AWS::AllSupported"`— 指定結果可包含符合查詢之任何類型的資源。
    - `"AWS::`*`service-id`*`::`*`resource-type`*— 以逗號分隔的資源類型規格字串清單，其格式為：，例如。`"AWS::EC2::Instance"`

  - `StackIdentifier`

    此元素指定要包含在群組中的資源之 AWS CloudFormation 堆疊的 Amazon 資源名稱 (ARN)。

所有這些JSON元素都必須組合成JSON結構的單行字符串表示。例如，考慮一個`Query`具有以下示例JSON結構。此查詢僅比對屬於指定 AWS CloudFormation 堆疊一部分的 Amazon S3 儲存貯體。

```
{
    "ResourceTypeFilters": [ "AWS::S3::Bucket" ],
    "StackIdentifier": "arn:aws:cloudformation:us-
west-2:123456789012:stack/MyCloudFormationStackName/fb0d5000-aba8-00e8-
aa9e-50d5cEXAMPLE"
}
```

可JSON以表示為以下單行字符串，並用作`Query`元素的值。因為JSON結構的值必須是雙引號字串，因此您必須在每個字元前加上反斜線，以逸出任何內嵌的雙引號字元或正斜線字元，如下所示：

```
"Query":"{\"ResourceTypeFilters\":[\"AWS::S3::Bucket\"],\"StackIdentifier\":
\"arn:aws:cloudformation:us-west-2:123456789012:stack\/MyCloudFormationStackName\/
fb0d5000-aba8-00e8-aa9e-50d5cEXAMPLE\"
```

然後將完整的`ResourceQuery`字串表示為CLI指令參數，如下所示：

```
--resource-query '{"Type":"CLOUDFORMATION_STACK_1_0","Query":"{\"ResourceTypeFilters
\":[\"AWS::S3::Bucket\"],\"StackIdentifier\":\"arn:aws:cloudformation:us-
west-2:123456789012:stack\/MyCloudFormationStackName\/fb0d5000-aba8-00e8-
aa9e-50d5cEXAMPLE\"}'
```

建立以標籤為基礎的查詢並建立群組

下列程序說明如何建立以標籤為基礎的查詢，並使用它來建立資源群組。

Console

1. 登入 AWS Resource Groups 主控台。
2. 在功能窗格中，選擇 [建立資源群組]。
3. 在 [建立查詢型群組] 頁面的 [群組類型] 下，選擇 [標記型群組類型]。
4. 在 [分組準則] 底下，選擇您要加入資源群組的資源類型。您在查詢中最多可以有 20 個資源類型。對於本逐步解說，請選擇AWS::EC2: 執行個體和:: S3AWS:: 儲存貯體。
5. 仍在「分組條件」下，對於「標籤」，指定標籤鍵或標籤鍵和值配對，以限制相符資源僅包含使用指定值標記的資源。完成標籤時，選擇 Add (新增) 或按下 Enter 鍵。在這個範例中，對擁有 Stage (階段) 標籤索引鍵的資源進行篩選。標籤值是選用的，但可以進一步縮小查詢的結果。您可以在標籤值之間加入OR運算子，為標籤鍵新增多個值。若要新增更多標籤，請選擇 Add (新增)。查詢會將 AND 運算子指派至標籤，因此，查詢會傳回符合指定資源類型和所有指定標籤的任何資源。
6. 仍在 [分組準則] 下方，選擇 [預覽群組資源] 以傳回帳戶中符合指定標籤金鑰的EC2執行個體和 S3 儲存貯體清單。
7. 取得所需結果後，請根據此查詢建立群組。

   a. 在 [群組詳細資料] 下，對於 [群組名稱]，輸入資源群組的名稱。

      資源群組名稱最多可有 128 個字元，包括字母、數字、連字號、句點和底線。名稱開頭不可是 AWS 或 aws。這些是預留字。資源群組名稱在您帳戶的目前區域中必須是唯一的。

   b. (選用) 在 Group description (群組描述) 中，輸入群組的描述。

   c. (選用) 在 Group tags (群組標籤) 中，新增只適用於資源群組 (而非群組中的成員資源) 的標籤索引鍵和值組。

      如果您計劃讓此群組成為更大群組的成員，則群組標籤很有用。因為建立群組需要指定至少一個標籤索引鍵，請確保在 Group tags (群組標籤) 中將至少一個標籤索引鍵新增至您計劃要巢狀組合成更大群組的群組。

8. 完成後，請選擇 [建立群組]。

AWS CLI & AWS SDKs

以標籤為基礎的群組是根據類型 TAG_FILTERS_1_0 的查詢。

1. 在 AWS CLI 工作階段中，輸入下列命令，然後按 Enter 鍵，以您自己的名稱、說明、資源類型、標籤索引鍵和標籤值取代值。描述最多可有 512 個字元，包括字母、數字、連字號、底線、標點符號和空格。您在查詢中最多可以有 20 個資源類型。資源群組名稱最多可有 128 個字元，包括字母、數字、連字號、句點和底線。名稱開頭不可是 AWS 或 aws。這些是預留字。資源群組名稱在您的帳戶中必須是唯一的。

   ResourceTypeFilters 至少需要一個值。若要指定所有資源類型，請使用 AWS::AllSupported 作為 ResourceTypeFilters 值。

   ```
   $ aws resource-groups create-group \
       --name resource-group-name \
       --resource-query '{"Type":"TAG_FILTERS_1_0","Query":"{\"ResourceTypeFilters
   \":[\"resource_type1\",\"resource_type2\"],\"TagFilters\":[{\"Key\":\"Key1\",
   \"Values\":[\"Value1\",\"Value2\"]},{\"Key\":\"Key2\",\"Values\":[\"Value1\",
   \"Value2\"]}]}"}'
   ```

   下列是範例命令。

   ```
   $ aws resource-groups create-group \
       --name my-resource-group \
       --resource-query '{"Type":"TAG_FILTERS_1_0","Query":"{\"ResourceTypeFilters
   \":[\"AWS::EC2::Instance\"],\"TagFilters\":[{\"Key\":\"Stage\",\"Values\":
   [\"Test\"]}]}"}'
   ```

   以下命令為包含所有支援的資源類型的範例。

   ```
   $ aws resource-groups create-group \
       --name my-resource-group \
       --resource-query '{"Type":"TAG_FILTERS_1_0","Query":"{\"ResourceTypeFilters
   \":[\"AWS::AllSupported\"],\"TagFilters\":[{\"Key\":\"Stage\",\"Values\":[\"Test
   \"]}]}"}'
   ```

2. 以下是回應命令而傳回的。

   - 您已建立之群組的完整說明。
   - 您用來建立群組的資源查詢。

- 與群組相關聯的標籤。

建立 AWS CloudFormation 以堆疊為基礎的群組

下列程序說明如何建置以堆疊為基礎的查詢，並使用它來建立資源群組。

Console

1. 登入 AWS Resource Groups 主控台。
2. 在功能窗格中，選擇 [建立資源群組]。
3. 在 [建立查詢型群組] 上的 [群組類型] 下，選擇CloudFormation 堆疊型群組類型。
4. 選擇您想要成為您的群組基礎的堆疊。一個資源群組只能根據一個堆疊。若要篩選堆疊的清單，請從輸入堆疊的名稱開始。只有具有支援狀態的堆疊會顯示在清單中。
5. 選擇堆疊中您想要包含在群組中的資源類型。針對此逐步解說，保留預設值，All supported resource types (所有支援的資源類型)。如需支援及可在群組中的資源類型的詳細資訊，請參閱可與標籤編輯器搭配使用 AWS Resource Groups 的資源類型。
6. 選擇檢視群組資源以傳回 AWS CloudFormation 堆疊中符合所選資源類型的資源清單。
7. 取得所需結果後，請根據此查詢建立群組。

   a. 在 [群組詳細資料] 下，對於 [群組名稱]，輸入資源群組的名稱。

      資源群組名稱最多可有 128 個字元，包括字母、數字、連字號、句點和底線。名稱開頭不可是 AWS 或 aws。這些是預留字。資源群組名稱在您帳戶的目前區域中必須是唯一的。

   b. (選用) 在 Group description (群組描述) 中，輸入群組的描述。

   c. (選用) 在 Group tags (群組標籤) 中，新增只適用於資源群組 (而非群組中的成員資源) 的標籤索引鍵和值組。

      如果您計劃讓此群組成為更大群組的成員，則群組標籤很有用。因為建立群組需要指定至少一個標籤索引鍵，請確保在 Group tags (群組標籤) 中將至少一個標籤索引鍵新增至您計劃要巢狀組合成更大群組的群組。

8. 完成後，請選擇 [建立群組]。

AWS CLI & AWS SDKs

AWS CloudFormation 以堆疊為基礎的群組是以類型`CLOUDFORMATION_STACK_1_0`的查詢為基礎。

1. 執行下列命令，以您自己的指令取代群組名稱、描述、堆疊識別碼和資源類型的值。描述最多可有 512 個字元，包括字母、數字、連字號、底線、標點符號和空格。

   如果未指定資源類型，Resource Groups 會在堆疊中包含所有支援的資源類型。您在查詢中最多可以有 20 個資源類型。資源群組名稱最多可有 128 個字元，包括字母、數字、連字號、句點和底線。名稱開頭不可是 AWS 或 aws。這些是預留字。資源群組名稱在您的帳戶中必須是唯一的。

   所以此 *stack_identifier* 是堆疊ARN，如範例指令所示。

   ```
   $ aws resource-groups create-group \
       --name group_name \
       --description "description" \
       --resource-query
    '{"Type":"CLOUDFORMATION_STACK_1_0","Query":"{\"StackIdentifier\":
   \"stack_identifier\",\"ResourceTypeFilters\":[\"resource_type1\",
   \"resource_type2\"]}"}'
   ```

   下列是範例命令。

   ```
   $ aws resource-groups create-group \
       --name My-CFN-stack-group \
       --description "My first CloudFormation stack-based group" \
       --resource-query
    '{"Type":"CLOUDFORMATION_STACK_1_0","Query":"{\"StackIdentifier\":
   \"arn:aws:cloudformation:us-west-2:123456789012:stack\/AWStestuseraccount\/
   fb0d5000-aba8-00e8-aa9e-50d5cEXAMPLE\",\"ResourceTypeFilters\":
   [\"AWS::EC2::Instance\",\"AWS::S3::Bucket\"]}"}'
   ```

2. 以下是回應命令而傳回的。

   - 您已建立之群組的完整說明。
   - 您用來建立群組的資源查詢。

更新群組於 AWS Resource Groups

若要更新 Resource Groups 中以標籤為基礎的資源群組，您可以編輯做為群組基礎的查詢和標籤。您只能透過套用查詢或標籤的變更，從群組中新增和移除資源。您無法選取要新增至群組或從群組中移除的特定資源。在群組中新增或移除特定資源的最佳方式是編輯資源的標籤。然後確認您的資源群組標籤查詢是否包含或省略標籤，具體取決於您是否要在群組中使用資源。

若要更新以 AWS CloudFormation 堆疊為基礎的資源群組，您可以選擇不同的堆疊。您也可以從堆疊中新增或移除要成為群組一部分的資源類型。若要變更堆疊中可用的資源，請更新用來建立堆疊的 AWS CloudFormation 範本，然後在中更新堆疊 AWS CloudFormation。如需有關如何更新 AWS CloudFormation 堆AWS CloudFormation 疊的詳細資訊，請參閱AWS CloudFormation 使用者指南中的堆疊更新。

在中 AWS CLI，您可以使用兩個指令更新群組。

- `update-group`，您會執行此命令來更新群組說明。
- `update-group-query`，您會執行此命令來更新資源查詢和標籤，標籤會決定群組成員的資源。

在主控台中，您無法將 AWS CloudFormation 堆疊型群組變更為以標籤為基礎的查詢群組，反之亦然。但是，您可以使用 Resource Groups 來執行此操作API，包括在 AWS CLI.

更新標籤式查詢群組

下列程序說明如何更新以標籤為基礎的查詢群組。

Console

變更群組所依據的查詢中的資源類型或標籤，來更新以標籤為基礎的群組。您也可以新增或變更群組的描述。

1. 登入 AWS Resource Groups 主控台。
2. 在功能窗格的 [儲存的 Resource Groups] 下，選擇群組的名稱，然後選擇 [編輯]。

> **Note**
>
> 您只能更新您擁有的資源群組。[擁有者] 欄會顯示每個資源群組的帳號擁有權。除了您登入的帳戶擁有者以外的任何群組，都會在其中建立 AWS License Manager。如需詳

細資訊，請參閱《L icense Manager 使用指南》AWS License Manager中的〈主機資源群組〉。

3. 在 [編輯群組] 頁面的 [分組條件] 下，新增或移除資源類型。您在查詢中最多可以有 20 個資源類型。若要移除資源類型，選擇資源類型標籤上的 X。選擇 View group resources (檢視群組資源) 以查看該變更如何影響您的資源群組成員。在本逐步解說中，我們將資源類型AWS:RDS::新增DBInstance至查詢。
4. 仍在「分組準則」下，依需要編輯標籤。在這個範例中，我們對擁有 Stage (階段) 標籤索引鍵的資源進行篩選並新增 Test (測試) 的標籤值。標籤值是選用的，但可以進一步縮小查詢的結果。若要移除標籤，請選擇標籤的標記上的 X。
5. 在 Additional information (其他資訊) 區域，您可以編輯群組描述。您不能在群組建立後編輯群組的名稱。
6. (選擇性) 在群組標籤中，您可以新增或移除標記。群組標籤是有關資源群組的中繼資料。他們不會影響成員資源。若要變更資源群組查詢傳回的資源，請編輯 [分組條件] 下找到的標籤。

   如果您計劃讓此群組成為更大群組的成員，則群組標籤很有用。建立群組至少需要指定標籤金鑰。因此，請務必至少在群組標籤中新增標籤鍵至少到您打算巢狀成較大群組的群組。
7. 選擇預覽群組資源以擷取帳戶中符合指定標籤金鑰的更新執行個體、S3 儲存貯體和 Amazon 資RDS料庫執行個體清單。EC2如果您沒有在預期的清單中看到資源，請確定系統使用您在 Grouping criteria (群組條件) 中指定之標籤為資源加上標籤。
8. 完成時，請選擇 Save changes (儲存變更)。

AWS CLI & AWS SDKs

在中 AWS CLI，您可以使用兩個不同的命令來更新群組的查詢並更新資源群組的描述。您無法編輯現有群組的名稱。在中 AWS CLI，您可以將以標籤為基礎的群組變更為 CloudFormation 堆疊式群組，反之亦然。

1. 如果您不想要變更群組的說明，請略過此步驟並移至下一個步驟。在 AWS CLI 工作階段中，鍵入下列命令，然後按 Enter，將群組名稱和描述的值取代為您自己的值。

```
$ aws resource-groups update-group \
    --group-name resource-group-name \
    --description "description_text"
```

   下列是範例命令。

```
$ aws resource-groups update-group \
    --group-name my-resource-group \
    --description "EC2 instances, S3 buckets, and RDS DBs that we are using for
 the test stage."
```

此命令會傳回完整更新的群組說明。

2. 若要更新群組的查詢和標籤，請鍵入下列命令。將群組名稱、資源類型、標籤索引鍵和標籤值的值取代為您自己的值。然後預先輸入。您在查詢中最多可以有 20 個資源類型。

```
$ aws resource-groups update-group-query \
    --group-name resource-group-name \
    --resource-query '{"Type":"TAG_FILTERS_1_0","Query":"{\"ResourceTypeFilters
\":[\"resource_type1\",\"resource_type2\"],\"TagFilters\":[{\"Key\":\"Key1\",
\"Values\":[\"Value1\",\"Value2\"]},{\"Key\":\"Key2\",\"Values\":[\"Value1\",
\"Value2\"]}]}"}'
```

下列是範例命令。

```
$ aws resource-groups update-group-query \
    --group-name my-resource-group \
    --resource-query '{"Type":"TAG_FILTERS_1_0","Query":"{\"ResourceTypeFilters
\":[\"AWS::EC2::Instance\",\"AWS::S3::Bucket\",\"AWS::RDS::DBInstance\"],
\"TagFilters\":[{\"Key\":\"Stage\",\"Values\":[\"Test\"]}]}"}'
```

此命令會傳回更新的查詢做為結果。

更新 AWS CloudFormation 以堆疊為基礎的群組

下列程序說明如何更新以 CloudFormation 堆疊為基礎的群組。

Console

您無法將 AWS CloudFormation 堆疊式群組變更為中的以標籤為基礎的群組。 AWS Management Console不過，您可以變更群組所依據的堆疊，或變更要包含在群組中的堆疊資源類型。您也可以新增或變更群組的描述。

1. 登入 AWS Resource Groups 主控台。
2. 在功能窗格的 [儲存的資源群組] 下，選擇群組的名稱，然後選擇 [編輯]。

3.
> **Note**
>
> 您只能更新您擁有的資源群組。[擁有者] 欄會顯示每個資源群組的帳號擁有權。除了您登入的帳戶擁有者以外的任何群組，都會在其中建立 AWS License Manager。如需詳細資訊，請參閱《L icense Manager 使用指南》AWS License Manager中的〈主機資源群組〉。

4. 在 [編輯群組] 頁面的 [分組準則] 下，若要變更群組所依據的堆疊，請從下拉式清單中選擇堆疊。一個資源群組只能根據一個堆疊。若要篩選堆疊的清單，請從輸入堆疊的名稱開始。只有具有支援狀態的堆疊會顯示在清單中。如需支援的狀態的清單，請參閱本指南中的建立以查詢為基礎的群組 AWS Resource Groups。
5. 新增或移除資源類型。只有堆疊中可用的資源類型才會顯示在下拉式清單。預設值是 All supported resource types (所有支援的資源類型)。您在查詢中最多可以有 20 個資源類型。若要移除資源類型，選擇資源類型標籤上的 X。如需支援及可在群組中的資源類型的詳細資訊，請參閱可與標籤編輯器搭配使用 AWS Resource Groups 的資源類型。
6. 選擇 [預覽群組資源] 以擷取 AWS CloudFormation 堆疊中符合所選資源類型的資源清單。
7. 在 Additional information (其他資訊) 區域，您可以編輯群組描述。您不能在群組建立後編輯群組的名稱。
8. 在 Group tags (群組標籤) 中，新增或移除標籤。群組標籤是有關資源群組的中繼資料。他們不會影響成員資源。若要變更資源群組查詢傳回的資源，在 Grouping criteria (群組條件) 編輯標籤。

   如果您計劃讓此群組成為更大群組的成員，則群組標籤很有用。建立群組至少需要指定標籤金鑰。因此，請務必至少在群組標籤中新增標籤鍵至少到您打算巢狀成較大群組的群組。
9. 完成時，請選擇 Save changes (儲存變更)。

AWS CLI & AWS SDKs

在中 AWS CLI，您可以使用兩個不同的命令來更新群組的查詢並更新資源群組的描述。您無法編輯現有群組的名稱。在中 AWS CLI，您可以將以標籤為基礎的群組變更為 CloudFormation 堆疊式群組，反之亦然。

1. 如果您不想要變更群組的說明，請略過此步驟並移至下一個步驟。執行下列命令，以您自己的指令取代群組名稱和描述的值。

```
$ aws resource-groups update-group \
    --group-name "resource-group-name" \
```

```
    --description "description_text"
```

下列是範例命令。

```
$ aws resource-groups update-group \
    --group-name "My-CFN-stack-group" \
    --description "EC2 instances, S3 buckets, and RDS DBs that we are using for
 the test stage."
```

此命令會傳回完整更新的群組說明。

2. 若要更新群組的查詢和標記，請執行下列命令。將群組名稱、堆疊識別碼和資源類型的值取代為您自己的值。若要新增資源類型，請在命令中提供完整的資源類型清單，而不僅僅您要新增的資源類型。您在查詢中最多可以有 20 個資源類型。

   所以此 *stack_identifier* 是堆疊ARN，如範例指令所示。

```
$ aws resource-groups update-group-query \
    --group-name resource-group-name \
    --description "description" \
    --resource-query
 '{"Type":"CLOUDFORMATION_STACK_1_0","Query":"{\"StackIdentifier\":
\"stack_identifier\",\"ResourceTypeFilters\":[\"resource_type1\",
\"resource_type2\"]}"}'
```

   下列是範例命令。

```
$ aws resource-groups update-group-query \
    --group-name "my-resource-group" \
    --description "Updated CloudFormation stack-based group" \
    --resource-query
 '{"Type":"CLOUDFORMATION_STACK_1_0","Query":"{\"StackIdentifier\":
\"arn:aws:cloudformation:us-west-2:810000000000:stack\/AWStestuseraccount
\/fb0d5000-aba8-00e8-aa9e-50d5cEXAMPLE\",\"ResourceTypeFilters\":
[\"AWS::EC2::Instance\",\"AWS::S3::Bucket\"]}"}'
```

   此命令會傳回更新的查詢做為結果。

群組生命週期事件：監視資源群組的變更

使用 AWS Resource Groups 將資源組織成群組之後，您可以監視這些群組是否有作為事件公開給您的變更。您可以收到有關群組活動的通知，作為您採取某種行動的信號。例如，您可以設定每當群組成員資格變更時傳送的通知。您可以使用新增群組成員的事件來觸發 Lambda 函數，該函數會以程式設計方式檢閱變更，以確保新群組成員符合組織設定的合規要求。此類 Lambda 函數可針對未能滿足這些需求的任何新群組成員執行自動修復。移除群組成員所造成的事件可觸發 Lambda 函數，執行任何必要的清理，例如刪除連結的資源。

透過為資源群組開啟群組生命週期事件，您可以允許 Amazon 擷取群組變更的相關事件，EventBridge 並可供所有支 EventBridge 援的目標服務使用。然後，您可以將這些目標服務設定為自動採取您的案例所需的任何動作。這些目標包括各種 AWS 服務，例如 Amazon 簡單通知服務（AmazonSNS），Amazon 簡單隊列服務（AmazonSQS）和 AWS Lambda. 使用 Lambda 等服務，您的事件可以觸發程式設計回應，使用程式碼執行您需要的任何動作。有關可以使用目標 AWS 服務的列表 EventBridge，請參閱 Amazon EventBridge 用戶指南中的 Amazon EventBridge 目標。

當您開啟群組生命週期事件時， AWS Resource Groups 會建立下列項目：

- 一種 AWS Identity and Access Management （IAM）服務鏈接角色，具有監視您的資源是否對其標籤和堆棧對屬於 AWS CloudFormation 堆棧一部分的資源進行任何更改的權限。
- 「Resource Groups」受管 EventBridge 規則，可擷取資源的任何標籤或堆疊變更的詳細資料。EventBridge 使用此規則來通知 Resource Groups 有關這些變更的資訊。然後，Resource Groups 會產生要傳送的成員資格事件， EventBridge 供您的自訂規則處理。

服務連結角色只能由 Resource Groups 服務承擔。如需有關 Resource Groups 針對此功能所使用之服務連結角色的詳細資訊，請參閱對 Resource Groups 使用服務連結角色。

開啟此功能時，當您對 Resource Groups 進行下列任何變更時，資源群組會產生事件：

- 建立新的資源群組。
- 更新定義查詢式資源群組成員資格的查詢。
- 更新服務連結資源群組的組態。
- 更新資源群組的說明。
- 刪除資源群組。
- 從群組中新增或移除資源，以變更資源群組的成員資格。當標籤更改或 AWS CloudFormation 堆棧更改時，也可能會發生成員資格更改。

Important

- 若要成功接收並回應群組事件，您必須變更 Resource Groups 和 EventBridge。您可以按任何順序執行變更，但在您對這兩個服務進行變更之前，不會將群組事件發佈到 EventBridge 目標。
- 資源群組變更不包括對附加至資源群組本身的任何標籤所做的變更。若要根據群組的標籤變更產生事件，您必須使用使用來`aws.tag`源而非來`aws.resource-groups`源的 EventBridge 規則。如需詳細資訊，請參閱 Amazon EventBridge 使用者指南中的在AWS 資源上標記變更事件。

主題

開啟 Resource Groups 中的群組生命週期事件

若要接收有關資源群組生命週期變更的通知，您可以針對群組生命週期事件進行。然後，Resource Groups 會提供群組對 Amazon EventBridge 變更的相關資訊。在中 EventBridge，您可以使用您在 EventBridge 服務中定義的規則來評估變更並採取行動。

最低許可

若要在您的中開啟群組生命週期事件 AWS 帳戶，您必須使用下列權限以 AWS Identity and Access Management (IAM) 主體身分登入：

- `resource-groups:UpdateAccountSettings`
- `iam:CreateServiceLinkedRole`
- `events:PutRule`
- `events:PutTargets`
- `events:DescribeRule`

- events:ListTargetsByRule
- cloudformation:DescribeStacks
- cloudformation:ListStackResources
- tag:GetResources

當您一開始在中開啟群組生命週期事件時 AWS 帳戶，Resource Groups 會建立名為AWSServiceRoleForResourceGroups的服務連結角色。此受管理角色具有使用 Resource Groups 受管 EventBridge 規則的權限。此規則會監控附加至資源的標籤，以及帳戶中的 AWS CloudFormation 堆疊是否有任何變更。然後，Resource Groups 會將這些變更發佈到 Amazon 中的預設事件匯流排 EventBridge。此服務也會建立名為的 EventBridge 受管理規則Managed.ResourceGroups.TagChangeEvents。此規則會擷取資源標籤變更的詳細資訊。這可讓 Resource Groups 產生要傳送至的成員資格事件，以 EventBridge 供您的自訂規則處理。然後，您的 EventBridge 規則可以透過將通知傳送至規則設定的目標來回應事件。

完成這些步驟之後，尋找這些事件的規則應該會在幾分鐘內開始接收。

您可以使用或使用來自 AWS Management Console 或其中一個 SDK API 的命令來開啟群組生命週期事件。 AWS CLI

> **Note**
>
> 如果您的資源群組配額過高，則無法開啟群組生命週期事件。如需詳細資訊，請參閱檢視服務配額。

AWS Management Console

在 Resource Groups 主控台中開啟群組生命週期事件

1. 在 [Resource Groups] 主控台中開啟 [設定] 頁面。
2. 在「群組生命週期事件」區段中，選擇「通知已關閉」旁的開關。
3. 在確認對話方塊中，選擇 [開啟通知]。

   功能開關顯示通知已開啟。

這樣就完成了該過程的第一部分。開啟事件通知後，您可以在 Amazon 中建立規則來擷取 EventBridge事件並將事件傳送至特定 AWS 服務 事件進行處理。

AWS CLI

使用或 AWS SDK 開啟群組生命週期事 AWS CLI 件的步驟

下列範例顯示如何使用開啟 Resource Groups 中的群組生命週期事件。 AWS CLI 輸入具有服務主體參數的命令，如圖所示。輸出會同時顯示圖徵的目前狀態和所需的狀態。

```
$ aws resource-groups update-account-settings \
    --group-lifecycle-events-desired-status ACTIVE
{
    "AccountSettings": {
        "GroupLifecycleEventsDesiredStatus": "ACTIVE",
        "GroupLifecycleEventsStatus": "IN_PROGRESS"
    }
}
```

您可以執行下列範例命令來確認功能已開啟。如果兩個狀態欄位都顯示相同的值，則作業已完成。

```
$ aws resource-groups get-account-settings
{
    "AccountSettings": {
        "GroupLifecycleEventsDesiredStatus": "ACTIVE",
        "GroupLifecycleEventsStatus": "ACTIVE"
    }
}
```

如需詳細資訊，請參閱下列資源：

- AWS CLI — aws 資源群組和 aws 資源群 update-account-settings組 get-account-settings
- 應用程式介面UpdateAccountSettings及 GetAccountSettings

建立 EventBridge 規則以擷取群組生命週期事件並發佈通知

您可以為資源群組開啟群組生命週期事件，AWS Resource Groups以將事件發佈到 Amazon EventBridge。然後，您可以透過將這些事件傳送給其他事件以AWS 服務供進一步處理，來建立回應這些事件的 EventBridge規則。

AWS CLI

在 EventBridge 其中建立擷取事件並將事件傳送至所需目標服務的規則的程序會採用兩個獨立的 CLI 指令：

1. 建立規 EventBridge 則以擷取您想要的事件
2. 將可處理事件的目標附加至 EventBridge 規則

步驟 1：建立 EventBridge 規則以擷取事件

下列AWS CLIput-rule範例命令會建立擷取所有 Resource Groups 生命週期事件變更的 EventBridge 規則。

```
$ aws events put-rule \
    --name "CatchAllResourceGroupEvents" \
    --event-pattern '{"source":["aws.resource-groups"]}'
{
    "RuleArn": "arn:aws:events:us-east-1:123456789012:rule/
CatchAllResourceGroupEvents"
}
```

輸出包括新規則的 Amazon 資源名稱 (ARN)。

> **Note**
>
> 包含加引號字串的參數值會根據您使用的作業系統和殼層，具有不同的格式化規則。對於本指南中的示例，我們展示了在 Linux BASH 外殼上運行的命令。如需有關為其他作業系統 (例如 Windows 命令提示字元) 格式化字串的指示，請參閱《使用指南》中的〈在字串內使AWS Command Line Interface用引號〉。由於參數字串變得越來越複雜，接受來自文字檔案的參數值，而不是直接在命令列上輸入參數值，也會更容易出錯。

下列事件模式會將事件限制為只有與指定群組相關的事件 (由其 ARN 識別)。此事件模式是一個複雜的 JSON 字符串，當壓縮為單行，正確轉義的 JSON 字符串時，它的可讀性要低得多。您可以將其存儲在文件中。

將事件模式 JSON 字串儲存在檔案中。在下列程式碼範例中，檔案為eventpattern.txt。

```
{
```

```
    "source": [ "aws.resource-groups" ],
    "detail": {
        "group": {
            "arn": [ "my-resource-group-arn" ]
        }
    }
}
```

然後，發出以下命令以建立規則，從檔案擷取自訂事件模式。

```
$ aws events put-rule \
    --name "CatchResourceGroupEventsForMyGroup" \
    --event-pattern file://eventpattern.txt
{
    "RuleArn": "arn:aws:events:us-east-1:123456789012:rule/
CatchResourceGroupEventsForMyGroup"
}
```

若要擷取其他類型的 Resource Groups 事件，請使用類似區段中顯示的篩選器來取代`--event-pattern`字串針對不同使用案例的範例 EventBridge 自訂事件模式。

步驟 2：將可處理事件的目標附加至 EventBridge 規則

現在您有一個規則可擷取您感興趣的事件，您可以附加一或多個目標，以對事件執行某種類型的處理。

下列AWS CLI`put-targets`命令會附加 Amazon Simple Notification Service (Amazon SNS) 主題，命名`my-sns-topic`為您在上一個範例中建立的規則。當規則中指定的群組發生變更時，主題的所有訂閱者都會收到通知。

```
$ aws events put-targets \
    --rule CatchResourceGroupEventsForMyGroup \
    --targets Id=1,Arn=arn:aws:sns:us-east-1:123456789012:my-sns-topic
{
    "FailedEntryCount": 0,
    "FailedEntries": []
}
```

此時，任何與規則中事件模式相符的群組變更都會自動傳送至設定的一或多個目標。如前例所述，如果目標是 Amazon SNS 主題，則該主題的所有訂閱者都會收到包含事件的訊息，如中所述Resource Groups 生命週期事件的結構與語法。

如需詳細資訊，請參閱下列資源：

- AWS CLI— aws 事件放入規則和 aws 事件放置目標
- 應用程式介面PutRule及 PutTargets

建立規則以僅擷取特定群組生命週期事件類型

您可以使用自訂事件模式建立規則，該模式只會擷取您感興趣的事件。如需如何使用自訂事件模式篩選傳入事件的完整詳細資訊，請參閱 Amazon 使用 EventBridge 者指南中的 Amazon EventBridge 事件。

例如，假設您希望規則僅處理指示建立新 Resource Groups 的那些資源群組通知。您可以使用類似下列範例的自訂事件模式。

```
{
    "source": [ "aws.resource-groups" ],
    "detail-type": [ "ResourceGroups Group State Change" ],
    "detail": {
        "state-change": "create"
    }
}
```

該篩選器只會擷取在指定欄位中具有這些確切值的事件。如需可用欄位的完整清單，請參閱Resource Groups 生命週期事件的結構與語法。

關閉群組生命週期事件

您可以關閉群組生命週期事件，以停AWS Resource Groups止將事件傳送到 Amazon EventBridge。您可以使用，或使用來自AWS Management Console或其中一個 SDK API 的命令來執行此操作。AWS CLI

> **Note**
>
> 關閉群組生命週期事件會刪除用於掃描資源標籤和AWS CloudFormation堆疊中是否有變更的 Resource Groups 管理 EventBridge 規則。Resource Groups 無法再將這些變更傳遞給 EventBridge。您在 EventBridge 尋找 Resource Groups 事件時定義的任何規則都會停止接收要處理的事件。如果您打算在 future 再次開啟群組生命週期事件，您可以停用規則。若您不想再使用這些規則，您可以刪除它們。如需詳細資訊，請參閱 Amazon EventBridge 使用者指南中的停用或刪除 EventBridge 規則。

關閉群組生命週期事件並不會刪除服務連結角色。使用 IAM，您可以手動刪除服務連結角色。如果您稍後需要再次開啟群組生命週期事件，但服務連結角色不存在，則 Resource Groups 會自動重新建立該事件。

最低許可

若要關閉目前的群組生命週期事件AWS 帳戶，您必須使用下列權限以AWS Identity and Access Management (IAM) 主體身分登入：

- `resource-groups:UpdateAccountSettings`
- `events:DeleteRule`
- `events:RemoveTargets`
- `events:DescribeRule`
- `events:ListTargetsByRule`

AWS Management Console

關閉群組生命週期事件通知的步驟 EventBridge

1. 在 [Resource Groups] 主控台中開啟 [設定] 頁面。
2. 在「群組生命週期事件」區段中，選擇「通知已開啟」旁的開關。
3. 在確認對話方塊上，選擇關閉通知。

   顯示功能開關：事件通知已關閉。

此時，Resource Groups 不再將事件傳送至 EventBridge 預設事件匯流排，而且您不再接收要處理的群組通知事件的任何規則。您可以選擇刪除這些規則以完成清理。

AWS CLI

關閉群組生命週期事件通知的步驟 EventBridge

下列範例顯示如何使用來關閉 Resource Groups 中的群組生命週期事件。AWS CLI

```
$ aws resource-groups update-account-settings \
    ----group-lifecycle-events-desired-status INACTIVE
```

```
{
    "AccountSettings": {
        "GroupLifecycleEventsDesiredStatus": "INACTIVE",
        "GroupLifecycleEventsStatus": "INACTIVE"
    }
}
```

如需詳細資訊，請參閱下列資源：

- AWS CLI— aws 資源群組 update-account-settings和 aws 資源群組 get-account-settings
- API — UpdateAccountSettings和 GetAccountSettings

Resource Groups 生命週期事件的結構與語法

主題

- detail領域的結構
- 針對不同使用案例的範例 EventBridge 自訂事件模式

的生命週期事件 AWS Resource Groups 採用下列一般格式的JSON物件字串形式。

```
{
    "version": "0",
    "id": "08f00e24-2e30-ec44-b824-8acddf1ac868",
    "detail-type": "ResourceGroups Group ... Change",
    "source": "aws.resource-groups",
    "account": "123456789012",
    "time": "2020-09-29T09:59:01Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:resource-groups:us-east-1:123456789012:group/MyGroupName"
    ],
    "detail": {
        ...
    }
}
```

如需有關所有 Amazon EventBridge 事件通用欄位的詳細資訊，請參閱 Amazon EventBridge 使用者指南中的 Amazon EventBridge 事件。下表說明 Resource Groups 特有的詳細資訊。

欄位名稱	Type	描述
detail-type	字串	對於「Resource Groups」，detail-type 欄位永遠是下列其中一個值： • ResourceGroups Group State Change — 代表整體群組狀態及其內容的變更。 • ResourceGroups Group Membership Change— 代表群組成員資格的變更。
source	字串	對於 Resource Groups，此值一律為"aws.resource-groups" 。
resources	Amazon 資源名稱的數組（ARNs）	此欄位永遠包含群組的 Amazon 資源名稱 (ARN) 以及觸發此事件的變更。 如果適用，此欄位也可以包括新增至群組或從群組中移除ARNs的任何資源。
detail	JSON物件字串	這是事件的裝載。detail欄位的內容會根據的值而有所不同detail-type 。如需詳細資訊，請參閱下一節。

detail領域的結構

此detail欄位包含有關特定變更的所有 Resource Groups 服務特定詳細資料。根據上一節所述detail欄位的值，此欄位可採用兩種形式的其中一種，即群組狀態變更或成員資格變更。detail-type

> **Important**
>
> 這些事件中的資源群組由"unique-id"群組ARN和包含 UUID. 透過將作UUID為資源群組識別的一部分加入，您可以區分刪除的群組和稍後使用相同名稱建立的不同群組。我們建議您將ARN和唯一 ID 的串連視為程式中與這些事件互動之群組的索引鍵。

群組狀態變更

`"detail-type": "ResourceGroups Group State Change"`

此`detail-type`值表示群組本身的狀態 (包括其中繼資料) 已變更。建立、更新或刪除群組時，會發生此變更，如中的`"change"`欄位所指示`detail`。

指定此資訊時，`details`區段中包含`detail-type`的資訊包括下表所述的欄位。

欄位名稱	Type	描述
`event-sequence`	Double	單調遞增的數字，指定特定群組的事件順序。當您刪除群組並建立另一個具有相同名稱的群組時，編號會重設。
`group`	`Group`JSON物件	依照事件ARN、名稱和唯一 ID 與事件相關聯的群組物件。
`state-change`	字串	發生的狀態變更類型。可以是下列任一值： • `create` • `update` • `delete`
`old-state`	`GroupState` JSON物件	變更前的群組狀態。物件僅包含變更的性質值。
`new-state`	`GroupState` JSON物件	變更後的群組狀態。物件僅包含變更的性質值。

`group`JSON物件包含下表所述的元素。

欄位名稱	Type	描述
`arn`	字串	該ARN組的。
`name`	字串	群組的易記名稱。

欄位名稱	Type	描述
unique-id	GUID	一個唯一GUID值，用於區分已刪除的群組與稍後使用相同名稱和建立的不同群組。ARN在程式碼中使用這些事件時，請使用的串連ARN和這個值做為群組的唯一索引鍵。

GroupStateJSON物件包含下表所述的元素。

欄位名稱	Type	描述
description	字串	客戶提供的資源群組說明。
resource-query	ResourceQuery JSON物件	定義群組成員的查詢JSON表示法。此欄位僅適用於以查詢為基礎的群組。此欄位的語法由ResourceQuery API資料類型定義。此範例包含在「建立與更新」事件範例中。
group-configuration	Configuration JSON物件	與服務連結群組相關聯的組態參數的JSON表示。如需詳細資訊，請參閱AWS Resource Groups API參考資料中的資源群組的服務組態。

下列每個程式碼範例都會說明每個state-change類型的detail欄位內容。

建立

"state-change": "create"

此事件表示已建立新群組。此事件包含群組建立期間設定的所有群組中繼資料屬性。除非群組為空，否則此事件通常會接著其中一個以上的群組成員資格事件。具有 null 值的屬性不會顯示在事件主體中。

下列範例事件指出新建立的名為的資源群組my-service-group。在此範例中，群組使用標籤式查詢，該查詢僅與具有標籤"project"="my-service"的 Amazon 彈性運算雲端 (AmazonEC2) 執行個體相符。

```
{
    "version": "0",
    "id": "08f00e24-2e30-ec44-b824-8acddf1ac868",
```

```
    "detail-type": "ResourceGroups Group State Change",
    "source": "aws.resource-groups",
    "account": "123456789012",
    "time": "2020-09-29T09:59:01Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:resource-groups:us-east-1:123456789012:group/my-service-group"
    ],
    "detail": {
        "event-sequence": 1.0,
        "state-change": "create",
        "group": {
            "arn": "arn:aws:resource-groups:us-east-1:123456789012:group/my-service-
group",
            "name": "my-service-group",
            "unique-id": "3dd07ab7-3228-4410-8cdc-6c4a10fcceea"
        },
        "new-state": {
            "resource-query": {
                "type": "TAG_FILTERS_1_0",
                "query": "{
                    \"ResourceTypeFilters\": [\"AWS::EC2::Instance\"],
                    \"TagFilters\": [{\"Key\":\"project\", \"Values\":[\"my-service\"}]
                }"
            }
        }
    }
}
```

更新

`"state-change": "update"`

該事件表示現有組以某種方式進行了修改。此事件僅包含從先前狀態變更的屬性。未變更的屬性不會顯示在事件主體中。

下列範例事件指出上一個範例資源群組中的標籤式查詢已修改為同時在群組中包含 Amazon EC2 磁碟區資源。

```
{
    "version": "0",
    "id": "08f00e24-2e30-ec44-b824-8acddf1ac868",
    "detail-type": "ResourceGroups Group State Change",
```

```
    "source": "aws.resource-groups",
    "account": "123456789012",
    "time": "2020-09-29T09:59:01Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:resource-groups:us-east-1:123456789012:group/my-service-group"
    ],
    "detail": {
        "event-sequence": 3.0,
        "state-change": "update",
        "group": {
            "arn": "arn:aws:resource-groups:us-east-1:123456789012:group/my-service-
group",
            "name": "my-service",
            "unique-id": "3dd07ab7-3228-4410-8cdc-6c4a10fcceea"
        },
        "new-state": {
            "resource-query": {
                "type": "TAG_FILTERS_1_0",
                "query": "{
                    \"ResourceTypeFilters\": [\"AWS::EC2::Instance\",
 \"AWS::EC2::Volume\"],
                    \"TagFilters\": [{\"Key\":\"project\", \"Values\":[\"my-service\"}]
                }"
            }
        },
        "old-state": {
            "resource-query": {
                "type": "TAG_FILTERS_1_0",
                "query": "{
                    \"ResourceTypeFilters\": [\"AWS::EC2::Instance\"],
                    \"TagFilters\": [{\"Key\":\"Project\", \"Values\":[\"my-service\"}]
                }"
            }
        }
    }
}
```

Delete

`"state-change": "delete"`

此事件表示已刪除現有群組。除了識別之外，詳細資料欄位不包含任何關於群組的中繼資料。該event-sequence字段在此事件之後重置，因為它是根據定義，此arn和的最後一個事件unique-id。

```
{
    "version": "0",
    "id": "08f00e24-2e30-ec44-b824-8acddf1ac868",
    "detail-type": "ResourceGroups Group State Change",
    "source": "aws.resource-groups",
    "account": "123456789012",
    "time": "2020-09-29T09:59:01Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:resource-groups:us-east-1:123456789012:group/my-service"
    ],
    "detail": {
        "event-sequence": 4.0,
        "state-change": "delete",
        "group": {
            "arn": "arn:aws:resource-groups:us-east-1:123456789012:group/my-service",
            "name": "my-service",
            "unique-id": "3dd07ab7-3228-4410-8cdc-6c4a10fcceea"
        }
    }
}
```

團體成員變更

`"detail-type": "ResourceGroups Group Membership Change"`

此detail-type值表示群組的成員資格已由新增至群組或從群組中移除的資源而變更。指定detail-type此選項時，頂層resources欄位會包括已變更其成員資格的群組，以及新增至群組或從群組中移除的任何資源。ARN ARNs

指定此資訊時，details區段中包含detail-type的資訊包括下表所述的欄位。

欄位名稱	Type	描述
event-sequence	Double	單調遞增的數字，表示特定群組的事件順序。編號會在刪除群組且其唯一 ID 變更時重設。

欄位名稱	Type	描述
group	GroupJSON物件	按照事件ARN、名稱和唯一 ID 來識別與事件相關聯的群組物件。
resources	ResourceChange JSON物件陣列	群組成員資格已變更的資源陣列。 此ResourceChange 物件包含每個資源的下列欄位： • membership-change — 值為"add"或"remove"。 • arn— 新增或移除ARN的資源。 • resource-type — 新增或移除的資源類型。

下列程式碼範例會說明典型成員資格變更類型的事件內容。此範例顯示新增至群組的一個資源，以及一個從群組中移除的資源。

```
{
    "version": "0",
    "id": "08f00e24-2e30-ec44-b824-8acddf1ac868",
    "detail-type": "ResourceGroups Group Membership Change",
    "source": "aws.resource-groups",
    "account": "123456789012",
    "time": "2020-09-29T09:59:01Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:resource-groups:us-east-1:123456789012:group/my-service",
        "arn:aws:ec2:us-east-1:123456789012:instance/i-abcd1111",
        "arn:aws:ec2:us-east-1:123456789012:instance/i-efef2222"
    ],
    "detail": {
        "event-sequence": 2.0,
        "group": {
            "arn": "arn:aws:resource-groups:us-east-1:123456789012:group/my-service",
            "name": "my-service",
            "unique-id": "3dd07ab7-3228-4410-8cdc-6c4a10fcceea"
        },
        "resources": [
            {
```

```
                "membership-change": "add",
                "arn": "arn:aws:ec2:us-east-1:123456789012:instance/i-abcd1111",
                "resource-type": "AWS::EC2::Instance"
            },
            {
                "membership-change": "remove",
                "arn": "arn:aws:ec2:us-east-1:123456789012:instance/i-efef2222",
                "resource-type": "AWS::EC2::Instance"
            }
        ]
    }
}
```

針對不同使用案例的範例 EventBridge 自訂事件模式

下列範例 EventBridge 自訂事件模式會將 Resource Groups 所產生的事件篩選為僅針對特定事件規則和目標感興趣的事件。

在下列程式碼範例中，如果需要特定的群組或資源，請取代每個群組或資源 *user input placeholder* 使用您自己的信息。

所有 Resource Groups 事件

```
{
    "source": [ "aws.resource-groups" ]
}
```

群組狀態或成員資格變更事件

下列程式碼範例適用於所有群組狀態變更。

```
{
    "source": [ "aws.resource-groups" ],
    "detail-type": [ "ResourceGroups Group State Change " ]
}
```

下列程式碼範例適用於所有群組成員資格變更。

```
{
    "source": [ "aws.resource-groups" ],
    "detail-type": [ "ResourceGroups Group Membership Change" ]
```

```
}
```

特定群組的活動

```
{
    "source": [ "aws.resource-groups" ],
    "detail": {
        "group": {
            "arn": [ "my-group-arn" ]
        }
    }
}
```

上一個範例會擷取指定群組的變更。下列範例會執行相同動作，並在群組是另一個群組的成員資源時擷取變更。

```
{
    "source": [ "aws.resource-groups" ],
    "resources": [ "my-group-arn" ]
}
```

特定資源的事件

您只能篩選特定成員資源的群組成員資格變更事件。

```
{
    "source": [ "aws.resource-groups" ],
    "detail-type": [ "ResourceGroups Group Membership Change " ],
    "resources": [ "arn:aws:ec2:us-east-1:123456789012:instance/i-b188560f" ]
}
```

特定資源類型的事件

您可以使用前綴匹配ARNs來匹配特定資源類型的事件。

```
{
    "source": [ "aws.resource-groups" ],
    "resources": [
        { "prefix": "arn:aws:ec2:us-east-1:123456789012:instance" }
    ]
}
```

或者，您可以通過使用resource-type標識符來使用精確匹配，這可能會簡潔地匹配多個類型。與前面的範例不同，下列範例只比對群組成員資格變更事件，因為群組狀態變更事件不包含resources欄位在其detail欄位中。

```
{
    "source": [ "aws.resource-groups" ],
    "detail": {
        "resources": {
                "resource-type": [ "AWS::EC2::Instance", "AWS::EC2::Volume" ]
         }
    }
}
```

所有資源移除事件

```
{
    "source": [ "aws.resource-groups" ],
    "detail-type": [ "ResourceGroups Group Membership Change" ],
    "detail": {
        "resources": {
                "membership-change": [ "remove" ]
        }
    }
}
```

特定資源的所有資源移除事件

```
 {
    "source": [ "aws.resource-groups" ],
    "detail-type": [ "ResourceGroups Group Membership Change" ],
    "detail": {
        "resources": {
                "membership-change": [ "remove" ],
                "arn": [ "arn:aws:ec2:us-east-1:123456789012:instance/i-b188560f" ]
         }
    }
}
```

您無法將本節第一個範例中使用的頂層resources陣列用於此類型的事件篩選。這是因為頂層resources元素中的資源可能是新增至群組的資源，而且事件仍然會相符。換句話說，下列程式碼範例可能會傳回未預期的事件。請改用上一個範例中顯示的語法。

```
{
    "source": [ "aws.resource-groups" ],
    "detail-type": [ "ResourceGroups Group Membership Change" ],
    "resources": [ "arn:aws:ec2:us-east-1:123456789012:instance/i-b188560f" ],
    "detail": {
        "resources": {
                "membership-change": [ "remove" ]
         }
     }
}
```

刪除資源群組 AWS Resource Groups

您可以使用AWS Resource Groups 主控台或從中刪除資源群組 AWS Resource Groups。 AWS CLI 刪除資源群組不會刪除屬於群組成員的資源或成員資源上的標籤。它只會刪除群組架構和任何群組層級標籤。

Console

若要刪除資源群組

1. 登入 AWS Resource Groups 主控台。
2. 在功能窗格中，選擇 [儲存的 Resource Groups]。
3. 選擇您要刪除的資源群組名稱，然後選擇 [檢視詳細資訊]。
4. 在群組的詳細資訊頁面上，選擇右上角的 [刪除]。
5. 出現提示要您確認刪除時，選擇 Delete (刪除)。

AWS CLI & AWS SDKs

若要刪除資源群組

1. 運行以下命令，替換 *resource_group_name* 使用您的組的名稱。

```
$ aws resource-groups delete-group \
    --group-name resource_group_name
```

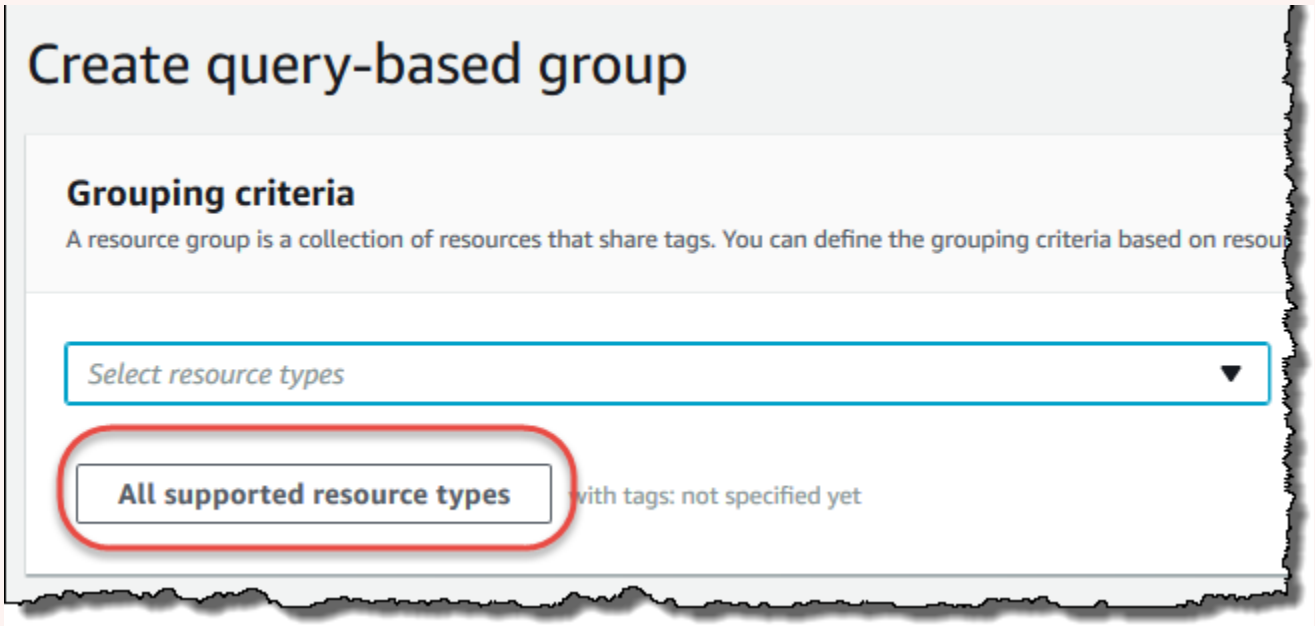
2. 當系統提示您確認刪除時，請鍵入 `yes`，然後按下 Enter 鍵。

可與標籤編輯器搭配使用 AWS Resource Groups 的資源類型

您可以使用 AWS Management Console 或建立資源群組，然後透過這些群組與成員資源互動。 AWS CLI 您可以將標籤新增至許多 AWS 資源，然後使用這些標籤來管理群組成員資格。本主題說明您可以使用來包含在資源群組中的資源類型 AWS Resource Groups，以及您可以使用標籤編輯器標記的資源類型。 AWS

Important

根據查詢「所有支援的資源類型」的 Resource Groups 可以隨著時間的推移自動新增成員，因為資源群組支援新資源。當您根據 [所有支援的資源類型] 在現有的資源群組上執行自動化或其他批次處理工作時，請注意，在您第一次建立群組時，動作可能會在群組中執行的資源多於群組中的資源。這也表示您為其他資源建立的自動化作業或工作會套用至可能非預期的資源，或是無法順利完成工作的資源。在這些情況下，您可以新增資源類型篩選器，以指定只有指定類型的資源可以成為群組的一部分。



下表列出在標籤編輯器中標記所支援的資源類型、標籤查詢型群組中的成員資格，以及 AWS CloudFormation 堆疊型群組中的成員資格支援哪些資源類型。

欄定義

- 標籤編輯器標記 — 您可以使用標籤編輯器主控台來標記此類型的資源。否則，您必須使用該資源擁有服務本機支援的AWS Resource Groups Tagging API或標記服務。

- 以標籤為基礎的群組 — 您可以在資源群組中包含此類型的資源，這些資源群組的成員資格是由附加至資源的標籤所決定。該組指定標籤鍵名稱和值，任何具有匹配標籤的資源都會自動成為該組的一部分
- AWS CloudFormation 堆疊式群組 — 您可以在資源群組中包含此類型的資源，這些資源群組的成員資格是由建立為 CloudFormation 堆疊一部分的資源所組成。該組指定堆棧的 ARN，並且其所有資源自動成為該組的成員。將標籤新增至 AWS CloudFormation 堆疊會導致堆疊的更新。

如需已取代且不再受 Resource Groups 支援的資源類型清單，請參閱本主題結尾的章棄用的資源類型節。

> **Note**
>
> Resource Groups 和標籤編輯器支援下表中的資源類型，但是您的中可能無法使用某些資源類型 AWS 區域。

Amazon API Gateway

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::ApiGateway::Account	✗ 否	✗ 否	✓ 是
AWS::ApiGateway::ApiKey	✗ 否	✓ 是	✓ 是
AWS::ApiGateway::ClientCertificate	✗ 否	✓ 是	✗ 否
AWS::ApiGateway::DomainName	✗ 否	✗ 否	✓ 是
AWS::ApiGateway::RestApi	✗ 否	✓ 是	✓ 是
AWS::ApiGateway::Stage	✗ 否	✓ 是	✗ 否
AWS::ApiGateway::UsagePlan	✗ 否	✓ 是	✓ 是

Amazon API Gateway V2

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::ApiGatewayV2::Api	✗ 否	✓ 是	✗ 否

IAM Access Analyzer

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::AccessAnalyzer::Analyzer	✗ 否	✓ 是	✗ 否

AWS Amplify

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::Amplify::App	✗ 否	✓ 是	✗ 否

AWS App Mesh

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::AppMesh::Mesh	✗ 否	✓ 是	✗ 否

Amazon AppStream

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::AppStream::AppBlock	✗ 否	✓ 是	✗ 否
AWS::AppStream::Application	✗ 否	✓ 是	✗ 否
AWS::AppStream::Fleet	✓ 是	✓ 是	✓ 是
AWS::AppStream::ImageBuilder	✓ 是	✓ 是	✓ 是
AWS::AppStream::Stack	✓ 是	✓ 是	✓ 是

AWS AppSync

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::AppSync::DataSource	✗ 否	✗ 否	✓ 是

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::AppSync::GraphQLApi	✗ 否	✗ 否	✓ 是

Amazon Athena

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::Athena::DataCatalog	✗ 否	✓ 是	✗ 否
AWS::Athena::WorkGroup	✗ 否	✓ 是	✗ 否

AWS Backup

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::Backup::BackupPlan	✗ 否	✓ 是	✗ 否
AWS::Backup::BackupVault	✗ 否	✓ 是	✗ 否
AWS::Backup::ReportPlan	✗ 否	✓ 是	✗ 否

AWS Batch

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::Batch::ComputeEnvironment	✗ 否	✓ 是	✗ 否
AWS::Batch::JobQueue	✗ 否	✓ 是	✗ 否
AWS::Batch::SchedulingPolicy	✗ 否	✓ 是	✗ 否

AWS Billing Conductor

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::BillingConductor::BillingGroup	✗ 否	✓ 是	✓ 是
AWS::BillingConductor::CustomLineItem	✗ 否	✓ 是	✓ 是
AWS::BillingConductor::PricingPlan	✗ 否	✓ 是	✓ 是
AWS::BillingConductor::PricingRule	✗ 否	✓ 是	✓ 是

Amazon Braket

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::Braket::Job	✗ 否	✓ 是	✗ 否
AWS::Braket::QuantumTask	✓ 是	✓ 是	✗ 否

AWS Certificate Manager

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::CertificateManager::Certificate	✓ 是	✓ 是	✓ 是

AWS Certificate Manager 私人憑證授權單

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::ACMPCA::CertificateAuthority	✗ 否	✓ 是	✗ 否

AWS Cloud9

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::Cloud9::Environment	✓ 是	✓ 是	X 否

AWS CloudFormation

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::CloudFormation::Stack	✓ 是	✓ 是	✓ 是

Amazon CloudFront

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::CloudFront::Distribution	✓ 是 [1]	✓ 是	✓ 是
AWS::CloudFront::StreamingDistribution	✓ 是 [1]	✓ 是	✓ 是

[1] 這是在美國東部 (維吉尼亞北部) 區域託管的全球服務的資源。若要使用標籤編輯器建立或修改此資源類型的標籤，您必須us-east-1從「標籤編輯器」主控台中「尋找要標記的資源」下的 「選取地區」清單中加入。

[2] 這是在美國東部 (維吉尼亞北部) 區域託管的全球服務資源。由於 Resource Groups 會針對每個區域分別維護，因 AWS 區域 此您必須 AWS Management Console 將您的切換至包含要包含在群組中之資源的。若要建立包含全域資源的資源群組，您必須使用右上角的「區域」選取器， AWS Management Console 將您的設定為美國東部 (維吉尼亞北部) us-east-1。 AWS Management Console

AWS Cloud Map

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::ServiceDiscovery::Service	✗ 否	✓ 是	✗ 否

AWS CloudTrail

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::CloudTrail::Channel	✗ 否	✓ 是	✗ 否
AWS::CloudTrail::EventDataStore	✗ 否	✓ 是	✗ 否
AWS::CloudTrail::Trail	✓ 是	✓ 是	✓ 是

Amazon CloudWatch

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::CloudWatch::Alarm	✓ 是	✓ 是	✓ 是

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::CloudWatch::Dashboard	✗ 否	✗ 否	✓ 是
AWS::CloudWatch::InsightRule	✗ 否	✓ 是	✗ 否
AWS::CloudWatch::MetricStream	✗ 否	✓ 是	✗ 否
AWS::CloudWatch::ServiceLevelObjective	✗ 否	✓ 是	✗ 否

Amazon CloudWatch 日誌

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::Logs::Destination	✗ 否	✓ 是	✗ 否
AWS::Logs::LogGroup	✗ 否	✓ 是	✓ 是

Amazon CloudWatch Synthetics

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::Synthetics::Canary	✗ 否	✓ 是	✓ 是

AWS CodeArtifact

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::CodeArtifact::Domain	✓ 是	✓ 是	✓ 是
AWS::CodeArtifact::Repository	✓ 是	✓ 是	✓ 是

AWS CodeBuild

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::CodeBuild::Project	✓ 是	✓ 是	X 否

AWS CodeCommit

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::CodeCommit::Repository	✓ 是	✓ 是	X 否

AWS CodeDeploy

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::CodeDeploy::Application	✗ 否	✓ 是	✓ 是
AWS::CodeDeploy::DeploymentConfig	✗ 否	✗ 否	✓ 是

Amazon 評論 CodeGuru 家

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::CodeGuruReviewer::RepositoryAssociation	✓ 是	✓ 是	✓ 是

Amazon CodeGuru 分析器

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::CodeGuruProfiler::ProfilingGroup	✗ 否	✓ 是	✗ 否

AWS CodePipeline

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::CodePipeline::CustomActionType	✗ 否	✓ 是	✗ 否
AWS::CodePipeline::Pipeline	✓ 是	✓ 是	✓ 是
AWS::CodePipeline::Webhook	✓ 是	✓ 是	✓ 是

AWS CodeConnections

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::CodeStarConnections::Connection	✗ 否	✓ 是	✗ 否

Amazon Cognito

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::Cognito::IdentityPool	✓ 是	✓ 是	✓ 是
AWS::Cognito::UserPool	✓ 是	✓ 是	✓ 是

Amazon Comprehend

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::Comprehend::DocumentClassifier	✓ 是	✓ 是	X 否
AWS::Comprehend::EntityRecognizer	✓ 是	✓ 是	X 否

AWS Config

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::Config::AggregationAuthorization	X 否	✓ 是	X 否
AWS::Config::ConfigRule	✓ 是	✓ 是	X 否
AWS::Config::ConfigurationAggregator	X 否	✓ 是	X 否
AWS::Config::StoredQuery	X 否	✓ 是	X 否

Amazon Connect

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::Connect::Instance	X 否	✓ 是	X 否

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::Connect::PhoneNumber	✗ 否	✓ 是	✗ 否

Amazon Connect Wisdom

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::Wisdom::Assistant	✗ 否	✓ 是	✓ 是
AWS::Wisdom::AssistantAssociation	✗ 否	✓ 是	✓ 是
AWS::Wisdom::Content	✗ 否	✓ 是	✗ 否
AWS::Wisdom::KnowledgeBase	✗ 否	✓ 是	✓ 是
AWS::Wisdom::Session	✗ 否	✓ 是	✗ 否

AWS Data Exchange

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::DataExchange::DataSet	✓ 是	✓ 是	✗ 否
AWS::DataExchange::Revision	✗ 否	✓ 是	✗ 否

AWS Data Pipeline

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::DataPipeline::Pipeline	✓ 是	✓ 是	✓ 是

AWS DataSync

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::DataSync::Task	✗ 否	✓ 是	✗ 否

AWS Database Migration Service

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::DMS::Certificate	✓ 是	✓ 是	✗ 否
AWS::DMS::Endpoint	✓ 是	✓ 是	✓ 是
AWS::DMS::EventSubscription	✓ 是	✓ 是	✗ 否
AWS::DMS::ReplicationInstance	✓ 是	✓ 是	✓ 是
AWS::DMS::ReplicationSubnetGroup	✓ 是	✓ 是	✗ 否

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::DMS::ReplicationTask	✓ 是	✓ 是	X 否

AWS Device Farm

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::DeviceFarm::InstanceProfile	X 否	✓ 是	X 否
AWS::DeviceFarm::Project	X 否	✓ 是	X 否
AWS::DeviceFarm::TestGridProject	X 否	✓ 是	X 否

Amazon DynamoDB

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::DynamoDB::Table	✓ 是	✓ 是	✓ 是

Amazon EMR

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::EMR::Cluster	✓ 是	✓ 是	✓ 是

Amazon EMR 容器

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::EMRContainers::JobRun	X 否	✓ 是	X 否
AWS::EMRContainers::VirtualCluster	✓ 是	✓ 是	✓ 是

Amazon EMR Serverless

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::EMRServerless::Application	X 否	✓ 是	✓ 是
AWS::EMRServerless::JobRun	X 否	✓ 是	X 否

Amazon ElastiCache

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::ElastiCache::CacheCluster	✓ 是	✓ 是	✓ 是
AWS::ElastiCache::ParameterGroup	X 否	✓ 是	X 否
AWS::ElastiCache::SecurityGroup	X 否	✓ 是	X 否
AWS::ElastiCache::Snapshot	✓ 是	✓ 是	X 否
AWS::ElastiCache::SubnetGroup	X 否	✓ 是	X 否
AWS::ElastiCache::User	X 否	✓ 是	X 否
AWS::ElastiCache::UserGroup	X 否	✓ 是	X 否

AWS Elastic Beanstalk

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::ElasticBeanstalk::Application	✓ 是	✓ 是	X 否
AWS::ElasticBeanstalk::ApplicationVersion	X 否	✓ 是	X 否
AWS::ElasticBeanstalk::ConfigurationTemplate	X 否	✓ 是	X 否
AWS::ElasticBeanstalk::Environment	X 否	✓ 是	X 否

Amazon Elastic Compute Cloud (Amazon EC2)

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::EC2::CapacityReservation	✗ 否	✓ 是	✗ 否
AWS::EC2::CapacityReservationFleet	✗ 否	✓ 是	✗ 否
AWS::EC2::CarrierGateway	✗ 否	✓ 是	✗ 否
AWS::EC2::ClientVpnEndpoint	✗ 否	✓ 是	✗ 否
AWS::EC2::CoipPool	✗ 否	✓ 是	✗ 否
AWS::EC2::CustomerGateway	✓ 是	✓ 是	✓ 是
AWS::EC2::DHCPOptions	✓ 是	✓ 是	✓ 是
AWS::EC2::EC2Fleet	✗ 否	✓ 是	✗ 否
AWS::EC2::EgressOnlyInternetGateway	✗ 否	✓ 是	✗ 否
AWS::EC2::EIP	✓ 是	✓ 是	✗ 否
AWS::EC2::ExportImageTask	✗ 否	✓ 是	✗ 否
AWS::EC2::ExportInstanceTask	✗ 否	✓ 是	✗ 否
AWS::EC2::FlowLog	✗ 否	✓ 是	✗ 否
AWS::EC2::FpgaImage	✗ 否	✓ 是	✗ 否
AWS::EC2::Host	✗ 否	✓ 是	✗ 否
AWS::EC2::HostReservation	✗ 否	✓ 是	✗ 否
AWS::EC2::Image	✓ 是	✓ 是	✗ 否

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::EC2::ImportImageTask	✗ 否	✓ 是	✗ 否
AWS::EC2::ImportSnapshotTask	✗ 否	✓ 是	✗ 否
AWS::EC2::Instance	✓ 是	✓ 是	✓ 是
AWS::EC2::InstanceEventWindow	✗ 否	✓ 是	✗ 否
AWS::EC2::InternetGateway	✓ 是	✓ 是	✓ 是
AWS::EC2::IPv4Pool	✗ 否	✓ 是	✗ 否
AWS::EC2::IPv6Pool	✗ 否	✓ 是	✗ 否
AWS::EC2::KeyPair	✗ 否	✓ 是	✗ 否
AWS::EC2::LaunchTemplate	✗ 否	✓ 是	✓ 是
AWS::EC2::LocalGateway	✗ 否	✓ 是	✗ 否
AWS::EC2::LocalGatewayRouteTable	✗ 否	✓ 是	✗ 否
AWS::EC2::LocalGatewayRouteTableVirtualInterfaceGroupAssociation	✗ 否	✓ 是	✗ 否
AWS::EC2::LocalGatewayRouteTableVPCAssociation	✗ 否	✓ 是	✗ 否
AWS::EC2::LocalGatewayVirtualInterface	✗ 否	✓ 是	✗ 否
AWS::EC2::LocalGatewayVirtualInterfaceGroup	✗ 否	✓ 是	✗ 否
AWS::EC2::NatGateway	✓ 是	✓ 是	✓ 是

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::EC2::NetworkAcl	✓ 是	✓ 是	✓ 是
AWS::EC2::NetworkInsightsAccessScope	✗ 否	✓ 是	✗ 否
AWS::EC2::NetworkInsightsAccessScopeAnalysis	✗ 否	✓ 是	✗ 否
AWS::EC2::NetworkInsightsAnalysis	✗ 否	✓ 是	✗ 否
AWS::EC2::NetworkInsightsPath	✗ 否	✓ 是	✗ 否
AWS::EC2::NetworkInterface	✓ 是	✓ 是	✓ 是
AWS::EC2::PlacementGroup	✗ 否	✓ 是	✓ 是
AWS::EC2::PrefixList	✗ 否	✓ 是	✗ 否
AWS::EC2::ReplaceRootVolumeTask	✗ 否	✓ 是	✗ 否
AWS::EC2::ReservedInstance	✓ 是	✓ 是	✗ 否
AWS::EC2::RouteTable	✓ 是	✓ 是	✓ 是
AWS::EC2::SecurityGroup	✓ 是	✓ 是	✓ 是
AWS::EC2::Snapshot	✓ 是	✓ 是	✗ 否
AWS::EC2::SpotFleet	✗ 否	✓ 是	✗ 否
AWS::EC2::SpotInstanceRequest	✓ 是	✓ 是	✗ 否
AWS::EC2::Subnet	✓ 是	✓ 是	✓ 是
AWS::EC2::SubnetCidrReservation	✗ 否	✓ 是	✗ 否
AWS::EC2::TrafficMirrorFilter	✗ 否	✓ 是	✗ 否

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::EC2::TrafficMirrorSession	✗ 否	✓ 是	✗ 否
AWS::EC2::TrafficMirrorTarget	✗ 否	✓ 是	✗ 否
AWS::EC2::TransitGateway	✗ 否	✓ 是	✗ 否
AWS::EC2::TransitGatewayAttachment	✗ 否	✓ 是	✗ 否
AWS::EC2::TransitGatewayConnectPeer	✗ 否	✓ 是	✗ 否
AWS::EC2::TransitGatewayMulticastDomain	✗ 否	✓ 是	✗ 否
AWS::EC2::TransitGatewayPolicyTable	✗ 否	✓ 是	✗ 否
AWS::EC2::TransitGatewayRouteTable	✗ 否	✓ 是	✗ 否
AWS::EC2::TransitGatewayRouteTableAnnouncement	✗ 否	✓ 是	✗ 否
AWS::EC2::VerifiedAccessEndpoint	✗ 否	✓ 是	✗ 否
AWS::EC2::VerifiedAccessGroup	✗ 否	✓ 是	✗ 否
AWS::EC2::VerifiedAccessInstance	✗ 否	✓ 是	✗ 否
AWS::EC2::VerifiedAccessTrustProvider	✗ 否	✓ 是	✗ 否
AWS::EC2::Volume	✓ 是	✓ 是	✓ 是
AWS::EC2::VPC	✓ 是	✓ 是	✓ 是
AWS::EC2::VPCEndpoint	✗ 否	✓ 是	✗ 否
AWS::EC2::VPCEndpointConnection	✗ 否	✓ 是	✗ 否

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::EC2::VPCEndpointService	✗ 否	✓ 是	✗ 否
AWS::EC2::VPCEndpointServicePermissions	✗ 否	✓ 是	✗ 否
AWS::EC2::VPCPeeringConnection	✗ 否	✓ 是	✓ 是
AWS::EC2::VPNConnection	✓ 是	✓ 是	✓ 是
AWS::EC2::VPNGateway	✓ 是	✓ 是	✓ 是

Amazon Elastic Container Registry

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::ECR::Repository	✗ 否	✓ 是	✗ 否

Amazon Elastic Container Service

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::ECS::CapacityProvider	✗ 否	✓ 是	✗ 否
AWS::ECS::Cluster	✓ 是	✓ 是	✗ 否

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::ECS::ContainerInstance	✗ 否	✓ 是	✗ 否
AWS::ECS::Service	✗ 否	✓ 是	✗ 否
AWS::ECS::Task	✗ 否	✓ 是	✗ 否
AWS::ECS::TaskDefinition	✓ 是	✓ 是	✗ 否
AWS::ECS::TaskSet	✗ 否	✓ 是	✗ 否

Amazon Elastic File System

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::EFS::FileSystem	✓ 是	✓ 是	✓ 是

Amazon Elastic Inference

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::ElasticInference::ElasticInferenceAccelerator	✓ 是	✓ 是	✗ 否

Amazon Elastic Kubernetes Service (Amazon EKS)

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::EKS::Addon	✗ 否	✓ 是	✗ 否
AWS::EKS::Cluster	✓ 是	✓ 是	✓ 是

Elastic Load Balancing

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::ElasticLoadBalancing::LoadBalancer	✓ 是	✓ 是	✓ 是
AWS::ElasticLoadBalancingV2::Listener	✗ 否	✓ 是	✓ 是
AWS::ElasticLoadBalancingV2::ListenerRule	✗ 否	✓ 是	✓ 是
AWS::ElasticLoadBalancingV2::LoadBalancer	✓ 是	✓ 是	✓ 是
AWS::ElasticLoadBalancingV2::TargetGroup	✓ 是	✓ 是	✓ 是

Amazon OpenSearch 服務

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::Elasticsearch::Domain	✓ 是	✓ 是	✓ 是

Amazon CloudWatch 活動

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::Events::EventBus	X 否	✓ 是	X 否
AWS::Events::Rule	✓ 是	✓ 是	✓ 是

> **Note**
>
> 標籤編輯器不支援自訂事件匯流排中的規則。

Amazon EventBridge 模式

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::EventSchemas::Discoverer	X 否	✓ 是	X 否

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::EventSchemas::Registry	✗ 否	✓ 是	✗ 否
AWS::EventSchemas::Schema	✗ 否	✓ 是	✗ 否

Amazon FSx

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::FSx::FileSystem	✓ 是	✓ 是	✗ 否
AWS::FSx::StorageVirtualMachine	✗ 否	✓ 是	✗ 否
AWS::FSx::Volume	✗ 否	✓ 是	✗ 否

Amazon Forecast

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::Forecast::Dataset	✓ 是	✓ 是	✗ 否
AWS::Forecast::DatasetGroup	✓ 是	✓ 是	✗ 否
AWS::Forecast::DatasetImportJob	✓ 是	✓ 是	✗ 否
AWS::Forecast::Forecast	✓ 是	✓ 是	✗ 否

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::Forecast::ForecastExportJob	✓ 是	✓ 是	X 否
AWS::Forecast::Predictor	✓ 是	✓ 是	X 否
AWS::Forecast::PredictorBacktestExportJob	✓ 是	✓ 是	X 否

Amazon Fraud Detector

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::FraudDetector::Detector	✓ 是	✓ 是	X 否
AWS::FraudDetector::DetectorVersion	X 否	✓ 是	X 否
AWS::FraudDetector::EntityType	✓ 是	✓ 是	X 否
AWS::FraudDetector::EventType	✓ 是	✓ 是	X 否
AWS::FraudDetector::ExternalModel	✓ 是	✓ 是	X 否
AWS::FraudDetector::Label	✓ 是	✓ 是	X 否
AWS::FraudDetector::Model	✓ 是	✓ 是	X 否
AWS::FraudDetector::ModelVersion	X 否	✓ 是	X 否
AWS::FraudDetector::Outcome	✓ 是	✓ 是	X 否
AWS::FraudDetector::Rule	X 否	✓ 是	X 否

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::FraudDetector::Variable	✓ 是	✓ 是	X 否

Amazon GameLift

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::GameLift::Alias	X 否	✓ 是	X 否
AWS::GameLift::GameSessionQueue	X 否	✓ 是	X 否
AWS::GameLift::Location	X 否	✓ 是	X 否
AWS::GameLift::MatchmakingConfiguration	X 否	✓ 是	X 否
AWS::GameLift::MatchmakingRuleSet	X 否	✓ 是	X 否

AWS Global Accelerator

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::GlobalAccelerator::Accelerator	X 否	✓ 是	X 否

AWS Glue

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::Glue::Crawler	✓ 是	✓ 是	✗ 否
AWS::Glue::Database	✗ 否	✓ 是	✓ 是
AWS::Glue::Job	✓ 是	✓ 是	✗ 否
AWS::Glue::MLTransform	✗ 否	✓ 是	✗ 否
AWS::Glue::Registry	✗ 否	✓ 是	✗ 否
AWS::Glue::Trigger	✓ 是	✓ 是	✗ 否
AWS::Glue::Workflow	✗ 否	✓ 是	✗ 否

AWS Glue DataBrew

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::DataBrew::Dataset	✓ 是	✓ 是	✓ 是
AWS::DataBrew::Job	✓ 是	✓ 是	✓ 是
AWS::DataBrew::Project	✓ 是	✓ 是	✓ 是
AWS::DataBrew::Recipe	✓ 是	✓ 是	✓ 是
AWS::DataBrew::Schedule	✓ 是	✓ 是	✓ 是

AWS Ground Station

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::GroundStation::Config	✗ 否	✓ 是	✗ 否
AWS::GroundStation::DataflowEndpointGroup	✗ 否	✓ 是	✗ 否
AWS::GroundStation::MissionProfile	✗ 否	✓ 是	✗ 否

Amazon GuardDuty

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::GuardDuty::Detector	✗ 否	✓ 是	✓ 是
AWS::GuardDuty::Filter	✗ 否	✓ 是	✗ 否
AWS::GuardDuty::IPSet	✗ 否	✓ 是	✗ 否
AWS::GuardDuty::ThreatIntelSet	✗ 否	✓ 是	✗ 否

Amazon Interactive Video Service

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::IVS::Channel	✗ 否	✓ 是	✗ 否
AWS::IVS::RecordingConfiguration	✗ 否	✓ 是	✗ 否
AWS::IVS::StreamKey	✗ 否	✓ 是	✗ 否

AWS Identity and Access Management

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::IAM::InstanceProfile	✓ 是 [1]	✓ 是	✗ 否
AWS::IAM::ManagedPolicy	✓ 是 [1]	✓ 是	✗ 否
AWS::IAM::OpenIDConnectProvider	✓ 是 [1]	✓ 是	✗ 否
AWS::IAM::Role	✗ 否	✗ 否	✓ 是
AWS::IAM::SAMLProvider	✓ 是 [1]	✓ 是	✗ 否
AWS::IAM::ServerCertificate	✓ 是 [1]	✓ 是	✗ 否
AWS::IAM::VirtualMFADevice	✓ 是 [1]	✓ 是	✗ 否

[1] 這是在美國東部 (維吉尼亞北部) 區域託管的全球服務的資源。若要使用標籤編輯器建立或修改此資源類型的標籤，您必須us-east-1從「標籤編輯器」主控台中「尋找要標記的資源」下的 「選取地區」清單中加入。

[2] 這是在美國東部 (維吉尼亞北部) 區域託管的全球服務資源。由於 Resource Groups 會針對每個區域分別維護，因 AWS 區域 此您必須 AWS Management Console 將您的切換至包含要包含在群組中之資源的。若要建立包含全域資源的資源群組，您必須使用右上角的「區域」選取器， AWS Management Console 將您的設定為美國東部 (維吉尼亞北部) us-east-1。 AWS Management Console

EC2 Image Builder

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::ImageBuilder::Component	✗ 否	✓ 是	✗ 否
AWS::ImageBuilder::ContainerRecipe	✗ 否	✓ 是	✗ 否
AWS::ImageBuilder::DistributionConfiguration	✗ 否	✓ 是	✗ 否
AWS::ImageBuilder::Image	✗ 否	✓ 是	✗ 否
AWS::ImageBuilder::ImagePipeline	✗ 否	✓ 是	✗ 否
AWS::ImageBuilder::ImageRecipe	✗ 否	✓ 是	✗ 否
AWS::ImageBuilder::InfrastructureConfiguration	✗ 否	✓ 是	✗ 否

Amazon Inspector

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::Inspector::AssessmentTemplate	✗ 否	✓ 是	✓ 是

AWS IoT

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::IoT::Authorizer	✗ 否	✓ 是	✗ 否
AWS::IoT::BillingGroup	✗ 否	✓ 是	✗ 否
AWS::IoT::CACertificate	✗ 否	✓ 是	✗ 否
AWS::IoT::CustomMetric	✗ 否	✓ 是	✗ 否
AWS::IoT::Dimension	✗ 否	✓ 是	✗ 否
AWS::IoT::JobTemplate	✗ 否	✓ 是	✗ 否
AWS::IoT::MitigationAction	✗ 否	✓ 是	✗ 否
AWS::IoT::Policy	✗ 否	✓ 是	✗ 否
AWS::IoT::RoleAlias	✗ 否	✓ 是	✗ 否
AWS::IoT::ScheduledAudit	✗ 否	✓ 是	✗ 否
AWS::IoT::SecurityProfile	✗ 否	✓ 是	✗ 否
AWS::IoT::ThingGroup	✗ 否	✓ 是	✗ 否
AWS::IoT::ThingType	✗ 否	✓ 是	✗ 否
AWS::IoT::TopicRule	✗ 否	✓ 是	✓ 是

AWS IoT Analytics

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::IoTAnalytics::Channel	✗ 否	✓ 是	✗ 否
AWS::IoTAnalytics::Dataset	✓ 是	✓ 是	✗ 否
AWS::IoTAnalytics::Datastore	✗ 否	✓ 是	✗ 否
AWS::IoTAnalytics::Pipeline	✗ 否	✓ 是	✗ 否

AWS IoT Events

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::IoTEvents::AlarmModel	✗ 否	✓ 是	✗ 否
AWS::IoTEvents::DetectorModel	✓ 是	✓ 是	✓ 是
AWS::IoTEvents::Input	✓ 是	✓ 是	✓ 是

AWS IoT FleetWise

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::IoTFleetWise::Campaign	✗ 否	✓ 是	✓ 是
AWS::IoTFleetWise::DecoderManifest	✗ 否	✓ 是	✓ 是
AWS::IoTFleetWise::Fleet	✗ 否	✓ 是	✓ 是
AWS::IoTFleetWise::ModelManifest	✗ 否	✓ 是	✓ 是
AWS::IoTFleetWise::SignalCatalog	✗ 否	✓ 是	✓ 是
AWS::IoTFleetWise::Vehicle	✗ 否	✓ 是	✓ 是

AWS IoT Greengrass

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::Greengrass::ConnectorDefinition	✓ 是	✓ 是	✗ 否
AWS::Greengrass::CoreDefinition	✓ 是	✓ 是	✗ 否
AWS::Greengrass::DeviceDefinition	✓ 是	✓ 是	✗ 否
AWS::Greengrass::FunctionDefinition	✓ 是	✓ 是	✗ 否
AWS::Greengrass::Group	✓ 是	✓ 是	✗ 否
AWS::Greengrass::LoggerDefinition	✓ 是	✓ 是	✗ 否

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::Greengrass::ResourceDefinition	✓ 是	✓ 是	X 否
AWS::Greengrass::SubscriptionDefinition	✓ 是	✓ 是	X 否

AWS IoT Greengrass Version 2

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::GreengrassV2::ComponentVersion	X 否	✓ 是	X 否

AWS IoT SiteWise 主控台

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::IoTSiteWise::Asset	X 否	✓ 是	X 否
AWS::IoTSiteWise::AssetModel	X 否	✓ 是	X 否
AWS::IoTSiteWise::Dashboard	X 否	✓ 是	X 否
AWS::IoTSiteWise::Gateway	X 否	✓ 是	X 否
AWS::IoTSiteWise::Portal	X 否	✓ 是	X 否

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::IoTSiteWise::Project	✗ 否	✓ 是	✗ 否

AWS IoT Wireless

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::IoTWireless::Destination	✗ 否	✓ 是	✗ 否
AWS::IoTWireless::DeviceProfile	✗ 否	✓ 是	✗ 否
AWS::IoTWireless::FuotaTask	✗ 否	✓ 是	✗ 否
AWS::IoTWireless::MulticastGroup	✗ 否	✓ 是	✗ 否
AWS::IoTWireless::NetworkAnalyzerConfiguration	✗ 否	✓ 是	✗ 否
AWS::IoTWireless::ServiceProfile	✗ 否	✓ 是	✗ 否
AWS::IoTWireless::TaskDefinition	✗ 否	✓ 是	✗ 否
AWS::IoTWireless::WirelessDevice	✗ 否	✓ 是	✗ 否
AWS::IoTWireless::WirelessGateway	✗ 否	✓ 是	✗ 否

AWS Key Management Service

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::KMS::Alias	✗ 否	✗ 否	✓ 是
AWS::KMS::Key	✓ 是	✓ 是	✓ 是

Amazon Keyspaces (適用於 Apache Cassandra)

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::Cassandra::Keyspace	✗ 否	✓ 是	✓ 是
AWS::Cassandra::Table	✗ 否	✓ 是	✗ 否

Amazon Kinesis

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::Kinesis::Stream	✓ 是	✓ 是	✓ 是

Amazon Managed Service for Apache Flink

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::KinesisAnalytics::Application	✓ 是	✓ 是	✓ 是
AWS::KinesisAnalyticsV2::Application	X 否	X 否	✓ 是

Amazon 數據 Firehose

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::KinesisFirehose::DeliveryStream	X 否	✓ 是	✓ 是

AWS Lambda

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::Lambda::Alias	X 否	X 否	✓ 是
AWS::Lambda::EventSourceMapping	X 否	X 否	✓ 是
AWS::Lambda::Function	✓ 是	✓ 是	✓ 是
AWS::Lambda::LayerVersion	X 否	X 否	✓ 是

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::Lambda::Version	✗ 否	✗ 否	✓ 是

Amazon Lightsail

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::Lightsail::Bucket	✗ 否	✓ 是	✗ 否
AWS::Lightsail::Certificate	✗ 否	✓ 是	✗ 否
AWS::Lightsail::Container	✗ 否	✓ 是	✗ 否
AWS::Lightsail::Disk	✗ 否	✓ 是	✗ 否
AWS::Lightsail::Distribution	✗ 否	✓ 是	✗ 否
AWS::Lightsail::Instance	✗ 否	✓ 是	✗ 否
AWS::Lightsail::StaticIp	✗ 否	✓ 是	✗ 否

Amazon MQ

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::AmazonMQ::Broker	✓ 是	✓ 是	✗ 否

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::AmazonMQ::Configuration	✓ 是	✓ 是	X 否

Amazon Macie

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::Macie::ClassificationJob	✓ 是	✓ 是	X 否
AWS::Macie::CustomDataIdentifier	✓ 是	✓ 是	✓ 是
AWS::Macie::FindingsFilter	✓ 是	✓ 是	✓ 是
AWS::Macie::Member	✓ 是	✓ 是	X 否

Amazon Managed Blockchain

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::ManagedBlockchain::Accessor	X 否	✓ 是	X 否

Amazon Managed Streaming for Apache Kafka

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::Kafka::Cluster	✓ 是	✓ 是	X 否

AWS Elemental MediaConnect

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::MediaConnect::Flow	X 否	✓ 是	X 否
AWS::MediaConnect::FlowEntitlement	X 否	✓ 是	X 否
AWS::MediaConnect::FlowOutput	X 否	✓ 是	X 否
AWS::MediaConnect::FlowSource	X 否	✓ 是	X 否

AWS Elemental MediaPackage

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::MediaPackage::Channel	X 否	✓ 是	X 否
AWS::MediaPackage::PackagingConfiguration	X 否	✓ 是	X 否

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::MediaPackage::PackagingGroup	✗ 否	✓ 是	✗ 否

AWS Network Manager

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::NetworkManager::CoreNetwork	✗ 否	✓ 是	✗ 否
AWS::NetworkManager::Device	✗ 否	✓ 是	✗ 否
AWS::NetworkManager::GlobalNetwork	✗ 否	✓ 是	✗ 否
AWS::NetworkManager::Link	✗ 否	✓ 是	✗ 否
AWS::NetworkManager::Site	✗ 否	✓ 是	✗ 否
AWS::NetworkManager::VpcAttachment	✗ 否	✓ 是	✗ 否

Amazon OpenSearch 服務 OpenSearch

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::OpenSearchService::Domain	✓ 是	✓ 是	✓ 是

AWS OpsWorks

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::OpsWorks::Instance	✗ 否	✓ 是	✓ 是
AWS::OpsWorks::Layer	✗ 否	✓ 是	✓ 是
AWS::OpsWorks::Stack	✗ 否	✓ 是	✓ 是

AWS Organizations

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::Organizations::Account	✓ 是	✓ 是	✗ 否
AWS::Organizations::OrganizationalUnit	✗ 否	✓ 是	✗ 否
AWS::Organizations::Policy	✗ 否	✓ 是	✗ 否
AWS::Organizations::Root	✓ 是	✓ 是	✗ 否

Amazon Pinpoint

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::Pinpoint::App	✗ 否	✓ 是	✓ 是
AWS::Pinpoint::EmailTemplate	✗ 否	✓ 是	✓ 是
AWS::Pinpoint::PushTemplate	✗ 否	✓ 是	✓ 是
AWS::Pinpoint::SmsTemplate	✗ 否	✓ 是	✓ 是
AWS::Pinpoint::VoiceTemplate	✗ 否	✓ 是	✗ 否

Amazon Pinpoint SMS 和語音 API

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::PinpointSMSVoiceV2::Pool	✗ 否	✓ 是	✗ 否

Amazon Quantum Ledger Database (Amazon QLDB)

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::QLDB::Ledger	✓ 是	✓ 是	✓ 是

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::QLDB::Stream	✗ 否	✓ 是	✓ 是

Amazon Redshift

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::Redshift::Cluster	✓ 是	✓ 是	✓ 是
AWS::Redshift::ClusterParameterGroup	✓ 是	✓ 是	✓ 是
AWS::Redshift::ClusterSecurityGroup	✗ 否	✓ 是	✓ 是
AWS::Redshift::ClusterSubnetGroup	✓ 是	✓ 是	✓ 是
AWS::Redshift::DBGroup	✗ 否	✓ 是	✗ 否
AWS::Redshift::DBName	✗ 否	✓ 是	✗ 否
AWS::Redshift::DBUser	✗ 否	✓ 是	✗ 否
AWS::Redshift::EventSubscription	✗ 否	✓ 是	✗ 否
AWS::Redshift::HSMClientCertificate	✓ 是	✓ 是	✗ 否
AWS::Redshift::HSMConfiguration	✗ 否	✓ 是	✗ 否
AWS::Redshift::Namespace	✗ 否	✓ 是	✗ 否
AWS::Redshift::Snapshot	✗ 否	✓ 是	✗ 否
AWS::Redshift::SnapshotCopyGrant	✗ 否	✓ 是	✗ 否

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::Redshift::SnapshotSchedule	✗ 否	✓ 是	✗ 否
AWS::Redshift::UsageLimit	✗ 否	✓ 是	✗ 否

Amazon Relational Database Service (Amazon RDS)

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::RDS::CustomDBEngineVersion	✗ 否	✓ 是	✗ 否
AWS::RDS::DBCluster	✓ 是	✓ 是	✓ 是
AWS::RDS::DBClusterEndpoint	✗ 否	✓ 是	✗ 否
AWS::RDS::DBClusterParameterGroup	✓ 是	✓ 是	✓ 是
AWS::RDS::DBClusterSnapshot	✓ 是	✓ 是	✗ 否
AWS::RDS::DBInstance	✓ 是	✓ 是	✓ 是
AWS::RDS::DBParameterGroup	✓ 是	✓ 是	✓ 是
AWS::RDS::DBProxy	✗ 否	✓ 是	✗ 否
AWS::RDS::DBProxyEndpoint	✗ 否	✓ 是	✗ 否
AWS::RDS::DBProxyTargetGroup	✗ 否	✓ 是	✗ 否
AWS::RDS::DBSecurityGroup	✓ 是	✓ 是	✓ 是
AWS::RDS::DBSnapshot	✓ 是	✓ 是	✗ 否

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::RDS::DBSubnetGroup	✓ 是	✓ 是	✓ 是
AWS::RDS::Deployment	✗ 否	✓ 是	✗ 否
AWS::RDS::EventSubscription	✓ 是	✓ 是	✗ 否
AWS::RDS::OptionGroup	✓ 是	✓ 是	✗ 否
AWS::RDS::ReservedDBInstance	✓ 是	✓ 是	✗ 否

AWS Resource Access Manager

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::RAM::ResourceShare	✓ 是	✓ 是	✗ 否

AWS Resource Groups

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::ResourceGroups::Group	✓ 是	✓ 是	✓ 是

AWS 機器人製造

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::RoboMaker::DeploymentJob	✗ 否	✓ 是	✗ 否
AWS::RoboMaker::Fleet	✗ 否	✓ 是	✗ 否
AWS::RoboMaker::Robot	✗ 否	✓ 是	✗ 否
AWS::RoboMaker::RobotApplication	✓ 是	✓ 是	✗ 否
AWS::RoboMaker::SimulationApplication	✓ 是	✓ 是	✗ 否
AWS::RoboMaker::SimulationJob	✓ 是	✓ 是	✗ 否

Amazon Route 53

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::Route53::Domain	✓ 是 [1]	✓ 是	✗ 否
AWS::Route53::HealthCheck	✓ 是 [1]	✓ 是	✓ 是
AWS::Route53::HostedZone	✓ 是 [1]	✓ 是	✓ 是

[1] 這是在美國東部 (維吉尼亞北部) 區域託管的全球服務的資源。若要使用標籤編輯器建立或修改此資源類型的標籤，您必須us-east-1從「標籤編輯器」主控台中「尋找要標記的資源」下的 「選取地區」清單中加入。

[2] 這是在美國東部 (維吉尼亞北部) 區域託管的全球服務資源。由於 Resource Groups 會針對每個區域分別維護，因 AWS 區域 此您必須 AWS Management Console 將您的切換至包含要包含在群組中之資源的。若要建立包含全域資源的資源群組，您必須使用右上角的「區域」選取器， AWS Management Console 將您的設定為美國東部 (維吉尼亞北部) us-east-1。 AWS Management Console

Amazon Route 53 Resolver

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::Route53Resolver::FirewallDomainList	✗ 否	✓ 是	✗ 否
AWS::Route53Resolver::FirewallRuleGroup	✗ 否	✓ 是	✗ 否
AWS::Route53Resolver::FirewallRuleGroupAssociation	✗ 否	✓ 是	✗ 否
AWS::Route53Resolver::ResolverEndpoint	✓ 是 [1]	✓ 是	✗ 否
AWS::Route53Resolver::ResolverQueryLoggingConfig	✗ 否	✓ 是	✗ 否
AWS::Route53Resolver::ResolverRule	✓ 是 [1]	✓ 是	✗ 否

[1] 這是在美國東部 (維吉尼亞北部) 區域託管的全球服務的資源。若要使用標籤編輯器建立或修改此資源類型的標籤，您必須us-east-1從「標籤編輯器」主控台中「尋找要標記的資源」下的 「選取地區」清單中加入。

[2] 這是在美國東部 (維吉尼亞北部) 區域託管的全球服務資源。由於 Resource Groups 會針對每個區域分別維護，因 AWS 區域 此您必須 AWS Management Console 將您的切換至包含要包含在群組中之資源的。若要建立包含全域資源的資源群組，您必須使用右上角的「區域」選取器， AWS Management Console 將您的設定為美國東部 (維吉尼亞北部) us-east-1。 AWS Management Console

Amazon S3 Glacier

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::Glacier::Vault	✓ 是	✓ 是	X 否

Amazon SageMaker

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::SageMaker::AppImageConfig	X 否	✓ 是	X 否
AWS::SageMaker::CodeRepository	X 否	✓ 是	X 否
AWS::SageMaker::Endpoint	X 否	✓ 是	✓ 是
AWS::SageMaker::EndpointConfig	X 否	✓ 是	✓ 是
AWS::SageMaker::HyperParameterTuningJob	X 否	✓ 是	X 否
AWS::SageMaker::Image	X 否	✓ 是	X 否
AWS::SageMaker::LabelingJob	X 否	✓ 是	X 否
AWS::SageMaker::Model	X 否	✓ 是	✓ 是
AWS::SageMaker::ModelPackageGroup	X 否	✓ 是	✓ 是
AWS::SageMaker::NotebookInstance	✓ 是	✓ 是	✓ 是
AWS::SageMaker::Pipeline	X 否	✓ 是	X 否

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::SageMaker::Project	✗ 否	✓ 是	✓ 是
AWS::SageMaker::TrainingJob	✗ 否	✓ 是	✗ 否
AWS::SageMaker::TransformJob	✗ 否	✓ 是	✗ 否
AWS::SageMaker::Workteam	✗ 否	✓ 是	✗ 否

AWS Secrets Manager

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::SecretsManager::Secret	✓ 是	✓ 是	✓ 是

AWS Service Catalog

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::ServiceCatalog::CloudFormationProduct	✗ 否	✓ 是	✓ 是
AWS::ServiceCatalog::Portfolio	✗ 否	✓ 是	✓ 是

AWS Service Catalog AppRegistry

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::ServiceCatalogAppRegistry::Application	✗ 否	✓ 是	✗ 否
AWS::ServiceCatalogAppRegistry::AttributeGroup	✗ 否	✓ 是	✗ 否

Service Quotas

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::ServiceQuotas::Quota	✗ 否	✓ 是	✗ 否

Amazon Simple Email Service

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::SES::ConfigurationSet	✓ 是	✓ 是	✓ 是
AWS::SES::ContactList	✓ 是	✓ 是	✓ 是
AWS::SES::DedicatedIpPool	✓ 是	✓ 是	✗ 否

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::SES::Identity	✓ 是	✓ 是	✗ 否

Amazon Simple Notification Service

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::SNS::Topic	✓ 是	✓ 是	✓ 是

Amazon Simple Queue Service

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::SQS::Queue	✓ 是	✓ 是	✓ 是

Amazon Simple Storage Service (Amazon S3)

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::S3::Bucket	✓ 是	✓ 是	✓ 是

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::S3::Job	✗ 否	✓ 是	✗ 否
AWS::S3::StorageLens	✗ 否	✓ 是	✗ 否

AWS Step Functions

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::StepFunctions::Activity	✓ 是	✓ 是	✓ 是
AWS::StepFunctions::StateMachine	✓ 是	✓ 是	✓ 是

Storage Gateway

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::StorageGateway::Gateway	✓ 是	✓ 是	✗ 否
AWS::StorageGateway::Volume	✗ 否	✓ 是	✗ 否

AWS Systems Manager

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::SSM::Association	✗ 否	✓ 是	✗ 否
AWS::SSM::AutomationExecution	✗ 否	✓ 是	✗ 否
AWS::SSM::Document	✗ 否	✓ 是	✓ 是
AWS::SSM::MaintenanceWindow	✗ 否	✓ 是	✗ 否
AWS::SSM::ManagedInstance	✗ 否	✓ 是	✗ 否
AWS::SSM::OpsItem	✗ 否	✓ 是	✗ 否
AWS::SSM::OpsMetadata	✗ 否	✓ 是	✗ 否
AWS::SSM::Parameter	✓ 是	✓ 是	✓ 是
AWS::SSM::PatchBaseline	✗ 否	✓ 是	✓ 是

AWS Systems Manager 適用於 SAP

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::SystemsManagerSAP::Application	✗ 否	✓ 是	✓ 是
AWS::SystemsManagerSAP::Database	✗ 否	✓ 是	✗ 否

Amazon Timestream

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::Timestream::ScheduledQuery	✗ 否	✓ 是	✓ 是

AWS Transfer Family

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::Transfer::Certificate	✗ 否	✓ 是	✗ 否
AWS::Transfer::Connector	✗ 否	✓ 是	✗ 否
AWS::Transfer::Profile	✗ 否	✓ 是	✗ 否
AWS::Transfer::Workflow	✗ 否	✓ 是	✗ 否

AWS WAF

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::WAF::Rule	✗ 否	✓ 是	✗ 否
AWS::WAF::WebACL	✗ 否	✓ 是	✗ 否

Amazon WorkSpaces

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::WorkSpaces::Workspace	✓ 是	✓ 是	✓ 是

AWS X-Ray

資源	標籤編輯器標記	基於標籤的群組	AWS CloudFormation 堆疊式群組
AWS::XRay::Group	X 否	✓ 是	X 否
AWS::XRay::SamplingRule	X 否	✓ 是	X 否

棄用的資源類型

指定的功能不再支援下列資源類型。

服務	Resource Type (資源類型)	Support 變更	日期
AWS RoboMaker	AWS::RoboMaker::Robot	標籤編輯器不再支援。	2022 年 5 月 2 日
AWS RoboMaker	AWS::RoboMaker::Fleet	標籤編輯器不再支援。	2022 年 5 月 2 日
AWS RoboMaker	AWS::RoboMaker::DeploymentJob	標籤編輯器不再支援。	2022 年 5 月 2 日

建立資源群組 AWS CloudFormation

AWS Resource Groups 與整合的服務可協助您建立資源模型並設定資 AWS 源 AWS CloudFormation，以減少建立和管理資源和基礎架構的時間。您可以建立一個範本來描述所需的所有資 AWS 源 (例如資源群組)，並為您 AWS CloudFormation 佈建和設定這些資源。

使用時 AWS CloudFormation，您可以重複使用範本，以一致且重複地設定資源群組。描述您的資源群組一次，然後在多 AWS 帳戶 個和區域中反覆佈建相同的資源群組。

Resource Groups 和 AWS CloudFormation 範本

若要佈建和設定 Resource Groups 及相關服務的資源，您必須瞭解AWS CloudFormation 範本。範本是在JSON或中格式化的文字檔案YAML。這些範本說明您要在 AWS CloudFormation 堆疊中佈建的資源。如果您不熟悉JSON或YAML，可以使用 AWS CloudFormation Designer 來協助您開始使用 AWS CloudFormation 範本。如需詳細資訊，請參閱什麼是 AWS CloudFormation 設計師？ 在《AWS CloudFormation 使用者指南》中。

Resource Groups 支援在中建立資源群組 AWS CloudFormation。如需詳細資訊，包括資源群組的範例JSON和範YAML本，請參閱《AWS CloudFormation 使用指南》中的AWS Resource Groups 資源類型參考。

進一步了解 AWS CloudFormation

若要進一步了解 AWS CloudFormation，請參閱下列資源：

- AWS CloudFormation
- AWS CloudFormation 使用者指南
- AWS CloudFormation API參考
- AWS CloudFormation 指令行介面使用者指南

AWS Resource Groups 中的安全性

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

安全是 AWS 與您共同的責任。共同的責任模型 將此描述為雲端 本身 的安全和雲端 內部 的安全：

- 雲端本身的安全：AWS 負責保護在 AWS Cloud 中執行 AWS 服務的基礎設施。AWS 也提供您可安全使用的服務。在 AWS 合規計劃中，第三方稽核員會定期測試並驗證我們的安全功效。若要進一步了解適用於 AWS Resource Groups 的合規計劃，請參閱 合規計劃範圍內的 AWS 服務。
- 雲端內部的安全 – 您的責任取決於所使用的 AWS 服務。您也必須對其他因素負責，包括資料的機密性、您公司的要求和適用法律和法規。

本文件有助於您了解如何在使用 Resource Groups 時套用共同責任模型。下列主題將示範如何將 Resource Groups 設定為滿足您的安全與合規目標。您也將了解如何使用其他AWS服務，協助您監控並保護 Resource Groups 資源。

主題

- 資料保護 AWS Resource Groups
- 的身分識別與存取管理 AWS Resource Groups
- Resource Groups 中的記錄和監控
- Resource Groups 的符合性驗證
- Resource Groups 中的復原功能
- Resource Groups 的基礎結構安全
- Resource Groups

資料保護 AWS Resource Groups

所以此 AWS 共同責任模型適用於資料保護 AWS Resource Groups。 如本模型所述， AWS 負責保護運行所有的全球基礎設施 AWS 雲端。 您有責任維持對託管在此基礎結構上的內容的控制權。您也必須負責 AWS 服務 你使用的。如需有關資料隱私權的詳細資訊，請參閱資料隱私權FAQ。 如需歐洲資料保護的相關資訊，請參閱 AWS 共同責任模型和GDPR博客文章 AWS 安全部落格。

出於數據保護目的，我們建議您進行保護 AWS 帳戶 憑據並設置個別用戶 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM)。如此一來，每個使用者都只會獲得授與完成其任務所必須的許可。我們也建議您採用下列方式保護資料：

- 對每個帳戶使用多重要素驗證 (MFA)。
- 使用SSL/TLS與之溝通 AWS 的費用。我們需要 TLS 1.2 並推薦 TLS 1.3。
- 設定API和使用者活動記錄 AWS CloudTrail。 如需使用 CloudTrail 軌跡進行擷取的相關資訊 AWS 活動，請參閱使用 CloudTrail 系統線 AWS CloudTrail 使用者指南。
- 使用 AWS 加密解決方案，以及其中的所有默認安全控制 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。
- 如果您在訪問時需要 FIPS 140-3 驗證的加密模塊 AWS 透過指令行介面或API使用FIPS端點。如需有關可用FIPS端點的詳細資訊，請參閱聯邦資訊處理標準 (FIPS) 140-3。

我們強烈建議您絕對不要將客戶的電子郵件地址等機密或敏感資訊，放在標籤或自由格式的文字欄位中，例如名稱欄位。這包括當您使用 Resource Groups 或其他資源群組時 AWS 服務 使用控制台 API， AWS CLI，或 AWS SDKs。您在標籤或自由格式文字欄位中輸入的任何資料都可能用於計費或診斷日誌。如果您提供URL給外部伺服器，我們強烈建議您不要在中包含認證資訊，URL以驗證您對該伺服器的要求。

資料加密

相較於其他 AWS 服務， AWS Resource Groups 具有最小的攻擊面，因為它不提供更改，添加或刪除的方式 AWS 除群組以外的資源。Resource Groups 會向您收集下列服務特定資訊。

- 群組名稱 (未加密，非私人)
- 群組描述 (未加密，但私密)
- 群組中的成員資源 (這些資源儲存在未加密的記錄檔中)

靜態加密

沒有其他方法可隔離特定於 Resource Groups 的服務或網路流量。如果適用，請使用 AWS特定的隔離。您可以在中使用 Resource Groups API 和主控台VPC來協助最大化隱私權和基礎結構安全性。

傳輸中加密

AWS Resource Groups 數據在傳輸到服務的內部數據庫進行備份時被加密。這不是使用者可設定的。

金鑰管理

AWS Resource Groups 目前未與整合 AWS Key Management Service 並且不支持 AWS KMS keys.

網際網路流量隱私權

AWS Resource Groups 用HTTPS於 Resource Groups 使用者之間的所有傳輸， AWS。 Resource Groups 使用傳輸層安全性 (TLS) 1.2，但也支援 TLS 1.0 和 1.1。

的身分識別與存取管理 AWS Resource Groups

AWS Identity and Access Management (IAM) 是 AWS 服務 可協助系統管理員安全地控制存取 AWS 的費用。IAM管理員控制誰可以驗證 (登入) 和授權 (具有權限) 來使用 Resource Groups 資源。IAM是一個 AWS 服務 您可以使用，無需額外費用。

主題

- 物件
- 使用身分驗證
- 使用政策管理存取權
- Resource Groups 如何使用 IAM
- AWS Resource Groups 的 AWS 受管政策
- 對 Resource Groups 使用服務連結角色
- AWS Resource Groups 身分型政策範例
- 疑難排解 AWS Resource Groups 身分和存取

物件

您如何使用 AWS Identity and Access Management (IAM) 會根據您在 Resource Groups 中執行的工作而有所不同。

服務使用者 — 如果您使用 Resource Groups 服務執行工作，則管理員會為您提供所需的認證和權限。當您使用更多 Resource Groups 功能來完成工作時，您可能需要其他權限。了解存取許可的管理方式可協助您向管理員請求正確的許可。如果您無法存取 Resource Groups 中的功能，請參閱疑難排解 AWS Resource Groups 身分和存取。

服務管理員 — 如果您負責公司的 Resource Groups 資源，您可能擁有 Resource Groups 的完整存取權。決定您的服務使用者應存取哪些 Resource Groups 功能和資源是您的工作。然後，您必須向IAM

管理員提交請求，才能變更服務使用者的權限。檢閱此頁面上的資訊，以瞭解的基本概念IAM。若要深入瞭解貴公司如何IAM與 Resource Groups 搭配使用，請參閱Resource Groups 如何使用 IAM。

IAM管理員 — 如果您是系統管理IAM員，您可能想要瞭解如何撰寫原則以管理 Resource Groups 存取權限的詳細資訊。若要檢視您可以在中使用的 Resource Groups 以身分為基礎的策略範例IAM，請參閱。AWS Resource Groups 身分型政策範例

使用身分驗證

驗證是您登入的方式 AWS 使用您的身份證明。您必須經過驗證 (登入 AWS) 作為 AWS 帳戶根使用者，以IAM使用者身分或假定IAM角色。

您可以登入 AWS 使用透過身分識別來源提供的認證做為聯合身分識別。 AWS IAM Identity Center (IAM身分識別中心) 使用者、貴公司的單一登入驗證，以及您的 Google 或 Facebook 認證都是聯合身分識別的範例。當您以同盟身分登入時，您的管理員先前會使用IAM角色設定聯合身分識別。當您存取 AWS 通過使用聯合，您間接擔任一個角色。

根據您所使用的使用者類型，您可以登入 AWS Management Console 或 AWS 存取入口網站。如需登入的詳細資訊 AWS，請參閱如何登入 AWS 帳戶 中的 AWS 登入 使用者指南。

如果您訪問 AWS 編程方式， AWS 提供軟體開發套件 (SDK) 和命令列介面 (CLI)，以使用您的認證以密碼編譯方式簽署您的要求。如果你不使用 AWS 工具，您必須自己簽署請求。如需使用建議的方法自行簽署要求的詳細資訊，請參閱簽署 AWS API《IAM用戶指南》中的請求。

無論您使用何種身分驗證方法，您可能都需要提供額外的安全性資訊。例如 AWS 建議您使用多重要素驗證 (MFA) 來增加帳戶的安全性。要了解更多信息，請參閱中的多因素身份驗證 AWS IAM Identity Center 用戶指南和使用多因素身份驗證（MFA）AWS (在 IAM 使用者指南中)

AWS 帳戶 根使用者

當您創建 AWS 帳戶時，您會從一個擁有完整存取權限的登入身分開始 AWS 服務 和帳戶中的資源。這個身份被稱為 AWS 帳戶 root 使用者，並透過使用您用來建立帳戶的電子郵件地址和密碼登入來存取。強烈建議您不要以根使用者處理日常任務。保護您的根使用者憑證，並將其用來執行只能由根使用者執行的任務。如需需要您以 root 使用者身分登入的完整工作清單，請參閱《使用指南》中的〈需要root 使用者認證的IAM工作〉。

IAM 使用者和群組

使IAM用者是您的身分 AWS 帳戶 具有單一人員或應用程式的特定權限。在可能的情況下，我們建議您仰賴臨時登入資料，而不要建立具有長期認證 (例如密碼和存取金鑰) 的IAM使用者。不過，如果您的特

定使用案例需要使用IAM者的長期認證，建議您輪換存取金鑰。如需詳細資訊，請參閱《使用指南》中的「IAM定期輪換存取金鑰」以瞭解需要長期認證的使用案例。

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

使用者與角色不同。使用者只會與單一人員或應用程式建立關聯，但角色的目的是在由任何需要它的人員取得。使用者擁有永久的長期憑證，但角色僅提供暫時憑證。要了解更多信息，請參閱《IAM用戶指南》中的創建用戶（而不是角色）的IAM時間。

IAM角色

IAM角色是您的身份 AWS 帳戶 具有特定權限。它類似於用IAM戶，但不與特定人員相關聯。您可以暫時IAM擔任 AWS Management Console 通過切換角色。您可以通過調用一個角色 AWS CLI 或 AWS API操作或通過使用自定義URL。如需有關使用角色方法的詳細資訊，請參閱《使用指南》中的IAM〈使用IAM角色〉。

IAM具有臨時認證的角色在下列情況下很有用：

- 聯合身分使用者存取 — 如需向聯合身分指派許可，請建立角色，並為角色定義許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並獲授予由角色定義的許可。如需聯合角色的相關資訊，請參閱《使用指南》中的〈建立第三方身分識別提供IAM者的角色〉。如果您使用IAM身分識別中心，則需要設定權限集。為了控制身分驗證後可以存取的內IAM容，IAMIdentity Center 會將權限集與中的角色相關聯。如需有關權限集的資訊，請參閱 AWS IAM Identity Center 使用者指南。
- 暫時IAM使用者權限 — IAM 使用者或角色可以假定某個IAM角色，暫時取得特定工作的不同權限。
- 跨帳戶存取 — 您可以使用IAM角色允許不同帳戶中的某個人 (受信任的主體) 存取您帳戶中的資源。角色是授予跨帳戶存取權的主要方式。但是，有一些 AWS 服務，您可以將策略直接附加到資源（而不是使用角色作為代理）。若要瞭解跨帳戶存取角色與以資源為基礎的政策之間的差異，請參閱《IAM使用指南》IAM中的〈跨帳號資源存取〉。
- 跨服務訪問 — 一些 AWS 服務 使用其他中的功能 AWS 服務。 例如，當您在服務中撥打電話時，該服務通常會在 Amazon 中執行應用程式EC2或將物件存放在 Amazon S3 中。服務可能會使用呼叫主體的許可、使用服務角色或使用服務連結角色來執行此作業。
  - 轉寄存取工作階段 (FAS) — 當您使用使用IAM者或角色在 AWS，您被視為校長。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS使用主體呼叫 AWS 服務，與請求相結合 AWS 服務 向下游服務提出請求。FAS只有當服務收到需要與其他人互動的請求時才會發出請求 AWS 服務 或要完成的資源。在此情況下，您必須具有執行這兩個動作的許可。有關提出FAS請求時的策略詳細信息，請參閱轉發訪問會話。

- 服務角色 — 服務角IAM色是服務代表您執行動作的角色。IAM管理員可以從中建立、修改和刪除服務角色IAM。如需詳細資訊，請參閱建立角色以將權限委派給 AWS 服務 (在 IAM 使用者指南中)
- 服務連結角色 — 服務連結角色是連結至 AWS 服務。 服務可以扮演角色代表您執行動作。服務連結角色會出現在 AWS 帳戶 並由該服務擁有。IAM管理員可以檢視 (但無法編輯服務連結角色) 的權限。

- 在 Amazon 上執行的應用程式 EC2 — 您可以使用IAM角色來管理在執行個體上EC2執行並製作的應用程式的臨時登入資料 AWS CLI 或 AWS API請求。這比在EC2執行個體中儲存存取金鑰更可取。若要指派 AWS EC2執行個體的角色並讓它可供其所有應用程式使用，您可以建立連接至執行個體的執行個體設定檔。執行個體設定檔包含角色，可讓執行個體上EC2執行的程式取得臨時登入資料。如需詳細資訊，請參閱使用者指南中的使用IAM角色將許可授與在 Amazon EC2 執行個體上執行的應IAM用程式。

要了解是否使用IAM角色還是用IAM戶，請參閱《用戶指南》中的「IAM創建IAM角色的時機（而不是用戶）」。

使用政策管理存取權

您可以控制存取 AWS 藉由建立原則並將其附加至 AWS 身分識別或資源。原則是中的物件 AWS 當與身分識別或資源相關聯時，會定義其權限。 AWS 當主參與者 (使用者、root 使用者或角色工作階段) 提出要求時，評估這些原則。政策中的許可決定是否允許或拒絕請求。大多數策略都儲存在 AWS 作為JSON文件。如需有關JSON原則文件結構和內容的詳細資訊，請參閱《IAM使用指南》中的策略概觀。JSON

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

預設情況下，使用者和角色沒有許可。若要授與使用者對所需資源執行動作的權限，IAM管理員可以建立IAM策略。然後，系統管理員可以將IAM原則新增至角色，使用者可以擔任這些角色。

IAM原則會定義動作的權限，不論您用來執行作業的方法為何。例如，假設您有一個允許 `iam:GetRole` 動作的政策。具有該策略的使用者可以從 AWS Management Console，該 AWS CLI，或 AWS API.

身分型政策

以身分識別為基礎的原則是您可以附加至身分識別 (例如使用者、使用IAM者群組或角色) 的JSON權限原則文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。若要瞭解如何建立以身分識別為基礎的策略，請參閱《IAM使用指南》中的〈建立IAM策略〉。

身分型政策可進一步分類成內嵌政策或受管政策。內嵌政策會直接內嵌到單一使用者、群組或角色。受管理的策略是獨立策略，您可以將其附加到您的多個使用者、群組和角色 AWS 帳戶。 受管政策包括 AWS 受管理的政策和客戶管理的政策。若要了解如何在受管策略或內嵌策略之間進行選擇，請參閱《IAM使用手冊》中的「在受管策略和內嵌策略之間進行選擇」。

資源型政策

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

資源型政策是位於該服務中的內嵌政策。你不能使用 AWS 在以資源為基礎的策略IAM中受管理的策略。

存取控制清單 (ACLs)

存取控制清單 (ACLs) 控制哪些主參與者 (帳戶成員、使用者或角色) 具有存取資源的權限。ACLs類似於以資源為基礎的策略，雖然它們不使用JSON政策文件格式。

Amazon S3， AWS WAF和 Amazon VPC 是支持的服務的例子ACLs。若要進一步了解ACLs，請參閱 Amazon 簡單儲存服務開發人員指南中的存取控制清單 (ACL) 概觀。

其他政策類型

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

- 權限界限 — 權限界限是一項進階功能，您可以在其中設定以身分識別為基礎的原則可授與給IAM實體 (IAM使用者或角色) 的最大權限。您可以為實體設定許可界限。所產生的許可會是實體的身分型政策和其許可界限的交集。會在 `Principal` 欄位中指定使用者或角色的資源型政策則不會受到許可界限限制。所有這類政策中的明確拒絕都會覆寫該允許。如需有關權限界限的詳細資訊，請參閱《IAM使用指南》中的IAM實體的權限界限。
- 服務控制策略（SCPs）— SCPs 是指定中組織或組織單位（OU）的最大權限的JSON策略 AWS Organizations. AWS Organizations 是一種用於分組和集中管理多個服務 AWS 帳戶 您的企業擁有。如果您啟用組織中的所有功能，則可以將服務控制策略 (SCPs) 套用至您的任何或所有帳戶。SCP限制成員帳戶中實體的權限，包括每個 AWS 帳戶根使用者。 如需有關 Organizations 的詳細資訊 SCPs，請參閱 AWS Organizations 使用者指南。
- 工作階段政策 – 工作階段政策是一種進階政策，您可以在透過編寫程式的方式建立角色或聯合使用者的暫時工作階段時，作為參數傳遞。所產生工作階段的許可會是使用者或角色的身分型政策和工作

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

多種政策類型

將多種政策類型套用到請求時，其結果形成的許可會更為複雜、更加難以理解。若要瞭解如何 AWS 決定當涉及多個原則類型時是否允許要求，請參閱《IAM使用指南》中的「原則評估邏輯」。

Resource Groups 如何使用 IAM

在您用IAM來管理 Resource Groups 的存取權限之前，您應該瞭解哪些IAM功能可用於 Resource Groups。若要取得 Resource Groups 和其他 AWS 服務如何使用的高階檢視IAM，請參閱IAM使用指南IAM中的可使用的AWS 服務。

主題

- Resource Groups 以識別為基礎的策略
- 資源型政策
- 以 Resource Groups 標籤為基礎的授權
- Resource Groups IAM 角色

Resource Groups 以識別為基礎的策略

使用以IAM身分識別為基礎的策略，您可以指定允許或拒絕的動作和資源，以及允許或拒絕動作的條件。Resource Groups 支援特定動作、資源和條件索引鍵。若要瞭解您在JSON策略中使用的所有元素，請參閱《使用IAM者指南》中的《IAMJSON策略元素參考》。

動作

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

JSON策略`Action`元素描述了您可以用來允許或拒絕策略中存取的動作。策略動作通常與關聯的 AWS API操作具有相同的名稱。有一些例外情況，例如沒有匹配API操作的僅限權限的操作。也有一些作業需要政策中的多個動作。這些額外的動作稱為相依動作。

政策會使用動作來授予執行相關聯動作的許可。

Resource Groups 中的策略動作會在動作之前使用下列前置詞：`resource-groups:`標籤編輯器動作完全在主控台中執行，但`resource-explorer`在記錄項目中具有前置詞。

例如，若要授與某人使用「Resource Groups」作業建立「Resource Groups」群組的權限，您可以將該resource-groups:CreateGroup動CreateGroupAPI作包含在他們的策略中。政策陳述式必須包含 Action 或 NotAction 元素。Resource Groups 會定義自己的一組動作，描述您可以使用此服務執行的工作。

若要在單一陳述式中指定多個 Resource Groups 和標籤編輯器動作，請以逗號分隔它們，如下所示：

```
"Action": [
      "resource-groups:action1",
      "resource-groups:action2",
      "resource-explorer:action3"
```

您也可以使用萬用字元 (*) 來指定多個動作。例如，若要指定開頭是 List 文字的所有動作，請包含以下動作：

```
"Action": "resource-groups:List*"
```

若要查看「Resource Groups」動作清單，請參閱《使用指南》 AWS Resource Groups中的 「動作」、「資源」和「條IAM件索引鍵」。

資源

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

ResourceJSON原則元素會指定要套用動作的一個或多個物件。陳述式必須包含 Resource 或 NotResource 元素。最佳做法是使用其 Amazon 資源名稱 (ARN) 指定資源。您可以針對支援特定資源類型的動作 (稱為資源層級許可) 來這麼做。

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

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

唯一的 Resource Groups 資源是一個群組。群組資源的ARN格式如下：

```
arn:${Partition}:resource-groups:${Region}:${Account}:group/${GroupName}
```

如需的格式的詳細資訊ARNs，請參閱 Amazon 資源名稱 (ARNs) 和 AWS 服務命名空間。

例如，若要在陳述式中指定my-test-group資源群組，請使用下列指令ARN：

```
"Resource": "arn:aws:resource-groups:us-east-1:123456789012:group/my-test-group"
```

若要指定屬於特定帳戶的所有群組，請使用萬用字元 (*)：

```
"Resource": "arn:aws:resource-groups:us-east-1:123456789012:group/*"
```

某些 Resource Groups 動作 (例如用來建立資源的動作) 無法在特定資源上執行。在這些情況下，您必須使用萬用字元 (*)。

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

某些 Resource Groups API 動作可能涉及多個資源。例如，DeleteGroup刪除群組，因此呼叫主參與者必須具有刪除特定群組或所有群組的權限。若要在單一陳述式中指定多個資源，請以ARNs逗號分隔。

```
"Resource": [
  "resource1",
  "resource2"
]
```

若要查看 Resource Groups 資源類型及其清單ARNs，並瞭解可以指定每個資源的ARN動作，請參閱《IAM使用指南》 AWS Resource Groups中的動作、資源和條件索引鍵。

條件索引鍵

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

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

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

您也可以在指定條件時使用預留位置變數。例如，只有在IAM使用者名稱標記資源時，您才可以授與IAM使用者存取資源的權限。如需詳細資訊，請參閱《IAM使用指南》中的IAM政策元素：變數和標籤。

AWS 支援全域條件金鑰和服務特定條件金鑰。若要查看所有 AWS 全域條件索引鍵，請參閱《使用指南》中的AWS 全域條件內IAM容索引鍵。

Resource Groups 會定義自己的一組條件索引鍵，並支援使用某些全域條件索引鍵。若要查看所有 AWS 全域條件索引鍵，請參閱使用指南中的AWS 全域條件內IAM容索引鍵。

若要查看 Resource Groups 條件索引鍵清單，並瞭解您可以使用條件索引鍵的動作和資源，請參閱《使IAM用指南》 AWS Resource Groups中的動作、資源和條件索引鍵。

範例

若要檢視 Resource Groups 以身分識別為基礎的策略範例，請參閱。AWS Resource Groups 身分型政策範例

資源型政策

Resource Groups 不支援以資源為基礎的政策。

以 Resource Groups 標籤為基礎的授權

您可以將標記附加到 Resource Groups 中的群組，或將請求中的標籤傳遞給 Resource Groups。如需根據標籤控制存取，請使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 條件索引鍵，在政策的條件元素中，提供標籤資訊。您可以在建立或更新群組時，將標記套用至群組。如需有關在 Resource Groups 中標記群組的詳細資訊，請參閱本指南更新群組於 AWS Resource Groups中的建立以查詢為基礎的群組 AWS Resource Groups和。

若要檢視身分型政策範例，以根據該資源上的標籤來限制存取資源，請參閱以標為為為為基礎的授。

Resource Groups IAM 角色

IAM角色是您 AWS 帳戶中具有特定權限的實體。Resource Groups 沒有或不使用服務角色。

搭配 Resource Groups 使用臨時認證

在 Resource Groups 中，您可以使用臨時認證來登入同盟、擔任IAM角色或擔任跨帳戶角色。您可以透過呼叫AssumeRole或之類的 AWS STS API作業來取得臨時安全登入資料GetFederationToken。

服務連結角色

服務連結角色可讓 AWS 服務存取其他服務中的資源，以代表您完成動作。

Resource Groups 沒有或使用服務連結角色。

服務角色

此功能可讓服務代表您擔任服務角色。

Resource Groups 沒有或不使用服務角色。

AWS Resource Groups 的 AWS 受管政策

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

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

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

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

AWS資源群組的管理策略

- ResourceGroupsServiceRolePolicy

AWS 受管政策：ResourceGroupsServiceRolePolicy

您無法附加`ResourceGroupsServiceRolePolicy`到您自己的任何 IAM 實體。此原則只能附加至允許資源群組代表您執行動作的服務連結角色。如需詳細資訊，請參閱對 Resource Groups 使用服務連結角色。

此原則會授與資源群組擷取資源群組中資源的相關資訊所需的權限，以及任何資源群組AWS CloudFormation這些資源所屬的堆疊。這可讓資源群組產生CloudWatch群組生命週期事件功能的事件。

要查看此最新版本AWS受管政策，請參閱`ResourceGroupsServiceRolePolicy`在 IAM 主控台中。

AWS受管理的策略： ResourceGroupsandTagEditorFullAccess

當您將原則附加至主參與者實體時，您會授與原則中定義的實體權限。AWS受管理的原則可讓您輕鬆地將適當的權限指派給使用者、群組和角色，而不是必須自行撰寫原則。

此原則會授與完整存取資源群組和標籤編輯器功能所需的權限。

要查看此最新版本AWS受管政策，請參閱ResourceGroupsandTagEditorFullAccess在 IAM 主控台中。

如需有關此原則的詳細資訊，請參閱 ResourceGroupsandTagEditorFullAccess在AWS受管理策略參考指南。

AWS受管理的策略： ResourceGroupsandTagEditorReadOnly存取

當您將原則附加至主參與者實體時，您會授與原則中定義的實體權限。AWS受管理的原則可讓您輕鬆地將適當的權限指派給使用者、群組和角色，而不是必須自行撰寫原則。

此原則授與資源群組和標籤編輯器功能唯讀存取權所需的權限。

要查看此最新版本AWS受管政策，請參閱ResourceGroupsandTagEditorReadOnlyAccess在 IAM 主控台中。

如需有關此原則的詳細資訊，請參閱 ResourceGroupsandTagEditorReadOnly存取在AWS受管理策略參考指南。

資源群組更新至AWS受管理政策

檢視有關更新的詳細資訊AWS由於此服務開始追蹤這些變更，因此資源群組的受管理策略。如需有關此頁面變更的自動警示，請訂閱資源群組文件記錄頁面。

變更	描述	日期
政策更新 —ResourceGroupsandTagEditorFullAccess	資源群組已更新策略以包含其他策略AWS CloudFormation權限。	2023年8月10日
政策更新 —ResourceGroupsandTagEditorReadOnlyAccess	資源群組已更新策略以包含其他策略AWS CloudFormation權限。	2023年8月10日

變更	描述	日期
新政策 —ResourceGroupsServiceRolePolicy	資源群組新增了新策略以支援其服務連結角色。	2022 年 11 月 17 日
資源群組已開始追蹤變更	資源群組已開始追蹤其變更AWS受管理的策略。	2022 年 11 月 17 日

對 Resource Groups 使用服務連結角色

AWS Resource Groups 使用 AWS Identity and Access Management (IAM) 服務連結的角色。服務連結角色是直接連結至 Resource Groups 的一種特殊 IAM 角色類型，可直接連結。服務連結角色由預先定義，並包含服務代您呼叫其他服務所需AWS 服務的所有許可。

服務連結角色可讓設定 Resource Groups 簡單，因為您不必手動新增必要的許可。Resource Groups 定義其服務連結角色的許可，並設定義其服務連結角色的信任政策，以確保僅有 Resource Groups 服務可以擔任其角色。定義的許可包括信任政策和許可政策，並且該許可政策不能連接到任何其他 IAM 實體。

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

Resource Groups 的服務連結角色許可

Resource Groups 使用下列服務連結角色支援群組事件支援群組事件。選擇角色名稱上的連結，以在建立 IAM 主控台後檢視該角色。

- AWSServiceRoleForResourceGroups

Resource Groups 使用此角色中的權限來查詢擁AWS 服務有您資源的權限，以協助解析群組成員資格並保留群組 up-to-date。它可讓 Resource Groups 向 Amazon EventBridge 服務發出與服務相關的事件。

服***AWSServiceRoleForResourceGroups***務連結角色信任下列服務來擔任此角色：

- `resourcegroups.amazonaws.com`

附加至角色的權限來自下列AWS受管理的策略。選擇政策上的連結，以檢視 IAM 主控台中的政策。

- AWS Resource Groups # AWS ####

為 Resource Groups 建立服務連結角色

> **Important**
>
> 此服務連結的角色可以顯示在您的帳戶，如果您於其他服務中完成一項動作時，可以使用支援此服務的功能。如需詳細資訊，請參閱我的新角色出現在我的AWS 帳戶.

若要建立服務連結角色，請開啟群組開啟「群組」功能。

編輯 Resource Groups 連結角色

Resource Groups 不允許您編輯 AWSServiceRoleForResourceGroups 服務連結角色。因為可能有各種實體會參考服務連結角色，所以您無法在建立角色之後變更其名稱。然而，您可使用 IAM 來編輯角色描述。如需詳細資訊，請參閱《IAM 使用者指南》中的編輯服務連結角色。

刪除服務連結 Resource Groups

只有在關閉群組之後，您才能刪除服務連結角色

> **Important**
>
> - AWS防止您移除服務連結角色，直到您首次關閉建立該角色的群組生命週期事件功能為止。
> - 建議您不要刪除服務連結角色，只要您的AWS 帳戶. 如果您刪除此角色，則 Resource Groups 服務無法與其他AWS 服務人互動以管理您的群組。

手動刪除服務連結角色

使用 IAM 主控台、AWS CLI 或 AWS API 來刪除 AWSServiceRoleForResourceGroups 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。

Console

刪除服 Resource Groups 結角色

1. 開啟 IAM 主控台前往「角色」頁面。
2. 尋找名為的角色 AWSServiceRoleForResourceGroups，然後選取該角色旁邊的核取方塊。
3. 選擇 Delete (刪除)。
4. 在方塊中輸入角色的名稱，以確認刪除角色的意圖，然後選擇 [刪除]。

此角色會消失在 IAM 中的角色清單中消失。

AWS CLI

刪除服 Resource Groups 結角色

若要刪除角色，請使用完全相同的參數輸入以下命令。請勿取代任何值。

```
$ aws iam delete-service-linked-role \
    --role-name AWSServiceRoleForResourceGroups
{
    "DeletionTaskId": "task/aws-service-role/resource-groups.amazonaws.com/
AWSServiceRoleForResourceGroups/34e58943-e9a5-4220-9856-fc565EXAMPLE"
}
```

命令會傳回工作。實際的角色刪除會以非同步方式發生。您可以將提供的工作識別碼傳遞給以下列 AWS CLI命令檢查角色的刪除狀態。

```
$ aws iam get-service-linked-role-deletion-status \
    --deletion-task-id "task/aws-service-role/resource-groups.amazonaws.com/
AWSServiceRoleForResourceGroups/34e58943-e9a5-4220-9856-fc565EXAMPLE"
{
    "Status": "SUCCEEDED"
}
```

Resource Groups 服務連結角色的支援區域

Resource Groups 支援在所有提供服務的服務中使用服務連結角色使用服務連結角色。AWS 區域如需詳細資訊，請參閱 AWS 區域與端點。

AWS Resource Groups 身分型政策範例

根據預設，IAM 主體 (例如角色和使用者) 不具備建立或修改 Resource Groups 資源的許可。他們也無法使用 AWS Management Console、AWS CLI 或 AWS API 執行任務。IAM 管理員必須建立 IAM 政策，授予主體在指定資源上執行特定 API 操作的所需許可。管理員接著必須將這些政策連接至需要這些許可的主參與者。

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

主題

政策最佳實務

以身分為基礎的政策會判斷您帳戶中的某個人員是否可以建立、存取或刪除 Resource Groups 資源。這些動作可能會讓您的 AWS 帳戶 產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

- 開始使用 AWS 受管政策並朝向最低權限許可的目標邁進 – 若要開始授予許可給使用者和工作負載，請使用 AWS 受管政策，這些政策會授予許可給許多常用案例。它們可在您的 AWS 帳戶 中使用。我們建議您定義特定於使用案例的 AWS 客戶管理政策，以便進一步減少許可。如需詳細資訊，請參閱 IAM 使用者指南中的 AWS 受管政策或任務職能的 AWS 受管政策。
- 套用最低權限許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的許可。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需使用 IAM 套用許可的詳細資訊，請參閱 IAM 使用者指南中的 IAM 中的政策和許可。
- 使用 IAM 政策中的條件進一步限制存取權 – 您可以將條件新增至政策，以限制動作和資源的存取。例如，您可以撰寫政策條件，指定必須使用 SSL 傳送所有請求。您也可以使用條件來授予對服務動作的存取權，前提是透過特定 AWS 服務 (例如 AWS CloudFormation) 使用條件。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM JSON 政策元素：條件。
- 使用 IAM Access Analyzer 驗證 IAM 政策，確保許可安全且可正常運作 – IAM Access Analyzer 驗證新政策和現有政策，確保這些政策遵從 IAM 政策語言 (JSON) 和 IAM 最佳實務。IAM Access

Analyzer 提供 100 多項政策檢查及切實可行的建議，可協助您編寫安全且實用的政策。如需詳細資訊，請參閱 IAM 使用者指南中的 IAM Access Analyzer 政策驗證。

- 需要多重要素驗證 (MFA) — 如果存在需要 IAM 使用者或根使用者的情況AWS 帳戶，請開啟 MFA 提供額外的安全性。若要在呼叫 API 操作時要求 MFA，請將 MFA 條件新增至您的政策。如需詳細資訊，請參閱 IAM 使用者指南中的設定 MFA 保護的 API 存取。

有關 IAM 中最佳實務的詳細資訊，請參閱 IAM 使用者指南中的 IAM 安全最佳實務。

使用 Resource Groups 主控台和 API

若要存取和AWS Resource Groups 這些許可必須允許您列出和檢視您AWS帳戶中 Resource Groups 資源的詳細資訊。如果您建立比最基本必要許可更嚴格的身分型政策，則對於具有該政策的主體 (IAM 角色或使用者) 而言，主控台和 API 命令就無法如預期運作。

為確保那些實體仍可使用 Resource Groups，請將以下政策 (或包含下列政策中許可的政策) 連接到實體。如需詳細資訊，請參閱《IAM 使用者指南》中的新增許可到使用者。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "resource-groups:*",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "tag:GetResources",
        "tag:TagResources",
        "tag:UntagResources",
        "tag:getTagKeys",
        "tag:getTagValues",
        "resource-explorer:List*"
      ],
      "Resource": "*"
    }
  ]
}
```

如需將存取 Resource Groups 的詳細資訊，請參閱本指南授與使用權限 AWS Resource Groups 和標籤編輯器中的。

允許使用者檢視他們自己的許可

此範例會示範如何建立政策，允許 IAM 使用者檢視連接到他們使用者身分的內嵌及受管政策。此政策包含在主控台上，或是使用 AWS CLI 或 AWS API 透過編寫程式的方式完成此動作的許可。

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

以標為為為為基礎的授

您可以身分為基礎的政策中使用條件，根據以標為基礎的授權。此範如何建立允許檢視資源 (在此範例中為資源群組中資源群組) 的政策。不過，只在群組代為project具有與連接至主要主體的授權project

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "resource-groups:ListGroups",
            "Resource": "arn:aws:resource-groups::region:account_ID:group/group_name"
        },
        {
            "Effect": "Allow",
            "Action": "resource-groups:ListGroups",
            "Resource": "arn:aws:resource-groups::region:account_ID:group/group_name",
            "Condition": {
                "StringEquals": {"aws:ResourceTag/project": "${aws:PrincipalTag/
project}"}
            }
        }
    ]
}
```

您可以將此政策連接至您帳戶中的主參與者。如果具有標籤索引鍵project和標籤值的主參與者alpha嘗試檢視資源群組，則該群組也必須加上標籤project=alpha。否則，用戶將被拒絕訪問。條件標籤鍵 project 符合 Project 和 project，因為條件索引鍵名稱不區分大小寫。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM JSON 政策元素：條件。

疑難排解 AWS Resource Groups 身分和存取

使用下列資訊可協助您診斷和修正使用 Resource Groups 和 IAM 時可能會遇到的常見問題。

主題

- 我沒有在 Resource Groups 中執行動作的授權
- 我沒有授權執行 iam：PassRole
- 我想允許我 AWS 帳戶以外的人員存取我的 Resource Groups

我沒有在 Resource Groups 中執行動作的授權

如果 AWS Management Console 告訴您您沒有執行動作的授權，則您必須聯絡管理員以尋求協助。您的管理員是為您提供簽署憑證的人員。

當使用者mateojackson嘗試使用主控台來檢視群組的詳細資料，但沒有resource-groups:ListGroups權限時，就會發生下列範例錯誤。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to
 perform: resource-groups:ListGroups on resource: arn:aws:resource-groups::us-
west-2:123456789012:group/my-test-group
```

在此情況下，Mateo 會請求管理員更新他的政策，允許他使用 my-test-group 動作存取 resource-groups:ListGroups 資源。

我沒有授權執行 iam：PassRole

如果您收到未授權執行iam:PassRole動作的錯誤訊息，則必須更新您的原則，以允許您將角色傳遞給 Resource Groups。

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

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

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

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

如果您需要協助，請聯絡您的 AWS 管理員。您的管理員提供您的簽署憑證。

我想允許我 AWS 帳戶以外的人員存取我的 Resource Groups

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

如需進一步了解，請參閱以下內容：

- 若要瞭解 Resource Groups 是否支援這些功能，請參閱Resource Groups 如何使用 IAM。

- 若要了解如何提供對您所擁有資源 AWS 帳戶 的存取權，請參閱 IAM 使用者指南中您擁有的另一 AWS 帳戶 個 IAM 使用者提供存取權限。
- 若要了解如何將資源存取權提供給第三方 AWS 帳戶，請參閱 IAM 使用者指南中的提供第三方 AWS 帳戶 擁有的存取權。
- 如需了解如何透過聯合身分提供存取權，請參閱 IAM 使用者指南中的將存取權提供給在外部進行身分驗證的使用者 (聯合身分)。
- 若要了解跨帳戶存取使用角色和以資源為基礎的政策之間的差異，請參閱 IAM 使用者指南中的 IAM 中的跨帳戶資源存取。

Resource Groups 中的記錄和監控

所有AWS Resource Groups動作都會登入AWS CloudTrail。

使用 AWS CloudTrail 記錄 AWS Resource Groups API 呼叫

AWS Resource Groups和 Tag Editor 與整合AWS CloudTrail，此服務會提供 Resource Groups 或標籤編輯器中由使用者、角色或採取動作的紀錄。AWS CloudTrail 將 Resource Groups 的所有 API 呼叫擷取為事件，包括來自 Resource Groups 或標籤編輯器主控台的呼叫，以及來自對 Resource Groups API 發出的程式碼呼叫。如果您建立追蹤，就可以將 CloudTrail 事件持續交付到 Amazon S3 儲存貯體，包括 Resource Groups 的事件。如果您不設定追蹤，仍然可以透過 CloudTrail 主控台中的 Event history (事件歷史記錄) 檢視最新的事件。您可以使用 CloudTrail收集的資訊來判斷向 Resource Groups 發出的請求，以及發出請求的 IP 地址、人員、時間和其他詳細資訊。

若要進一步了解 CloudTrail，請參閱使AWS CloudTrail用者指南。

Resource Groups 資訊 CloudTrail

CloudTrail 當您建立AWS帳戶時，系統即會在帳戶中啟用。當 Resource Groups 中或 Tag Editor 主控台中發生活動時，系統會將該活動記錄至事件，並將其他AWS服務 CloudTrail事件記錄到 Event history (事件歷史記錄) 中。您可以檢視、搜尋和下載 AWS 帳戶的最新事件。如需詳細資訊，請參閱使用 CloudTrail 事件歷程記錄檢視事件。

如需AWS帳戶中正在進行事件的記錄 (包括 Resource Groups 的事件)，請建立線索。追蹤可讓您 CloudTrail 將日誌檔案傳送至 Amazon S3 儲存貯體。根據預設，當您在主控台建立權杖時，權杖會套用到所有區域。線索會記錄來自 AWS 分割區中所有區域的事件，然後將所有日誌檔案交付到您指定的 Amazon S3 儲存貯體。此外，您可以設定其他 AWS 服務，以進一步分析和處理 CloudTrail 日誌中所收集的事件資料。如需詳細資訊，請參閱：

- 建立追蹤的概觀
- CloudTrail 支援的服務和整合
- 設定的 Amazon SNS 通知 CloudTrail
- 從多個區域接收 CloudTrail 日誌檔案及接收多個帳戶的 CloudTrail 日誌檔案

所有 Resource Groups 動作均由 CloudTrail 記錄，列在 AWS Resource GroupsAPI 參考中。中的「Resource Groups」動作 CloudTrail 會顯示為以 API 端點作`resource-groups.amazonaws.com`為其來源的事件。例如，呼叫`CreateGroup`、`GetGroup`、和`UpdateGroupQuery`動作會在 CloudTrail 記錄檔中產生項目。控制台中的標籤編輯器動作由記錄 CloudTrail，並顯示為內部 API 端點作`resource-explorer`為其來源的事件。

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

- 該請求是否使用根或 IAM 使用者憑證提出。
- 提出該請求時，是否使用了特定角色或聯合身分使用者的暫時安全憑證。
- 該請求是否由另一項 AWS 服務提出。

如需更多詳細資訊，請參閱 CloudTrail `userIdentity` 元素。

了解 Resource Groups 日誌檔案項目

追蹤是一種組態，能讓事件以日誌檔案的形式交付至您指定的 Amazon S3 儲存貯體。 CloudTrail 日誌檔案包含一個或多個日誌項目。一個事件為任何來源提出的單一請求，並包含請求動作、請求的日期和時間、請求參數等資訊。 CloudTrail 日誌檔案並非依公有 API 呼叫追蹤記錄的堆疊排序，因此不會以任何特定順序出現。

以下範例顯示的是展示動作的 CloudTrail 日誌項目`CreateGroup`。

```
{"eventVersion":"1.05",
"userIdentity":{
    "type":"AssumedRole",
    "principalId":"ID number:AWSResourceGroupsUser",
    "arn":"arn:aws:sts::831000000000:assumed-role/Admin/AWSResourceGroupsUser",
    "accountId":"831000000000","accessKeyId":"ID number",
    "sessionContext":{
        "attributes":{
            "mfaAuthenticated":"false",
            "creationDate":"2018-06-05T22:03:47Z"
            },
```

```
        "sessionIssuer":{
            "type":"Role",
            "principalId":"ID number",
            "arn":"arn:aws:iam::831000000000:role/Admin",
            "accountId":"831000000000",
            "userName":"Admin"
            }
        }
    },
"eventTime":"2018-06-05T22:18:23Z",
"eventSource":"resource-groups.amazonaws.com",
"eventName":"CreateGroup",
"awsRegion":"us-west-2",
"sourceIPAddress":"100.25.190.51",
"userAgent":"console.amazonaws.com",
"requestParameters":{
    "Description": "EC2 instances that we are using for application staging.",
    "Name": "Staging",
    "ResourceQuery": {
      "Query": "string",
      "Type": "TAG_FILTERS_1_0"
      },
    "Tags": {
      "Key":"Phase",
      "Value":"Stage"
      }
    },
"responseElements":{
    "Group": {
      "Description":"EC2 instances that we are using for application staging.",
      "groupArn":"arn:aws:resource-groups:us-west-2:831000000000:group/Staging",
      "Name":"Staging"
     },
    "resourceQuery": {
      "Query":"string",
      "Type":"TAG_FILTERS_1_0"
     }
    },
"requestID":"de7z64z9-d394-12ug-8081-7zz0386fbcb6",
"eventID":"8z7z18dz-6z90-47bz-87cf-e8346428zzz3",
"eventType":"AwsApiCall",
"recipientAccountId":"831000000000"
}
```

Resource Groups 的符合性驗證

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

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

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

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

> **Note**
>
> 並非所有 AWS 服務 人都HIPAA符合資格。如需詳細資訊，請參閱合HIPAA格服務參考。

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

Resource Groups 中的復原功能

AWS Resource Groups執行內部服務資源的自動備份。這些備份不是使用者可設定的。備份，無論是靜態備份還是傳輸中加密。Resource Groups 將客戶數據存儲在 Amazon DynamoDB 中。

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

即使完全丟失用户資源組也不會導致客户數據丟失，因為大多數客户數據都是跨AWS可用區域 (AZ)。如果您意外刪除羣組，請聯繫AWS SupportCenter。

如需 AWS 區域 與可用區域的詳細資訊，請參閱AWS全球基礎架構。

Resource Groups 的基礎結構安全

沒有其他方法可隔離 Resource Groups 所提供的服務或網路流量。如果適用，請使用 AWS特定的隔離。您可以在中使用 Resource Groups API 和主控台VPC來協助最大化隱私權和基礎結構安全性。

作為託管服務， AWS Resource Groups 受到 AWS 全球網絡安全的保護。有關 AWS 安全服務以及如何 AWS 保護基礎架構的詳細資訊，請參閱AWS 雲端安全 若要使用基礎架構安全性的最佳做法來設計您的 AWS 環境，請參閱安全性支柱架構良 AWS 好的架構中的基礎結構保護。

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

- 傳輸層安全性 (TLS)。我們需要 TLS 1.2 並推薦 TLS 1.3。
- 具有完美前向保密（ ）的密碼套件，例如（短暫的迪菲-赫爾曼PFS）或DHE（橢圓曲線短暫迪菲-赫爾曼）。ECDHE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主體相關聯的秘密存取金鑰來簽署。或者，您可以透過 AWS Security Token Service (AWS STS) 來產生暫時安全憑證來簽署請求。

Resource Groups 不支援以資源為基礎的政策。

Resource Groups

以下最佳實務為一般準則，並不代表完整的安全解決方案。這些最佳實務可能不適用或無法滿足您的環境需求，因此請將其視為實用建議就好，而不要當作是指示。

- 使用最小權限原則將存取權授與群組。Resource Groups 層級的許可。僅在特定使用者的需要時才授與特定群組的存取權。避免在將權限指派給所有使用者或所有群組的政策陳述式中使用星號。如需有關最低權限的詳細資訊，請參閱 IAM 使用者指南中的授與最低權限。
- 將私人信息保留在公共領域之外。 群組的名稱會被視為服務中繼資料。群組名稱未加密。請勿在群組名稱中加入敏感資訊。群組描述是私人的。

  請勿在標籤鍵或標籤值中放置私密或敏感資訊。
- 在適當時根據標記使用授權。Resource Groups 支援以標籤為基礎的授權。您可以標記群組，然後更新附加至 IAM 主體 (例如使用者和角色) 的政策，以根據套用至群組的標記來設定其存取層級。有關如何根據標籤使用授權的詳細AWS資訊，請參閱 IAM 使用者指南中的使用資源標籤控制對資源的存取。

  許多AWS服務支援以標籤為基礎的授權。請注意，可能會針對群組中的成員資源設定以標籤為基礎的授權。如果群組資源的存取受到標籤限制，未經授權的使用者或群組可能無法對這些資源執行動作或自動化作業。例如，如果您其中一個群組中的 Amazon EC2 執行個體標記標記了標籤金鑰`Confidentiality`且標籤值為`High`，且您未獲授權對已標記的資源執行命令`Confidentiality:High`，則您在 EC2 執行個體上執行的動作或自動化操作也會失敗，即使資源群組中其他資源的動作成功也是如此。如需哪些服務對其資源支援以標籤為基礎的授權的詳細資訊，請參閱 IAM 使用者指南中的與 IAM 搭配使用的AWS服務。

  有關為資源開發標記策略的詳細AWS資訊，請參閱AWS標記策略。

Resource Groups 的服務配額

下表說明 AWS Resource Groups (Resource Groups) 內的配額。若要調整配額，您可以在「Service Quotas」主控台中要求增加配額。

名稱	預設	可調整	描述
每個帳戶的資源群組數	每個受支援的區域：100	是	您可以在此帳號中建立的資源群組數目上限。資源群組是符合特定條件的 AWS 資源集合。

AWS Resource Groups 文件歷史

變更	描述	日期
已更新內容	更新了主題標題和重新整理的內容，以提高可讀性和可探索性。	2024年8月1日
Support 更多資源類型	Resource Groups 和標籤編輯器現在支援更多資源類型。	2024年5月30日
更新了 AWS 管理的政策和 ResourceGroupsandTagEditorFullAccess ResourceGroupsandTagEditorReadOnlyAccess	Resource Groups 更新了兩個 AWS 受管理的策略以新增其他 AWS CloudFormation 權限。	2023 年 8 月 10 日
Resource Groups 服務配額	您現在可以使用 Service Quotas 檢視 Resource Groups 配額限制。	2023 年 6 月 29 日
IAM最佳實踐更新	更新指南以符合最IAM佳做法。如需詳細資訊，請參閱 IAM.	2023 年 1 月 3 日
標籤編輯器資訊已移至自己的指南	標籤編輯器的文件已從本指南中移除，並移至新的「標籤編輯器使用者指南」。	2022 年 12 月 13 日
資源組現在可以包括 Amazon Keyspaces 的資源（阿帕奇卡桑德拉）	AWS Resource Groups 現在支持包括資源組 Amazon Keyspaces（阿帕奇卡桑德拉）資源。	2022 年 10 月 20 日
資源類型的棄用	標籤編輯器不再支援下列資源類型：AWS::RoboMaker::Robot AWS::Robo	2022 年 5 月 17 日

	`Maker::Fleet` 、和`AWS::RoboMaker::DeploymentJob` 。	
新的 AWS 受管理策略-ResourceGroupsServiceRolePolicy	Resource Groups 在 AWS Identity and Access Management (IAM) 中新增了新的 AWS 受管理策略，以支援服務的服務連結角色。	2022 年 1 月 12 日
組生命週期事件	Resource Groups 現在可以在 Amazon Events 中產生 CloudWatch 事件，以便在資源群組發生變更時提醒您。	2022 年 1 月 12 日
Amazon VPC 網路存取分析器現在可以使用資源群組來監控不必要的 AWS 資源網路流量。	您可以使用 AWS Resource Groups 來指定網路存取需求的來源和目的地。	2021 年 12 月 3 日
增加了對 AWS 恢復中心資源的支持	AWS Resource Groups 現在支援包括資源群組中 AWS 復原中樞的資源。	2021 年 11 月 18 日
增加了對 Amazon Pinpoint 的資源支持	AWS Resource Groups 現在支援在資源群組中包含 Amazon Pinpoint 位的資源。	2021 年 11 月 11 日
已新增設定及管理的資源群組支援 AppRegistry	AWS Resource Groups 現在支援包含您使用建立之應用程式中資源之服務組態的資源群組 AWS Service Catalog AppRegistry。如需詳細資訊，請參閱AWS Resource Groups API參考資料中的服務組態。	2021 年 9 月 15 日

增加了對 Amazon OpenSearch 服務的資源支持	AWS Resource Groups 現在支援在資源群組中包含 Amazon OpenSearch 服務的資源。	2021 年 8 月 11 日
增加了對 AWS 布拉克特資源的支持	AWS Resource Groups 現在支援在資源群組中包含 AWS Braket 的資源。	2021 年 6 月 30 日
增加了對 Amazon EMR 容器資源的支持	AWS Resource Groups 現在支援在資源群組中包含 Amazon EMR 容器的資源。	2021 年 4 月 27 日
增加了對其他 AWS 服務的資源支持	AWS Resource Groups 現在支援包括資源群組中下列服務的資源：Amazon CodeGuru 審閱者、Amazon Elastic Inference、Amazon Forecast、Amazon Fraud Detector 和 Service Quotas。	2021 年 2 月 25 日
新增有關安全性與合規性的章節。	討論 Resource Groups 如何保護您的資訊並遵守法規標準。	2020 年 7 月 30 日

已新增針對 AWS 服務設定之資源群組的支援	您現在可以建立與 AWS 服務相關聯的資源群組，並設定服務如何與群組中的資源互動。在此功能的第一版中，您可以建立包含 Amazon EC2 容量保留的資源群組，然後將 Amazon EC2 執行個體啟動到群組中。如果群組的一或多個保留區中有符合您執行個體的容量，則該執行個體會使用保留項目。如果執行個體與群組中的任何可用保留項不符，則會以隨需執行個體的形式啟動。如需詳細資訊，請參閱 Amazon EC2 使用者指南中的使用容量保留群組。	2020 年 7 月 29 日
增加了對 AWS IoT Greengrass 資源的支持。	AWS Resource Groups 和標籤編輯器現在支援更多資源類型。	2020 年 3 月 25 日

檢視的作業資料 AWS Resource Groups	在 AWS Systems Manager 主控台中， AWS Resource Groups 頁面會在四個索引標籤上顯示所選群組的作業資料：「詳細資料」、「組 Config」CloudTrail、「」OpsItems。在 Resource Groups 主控台中檢視群組時，無法使用這些標籤。您可以使用這些標籤上的資訊，協助您了解群組中的哪些資源合規且運作正確，以及哪些資源需要動作。如果您需要在資源上採取動作，您可以使用 Systems Manager Automation Runbook 來執行常見的操作維護和故障診斷任務。若要取得更多資訊，請參閱《AWS Systems Manager 使用指南》 AWS Resource Groups中的〈檢視作業資料〉。	2020 年 3 月 16 日
檢查是否符合標籤政策	使用建立標籤策略並將其附加至帳號之後 AWS Organizations，您可以在組織帳戶中的資源上找到不符合標籤。	2019 年 11 月 26 日
Support 更多資源類型	AWS Resource Groups 和標籤編輯器現在支援更多資源類型。	2019 年 10 月 4 日
支援的新資源類型 AWS Resource Groups	現在支援更多資源類型 AWS Resource Groups，尤其是以 AWS CloudFormation 堆疊為基礎的群組。	2019 年 8 月 5 日

支援的新資源類型 AWS Resource Groups	Amazon API 網關RESTAPIs、Amazon CloudWatch 活動事件和 Amazon SNS 主題現在支援中的資源類型 AWS Resource Groups。	2019 年 6 月 27 日
標籤編輯器現在支援尋找未標記的資源	您現在可以在「標籤編輯器」中搜尋未套用特定標籤鍵的標籤值的資源。	2019 年 6 月 18 日
AWS Resource Groups 和標籤編輯器支援的新資源類型	超過 50 種新的資源類型已新增至 AWS Resource Groups 和標籤編輯器支援。	2019 年 6 月 6 日
AWS Resource Groups 和標籤編輯器控制台移出 AWS Systems Manager 控制台	AWS Resource Groups 和標籤編輯器主控台現在獨立於 Systems Manager 主控台。雖然您仍然可以在 Systems Manager 左側導覽列中找到 AWS Resource Groups 主控台的指標，但是您可以直接從左上角的下拉式功能表開啟 Resource Groups 和標籤編輯器主控台 AWS Management Console。	2019 年 6 月 5 日
新增 Resource Groups 授權和存取控制功能	Resource Groups 現在支援以動作為基礎的策略、資源層級權限，以及以標籤為基礎的授權。	2019 年 5 月 24 日
舊版的舊版 Resource Groups 和標籤編輯器工具已無法使用	舊版、傳統或舊版 Resource Groups 和標籤編輯器的提及已移除；這些工具在中 AWS不再提供。請改用 AWS Resource Groups 和標籤編輯器。	2019 年 5 月 14 日

標籤編輯器現在支援跨多個區域標記資源	標籤編輯器現在可讓您跨多個區域搜尋和管理資源標籤，並且預設會將您目前的區域新增至資源查詢。	2019 年 5 月 2 日
標籤編輯器現在支援將查詢結果匯出至 CSV	您可以將 [尋找要標記的資源] 頁面上的查詢結果匯出至CSV格式化的檔案。標籤編輯器查詢結果中會顯示新的區域欄。標籤編輯器現在可讓您搜尋特定標籤索引鍵具有空白值的資源。標籤索引鍵值會在您輸入現有索引鍵中的唯一值時自動完成。	2019 年 4 月 2 日
標籤編輯器現在支援將所有資源類型新增至查詢	您最多可以在單一操作中對個別資源類型套用 20 個標籤，或者您可以選擇 All resource types (所有資源類型) 以查詢區域中的所有資源類型。自動完成已新增至查詢的 Tag key (標籤索引鍵) 欄位，以協助在資源間實現一致的標籤索引鍵。如果標籤變更在某些資源上失敗，您可以僅在標籤變更失敗的資源上變更重試標籤變更。	2019 年 3 月 19 日
標籤編輯器現在支援搜尋中的多種資源類型	您可以在單一操作中對最多 20 個資源類型套用標籤。您也可以選擇在搜尋結果中顯示的欄位，包含在您的搜尋結果中找到的每個唯一標籤索引鍵或從結果選取資源的欄位。	2019 年 2 月 26 日
文檔添加了新的標籤編輯器	「使用標籤編輯器」一節說明如何使用新的 AWS 標籤編輯器主控台體驗。	2019 年 2 月 13 日

Resource Groups 中群組支援的新資源類型	已新增 Resource Groups 現在支援的新資源類型。	2019 年 2 月 4 日
改善將標籤新增至以標籤為基礎的 Resource Groups 查詢的使用者	對主控台使用者體驗的次要變更，用於在以標籤為基礎的查詢中新增標籤。	2018 年 12 月 17 日
AWS CloudFormation 已新增至 Resource Groups 的堆疊式查詢支援	您可以建立查詢以 AWS CloudFormation 堆疊為基礎的資源群組。選擇堆疊之後，您可以從堆疊選擇要顯示在您的群組查詢的資源類型。	2018 年 11 月 13 日
Resource Groups 和 CloudTrail	Resource Groups 現在提供 AWS CloudTrail 支援。您可以檢視和使用中所有 Resource Groups API 呼叫的記錄 CloudTrail。	2018 年 6 月 29 日

- API版本:
- 文件最近更新時間：2019 年 9 月 24 日

舊版更新

下表描述 2018 年 6 月前，每個 AWS Resource Groups 使用者指南版本的重要變更。

變更	描述	日期
初始版本	下一代的初始版本 AWS Resource Groups	2017 年 11 月 29 日

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。