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，請參閱可搭配 AWS Resource Groups 運作的 AWS 服務。

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 Groups API，使用AWS CLI命令或 AWS SDK 程式設計語言。如需詳細資訊，請參閱 AWS Resource Groups API 參考。

在 AWS Management Console首頁上使用資源群組

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。

什麼是資源群組？

在 AWS 中，資源是指您可以使用的實體。範例包括 Amazon EC2 執行個體、AWS CloudFormation堆疊或 Amazon S3 儲存貯體。如果使用多個資源，則您可能發現將它們當作群組管理，而不是針對每個任務將它們從某個 AWS 服務移至另一個服務，這樣做很有用。如果您管理大量相關資源 (例如，組成應用程式層的 EC2 執行個體)，您可能需要一次在這些資源上執行大量動作。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**
  >
  > 請勿將個人識別資訊 (PII) 或其他機密或敏感資訊儲存在標籤中。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。

- 以 AWS CloudFormation 堆疊為基礎

  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。您可以將查詢僅以一個 AWS CloudFormation 堆疊為根據。

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 API 來建立和管理的資源群組。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 GroupsAPI 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

預設情況下，AWS Management Console 是透過 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。
- 一同用於為常見專案或您想要管理或監控做為群組的一組 AWS 資源。
- 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。每個版本都會在 Amazon EC2 上執行，並具有 Amazon 彈性區塊存放區儲存磁碟區。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 主體 (例如角色和使用者) 具有正確的 IAM 許可，他們就可以與您建立的資源群組搭配使用。

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。群組有與其關聯的唯一 Amazon Resource Name (ARN)。如需 ARN 的詳細資訊，請參閱 Amazon Web Services 一般參考 中的 Amazon Resource Name (ARN) 與 AWS 服務命名空間。

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

標籤是索引鍵和值組，可做為用於組織您的 AWS 資源的中繼資料。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**
>
> 請勿將個人識別資訊 (PII) 或其他機密或敏感資訊儲存在標籤中。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。

AWS Resource Groups 入門

在 AWS 中，資源是指您可以使用的實體。示例包括 Amazon EC2 實例、Amazon S3 存儲段或 Amazon Route 53 託管區域。如果使用多個資源，則您可能發現將它們當作群組管理，而不是針對每個任務將它們從某個 AWS 服務移至另一個服務，這樣做很有用。

本節向您示範如何開始使用 AWS Resource Groups。首先，在標籤編輯器中對 AWS 資源加上標籤來組織它們。然後，在 Resource Groups 中建置可將您要的資源類型併入羣組中的查詢，以及您已套用至資源的標籤。

在 Resource Groups 中創建資源組後，請使用AWS Systems Manager工具 (例如 Automation) 來簡化資源羣組上的管理任務。

如需有關入門的詳細資訊AWS Systems Manager功能和工具的詳細資訊，請參AWS Systems Manager使用者指南。

主題

- 使用的先決條件 AWS Resource Groups

使用的先決條件 AWS Resource Groups

開始使用資源群組之前，請確定您的作用中 AWS 帳戶具有現有資源和適當的權限，可對資源加上標籤和建立群組。

註冊成為 AWS

如果您沒有 AWS 帳戶，請完成以下步驟來建立一個。

若要註冊成為 AWS 帳戶

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

   部分註冊程序需接收來電，並在電話鍵盤輸入驗證碼。

   當您註冊時 AWS 帳戶，會建立AWS 帳戶根使用者一個。根使用者有權存取該帳戶中的所有 AWS 服務 和資源。作為最佳安全實務，將管理存取權指派給管理使用者，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 AWS Resource Groups 主控台和 API 所需的權限。

如果您是管理員，則可以透過 AWS Identity and Access Management (IAM) 服務建立政策，為使用者提供許可。首先，您可以建立主體 (例如 IAM 角色或使用者)，或使用類似 AWS IAM Identity Center的服務將外部身分與 AWS 環境建立關聯。然後，您可以使用您的使用者需要的權限來套用原則。如需建立和附加 IAM 政策的相關資訊，請參閱使用政策。

個別服務的權限

> **Important**
>
> 本節說明如果您想要將來自其他服務主控台和 API 的資源加上標籤，以及將這些資源新增到資源群組時所需的許可。

如什麼是資源群組？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 API 中標記動作的許可，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。如需此類 Amazon EC2 政策的範例，請參閱 Amazon EC2 執行個體使用者指南中的 Amazon EC2 主控台中使用的範例政策。

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 IAM 中的使用者政策陳述式。您可以新增由維護和保留的 AWS管理原 up-to-date 則 AWS，也可以建立和維護自己的自訂原則。

針對 Resource Groups 和標籤編輯器權限使用 AWS 受管策略

AWS Resource Groups 和標籤編輯器支援下列 AWS 受管理的策略，您可以使用這些策略向使用者提供預先定義的一組權限。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

此政策授予附加的 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

此政策授予附加的 IAM 角色或使用者權限，以呼叫任何 Resource Groups 作業，以及在標籤編輯器中進行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：

- AWS-managed 政策會ReadOnlyAccess授與每個服務資源之唯讀作業的權限。 AWS 在新 AWS 服務可用時，自動保持此政策的最新狀態。
- 許多服務提供服務特定的唯讀 AWS管理策略，您可以使用這些策略來限制只存取該服務所提供的資源。例如，Amazon EC2 提供亞馬遜 ReadOnlyAccess EC2。
- 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。目前不支援搭配`resource-groups:ListGroupResources`使用原則條件。

授與使用 AWS Resource Groups 和標籤編輯器的權限

若要將使用 AWS Resource Groups 和標籤編輯器的原則新增至使用者，請執行下列動作。

1. 開啟 IAM 主控台。
2. 在導覽窗格中，選擇使用者 。

3. 尋找您要授 AWS Resource Groups 與的使用者和「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 標籤上，貼上下列政策陳述式。

```
{
  "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 AWS Resource Groups 與和「標籤編輯器」動作的權限。它不允許存取 AWS Resource Groups 主控台中的 AWS Systems Manager 工作。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，請參閱使AWS Systems Manager 用者指南中的〈設定 Systems Manager 存取權限〉

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，政策已儲存在 IAM 中，您可以將其附加到其他使用者。如需有關如何新增政策至使用者的詳細資訊，請參閱《IAM 使用者指南》中的透過將政策直接附加到使用者來新增許可。

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 ARN 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。

Resource Groups 不使用任何服務連結角色。

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 使用者指南中的下列主題。

- AWS 與 IAM 搭配使用的服務
- 的動作、資源和條件索引鍵 AWS Resource Groups
- 使用原則控制存取

建立以查詢為基礎的群組AWS Resource Groups

主題

- 資源群組查詢的類型
- 建立以標籤為基礎的查詢並建立群組
- 建立AWS CloudFormation以堆疊為基礎的群組

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式AWS::*service*::*resource*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，其中包含用來執行應用程式測試階段的所有 Amazon EC2 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，然後指定標籤金鑰**Stage** (標籤值為)**Test**。

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。它包含具有下列元素的 JSON 結構的字串表示法：

  - ResourceTypeFilters

    此元素會將結果限制為僅符合篩選的那些 Resource Name。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。只有具有索引鍵名稱相符的標記的資源，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。群組的成員只有具有相符標籤鍵的相符標記鍵的值。

所有這些 JSON 元素都必須合併成 JSON 結構的單行字串表示法。例如，考慮一個`Query`與下面的示例 JSON 結構。此查詢旨在僅比對具有標籤「階段」且值為「測試」的 Amazon EC2 執行個體。

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

該 JSON 可以表示為以下單行字符串，並用作`Query`元素的值。由於 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 堆疊為基礎的查詢中，您可以選擇您的目前區域帳戶中的 AWS CloudFormation 堆疊，然後在堆疊中選擇您希望在群組中的資源類型。您可以將查詢僅以一個 AWS CloudFormation 堆疊為根據。

> **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。但是，由該 auto-scaling 群組建立的 Amazon EC2 執行個體作為其操作的一部分，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。它包含具有下列元素的 JSON 結構的字串表示法：

  - `ResourceTypeFilters`

    此元素會將結果限制為僅符合篩選的那些 Resource Name。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`

    此元素指定要將其 Resource Name (ARN) 的AWS CloudFormation堆疊的 Amazon Resource Name (ARN)。

所有這些 JSON 元素都必須合併成 JSON 結構的單行字串表示法。例如，考慮一個`Query`與下面的示例 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"
}
```

該 JSON 可以表示為以下單行字符串，並用作`Query`元素的值。由於 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. 在導覽窗格中，
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::Instance和AWS::S3::Bucket。
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. 仍在分組標準下，選擇預覽群組資源以傳回您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。Resource Name 在您帳戶中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，輸入以下值，然後按 Enter 鍵，將群組名稱、資源類型、標籤索引鍵和標籤值的值替換成您自己的值。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。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. 在導覽窗格中，
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 View group resources (檢視群組資源) 以傳回 AWS CloudFormation 堆疊中與您所選資源類型相符的資源清單。
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。Resource Name 在您帳戶中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 AWS CloudFormation 堆疊為基礎的群組是根據類型 CLOUDFORMATION_STACK_1_0 的查詢。

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。

   stack_identifier 是堆疊 ARN，如範例命令中所示。

   ```
   $ 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，請更新用於建立堆疊的 AWS CloudFormation 範本，然後在 AWS CloudFormation 中更新堆疊。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 AWS CLI 中，您以兩種命令更新群組。

- `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。不過，您可以使用 Resource Groups API 來這麼做，包括AWS CLI.

更新標籤籤籤籤籤籤籤籤

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**
>
> 只能更新自動動動動動動作。[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 使用者指南》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。在此逐步解說中，我們會將資源類型 AWS::RDS::DBInstance 新增至查詢。
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) 您可以在群組籤籤籤籤，可以新增或移除標籤。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，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，請務必在群組標籤中至少新增一個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 EC2 執行個體、S3 儲存貯體和 Amazon RDS 資料庫執行個體清單。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 AWS CLI 中，您可以使用兩個不同的命令，更新群組的查詢和更新資源群組的說明。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，輸入以下值，然後按 Enter 鍵，將群組名稱和描述值替換成您自己的值。

```
$ 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

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**
>
> 只能更新自動動動動動動作。[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 使用者指南》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，請務必在群組標籤中至少新增一個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 AWS CLI 中，您可以使用兩個不同的命令，更新群組的查詢和更新資源群組的說明。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. 若要更新群組別籤，請執行以下命令。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。

   stack_identifier 是堆疊 ARN，如範例命令中所示。

```
$ 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服務包括 Amazon Simple Notification Service (Amazon SNS)、Amazon Simple Queue Service (Amazon SQS) 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，請參閱亞馬遜 EventBridge 用戶指南中的亞馬遜 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，具有監控您的資源是否對其標籤和堆棧進行任何更改的AWS CloudFormation權限，以查看是否對屬於堆棧一部分的資源進行任何更改。
- 「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 Resource Groups 所使用服務連結結結結結結結結結結結結結結結結結結結結結結結結結結結結對 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。
- 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

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
- API — UpdateAccountSettings以及 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

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。

欄位名稱	Type	描述
source	字串	對於 Resource Groups，此值一律為"aws.resource-groups" 。
resources	Amazon 資源名稱（ARN）的數組	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之任何資源的 ARN。
detail	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。

該**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是由群組的 ARN 和包含 UU ID 的"unique-id"欄位組合來識別。透過將 UUID 納入資源群組識別的一部分，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物件	按照 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 物件	變更前的群組狀態。物件僅包含變更的性質值。
new-state	GroupState 物件	變更之後的群組狀態。物件僅包含變更的性質值。

groupJSON 物件包含下表所述的元素。

欄位名稱	Type	描述
arn	字串	群組的 ARN。
name	字串	群組的易記名稱。
unique-id	GUID	唯一的 GUID 值，可區分刪除的群組與稍後使用相同名稱和 ARN 建立的不同群組。在程式碼中使用這些事件時，請使用 ARN 和此值作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 物件	定義群組成員之查詢的 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 物件	與服務連結群組相關聯之組態參數的 JSON 表示法。如需詳細資訊，請參閱 AWS Resource GroupsAPI 參考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，該群組使用的標籤式查詢僅與具有標籤"project"="my-service"的 Amazon Elastic Compute Cloud (Amazon EC2) 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`欄位會包含已變更其成員資格之群組的 ARN，以及新增至群組或從群組中移除之任何資源的 ARN。

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。
`group`	`Group`物件	以 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`— 新增或移除資源的 ARN。 • `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，請以您自己的資訊取代每個*########*。

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 ARN 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

刪除資源群組

1. 登入 AWS Resource Groups 主控台。
2. 在導覽窗格中，選擇儲存儲存在的 Resource Groups。
3. 選擇要刪除的資源群組的名稱。
4. 在群組的詳細資料頁面上，按一下右上角的刪除。
5. 出現提示要您確認刪除時，選擇 Delete (刪除)。

AWS CLI & AWS SDKs

刪除資源群組

1. 執行下列命令，以您的群組名*#########*。

```
$ 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。

可搭配 AWS Resource Groups 運作的 AWS 服務

您可以在一起使用以下AWS服務AWS Resource Groups。

AWS 服務	與 Resource Groups
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。 如需詳細資訊，請參閱《AWS CloudFormation使用指南》中的ResourceGroups資源類型參考。

AWS 服務	與 Resource Groups
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 事件歷史記錄檢視事件。
Amazon CloudWatch — 可即時監控您的AWS資源和您在上執行的應用程式AWS。	將您的檢視專注於顯示單一資源群組中的指標和警示。 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。	監控您的 .NET 和 SQL Server 應用程式。 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 — 使用現有的每個通訊端、每個核心或每個 VM 軟體授權，包括 Windows Server、Microsoft SQL Server、SUSE 及 Linux Enterprise Server，以此類推。	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，請參閱適用於 Linux 執行個體 Amazon EC2 使用者指南中的專用主機。

AWS 服務	與 Resource Groups
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。如果稍後階段將相符的容量預留新增至目標群組，則執行個體會自動比對並移入預留容量。 如需詳細資訊，請參閱適用於 Linux 執行個體 Amazon EC2 使用者指南中的使用容量預留群組。
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 使用者指南》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干擾。	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使用者指南中的可共用資源。

AWS 服務	與 Resource Groups
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 Application Instance Manager 中的資訊，協助您判斷哪些資源合規且運作正確，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 — 識別對AWS的資源進行的不必要網路存取。	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 使用者指南中的網路存取範圍的 Resource Groups。

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組態，採用附加至群組的 JSON 資料結構形式。

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
- 服務組態的 JSON 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提供的工具 (例如該服務的管理主控台或其AWS CLI和 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 SDK 或其AWS CLI對等項目中的下列 API 作業與服務設定互動：

- 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。

服務組態的 JSON 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。

一個配置表示為一個 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和一個或多個陣列Values。下列含##位置的範例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。

```
{
    "Configuration": [
        {
            "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。需要此組態類型的服務連結群組會自動新增，例如AWS::EC2::CapacityReservationPool和AWS::EC2::HostManagment類型。

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使用 Amazon EC2 主機執行個體。

```
{
    "Configuration": [
        {
            "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。

```
{
    "Configuration": [
        {
            "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 AppRegistry指派之應用程式的 Amazon 資源名稱 (ARN) 路徑。

  值的資料類型：字串

  允許的值：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。

```
{
    "Configuration": [
        {
            "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 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：有效的 ARN。

  必要：是

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

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

```
{
    "Configuration": [
        {
            "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做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 Linux 執行個體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。

```
{
    "Configuration": [
        {
            "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，還是啟動至具有相符組態的任何可用主機。如需詳細資訊，請參閱 Amazon EC2 Linux 執行個體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

```
{
    "Configuration": [
        {
            "Type": "AWS::EC2::HostManagement",
            "Parameters": [
                {
                    "Name": "auto-allocate-host",
                    "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 執行個體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

```
{
    "Configuration": [
        {
            "Type": "AWS::EC2::HostManagement",
            "Parameters": [
                {
                    "Name": "auto-release-host",
                    "Values": [ "false" ]
                }
            ]
        },
        {
            "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。

```
{
    "Configuration": [
        {
            "Type": "AWS::EC2::HostManagement",
            "Parameters": [
                {
                    "Name": "allowed-host-families",
                    "Values": ["c5", "m5"]
                }
            ]
        },
        {
            "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：ARN 的陣列。

  允許的值：每個值都必須是有效的 License 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。

```
{
    "Configuration": [
        {
            "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。

```
{
    "Configuration": [
        {
            "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。

```
{
    "Configuration": [
        {
            "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之資源群組的 ARN，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。有關詳情，請參閱在AWS Network Firewall中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。

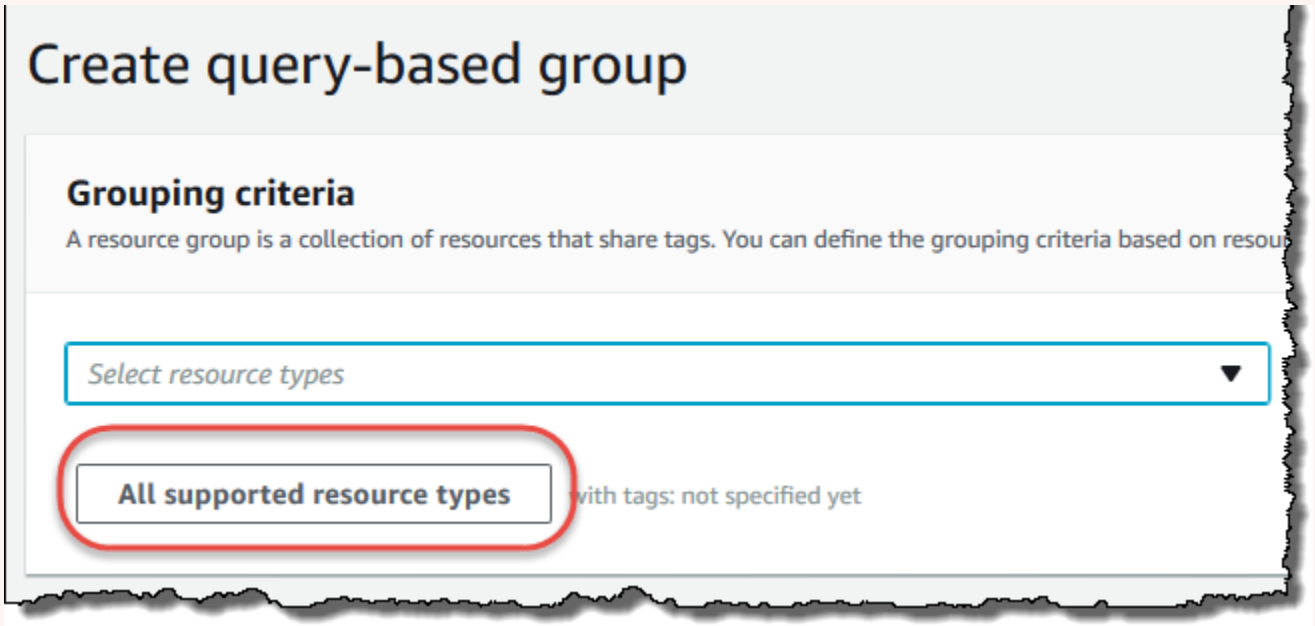
```
$ aws resource-groups create-group \
    --name test-group \
    --resource-query '{"Type": "TAG_FILTERS_1_0", "Query": "{\"ResourceTypeFilters\":
 [\"AWS::EC2::Instance\"], \"TagFilters\": [{\"Key\": \"environment\", \"Values\":
 [\"production\"]}]}"}' \
    --configuration '[{"Type": "AWS::NetworkFirewall::RuleGroup", "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"
    }
}
```

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才能成為群組的一部分。



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。

> **Note**
>
> 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。

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

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
AWS::AppSync::GraphQLApi	✗ 否	✗ 否	✓ 是

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

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::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	✗ 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 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
AWS::CloudWatch::Dashboard	X 否	X 否	✓ 是
AWS::CloudWatch::InsightRule	X 否	✓ 是	X 否
AWS::CloudWatch::MetricStream	X 否	✓ 是	X 否
AWS::CloudWatch::ServiceLevelObjective	X 否	✓ 是	X 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	X 否	✓ 是	X 否
AWS::Logs::LogGroup	X 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	✗ 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	X 否	✓ 是	✓ 是
AWS::CodeDeploy::DeploymentConfig	X 否	X 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::ConfigRule	✓ 是	✓ 是	X 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

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

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::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

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::UserGroup	✗ 否	✓ 是	✗ 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	✗ 否
AWS::ElasticBeanstalk::ApplicationVersion	✗ 否	✓ 是	✗ 否
AWS::ElasticBeanstalk::ConfigurationTemplate	✗ 否	✓ 是	✗ 否
AWS::ElasticBeanstalk::Environment	✗ 否	✓ 是	✗ 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

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::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
AWS::EC2::ImportImageTask	✗ 否	✓ 是	✗ 否
AWS::EC2::ImportSnapshotTask	✗ 否	✓ 是	✗ 否
AWS::EC2::Instance	✓ 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::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
AWS::EC2::NetworkAcl	✓ 是	✓ 是	✓ 是
AWS::EC2::NetworkInsightsAccessScope	✗ 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::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
AWS::EC2::TrafficMirrorSession	✗ 否	✓ 是	✗ 否
AWS::EC2::TrafficMirrorTarget	✗ 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::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
AWS::EC2::VPCEndpointService	✗ 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::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
AWS::ECS::ContainerInstance	✗ 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::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::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	X 否	✓ 是	✓ 是
AWS::ElasticLoadBalancingV2::ListenerRule	X 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

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
AWS::Forecast::ForecastExportJob	✓ 是	✓ 是	✗ 否
AWS::Forecast::Predictor	✓ 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::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
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	✗ 否	✓ 是	✗ 否
AWS::GameLift::GameSessionQueue	✗ 否	✓ 是	✗ 否
AWS::GameLift::MatchmakingConfiguration	✗ 否	✓ 是	✗ 否
AWS::GameLift::MatchmakingRuleSet	✗ 否	✓ 是	✗ 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	✗ 否	✓ 是	✗ 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

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::Job	✓ 是	✓ 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

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::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::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

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::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::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

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::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
AWS::Greengrass::ResourceDefinition	✓ 是	✓ 是	✗ 否
AWS::Greengrass::SubscriptionDefinition	✓ 是	✓ 是	✗ 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	✗ 否	✓ 是	✗ 否
AWS::IoTSiteWise::AssetModel	✗ 否	✓ 是	✗ 否
AWS::IoTSiteWise::Gateway	✗ 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	✗ 否	✗ 否	✓ 是
AWS::Lambda::EventSourceMapping	✗ 否	✗ 否	✓ 是
AWS::Lambda::Function	✓ 是	✓ 是	✓ 是
AWS::Lambda::LayerVersion	✗ 否	✗ 否	✓ 是
AWS::Lambda::Version	✗ 否	✗ 否	✓ 是

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
AWS::AmazonMQ::Configuration	✓ 是	✓ 是	✗ 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 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

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::FlowOutput	✗ 否	✓ 是	✗ 否
AWS::MediaConnect::FlowSource	✗ 否	✓ 是	✗ 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	✗ 否	✓ 是	✗ 否
AWS::MediaPackage::PackagingConfiguration	✗ 否	✓ 是	✗ 否
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

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::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
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

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::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
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

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::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
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	X 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	X 否	✓ 是	X 否
AWS::RoboMaker::Fleet	X 否	✓ 是	X 否
AWS::RoboMaker::Robot	X 否	✓ 是	X 否
AWS::RoboMaker::RobotApplication	✓ 是	✓ 是	X 否
AWS::RoboMaker::SimulationApplication	✓ 是	✓ 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::RoboMaker::SimulationJob	✓ 是	✓ 是	X 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	X 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::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	X 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::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	✗ 否	✓ 是	✗ 否
AWS::XRay::SamplingRule	✗ 否	✓ 是	✗ 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 已與 AWS CloudFormation 整合，這項服務可協助您建立 AWS 資源的模型和設定，以減少建立和管理資源和基礎設施的時間。您可以建立一個範本，描述所有所需的資AWS源 (例如資源群組)，就會為您AWS CloudFormation佈建和設定這些資源。

當您使用時AWS CloudFormation，您可以重複使您的範本，重複使您的範本，重複使您的範本，重複使您範本 只需描述一次您的資源群組，即可在多AWS 帳戶個帳戶與區域內重複佈建相同資源群組。

Resource Groups 和AWS CloudFormation範本

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

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 JSON 和 YAML 範例範例)，請參閱AWS CloudFormation使用者指南中的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 命令列介面使用者指南》

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

- AWS Resource Groups 中的資料保護
- 適用於 AWS Resource Groups 的 Identity and Access Management
- 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
- 資源群組的基礎結構安全
- Resource Groups

AWS Resource Groups 中的資料保護

AWS 共同的責任模型適用於 AWS Resource Groups 中的資料保護。如此模型所述，AWS 負責保護執行所有 AWS 雲端 的全球基礎設施。您必須負責維護在此基礎設施上託管之內容的控制權。您也必須負責您所使用的 AWS 服務 安全性設定和管理工作。如需有關資料隱私權的詳細資訊，請參閱資料隱私權常見問答集。如需有關歐洲資料保護的相關資訊，請參閱 AWS 安全性部落格上的 AWS 共同的責任模型和 GDPR 部落格文章。

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

- 每個帳戶均要使用多重要素驗證 (MFA)。
- 使用 SSL/TLS 與 AWS 資源通訊。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 使用 AWS CloudTrail 設定 API 和使用者活動記錄。
- 使用 AWS 加密解決方案，以及 AWS 服務 內的所有預設安全控制項。
- 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。
- 如果您在透過命令列介面或 API 存取 AWS 時，需要 FIPS 140-2 驗證的加密模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的詳細資訊，請參閱聯邦資訊處理標準 (FIPS) 140-2 概觀。

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

資料加密

與其他AWS服務相比，AWS Resource Groups具有最小的攻擊面，因為它不提供更改，添加或刪除除組之外的AWS資源的方法。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 VPC 中使用 Resource Groups API 和主控台來協助最大化隱私權和基礎架構安全性。

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且不支援AWS KMS keys。

網際網路流量隱私權

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

適用於 AWS Resource Groups 的 Identity and Access Management

AWS Identity and Access Management (IAM) 是一種 AWS 服務，讓管理員能夠安全地控制對 AWS 資源的存取權限。IAM 管理員控制哪些人可以驗證 (登入) 和授權 (具有權限) 以使用 Resource Groups 資源。IAM 是一種您可以免費使用的 AWS 服務。

主題

- 對象
- 使用身分來驗證
- 使用政策管理存取權
- Resource Groups 如何搭配 IAM 運作
- 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
- 對 AWS Resource Groups 身分與存取進行疑難排解

對象

根據您在 Resource Groups 中執行的工作，使用方式 AWS Identity and Access Management (IAM) 會有所不同。

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，請參閱對 AWS Resource Groups 身分與存取進行疑難排解。

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。您接著必須將請求提

交給您的 IAM 管理員，來變更您服務使用者的許可。檢閱此頁面上的資訊，了解 IAM 的基本概念。若要進一步了解貴公司如何將 IAM 與 Resource Groups 搭配使用，請參閱Resource Groups 如何搭配 IAM 運作。

IAM 管理員 — 如果您是 IAM 管理員，您可能想要瞭解如何撰寫政策來管理 Resource Groups 存取權限的詳細資訊。若要檢視可在 IAM 中使用的 Resource Groups 基於身分的政策範例，請參閱。AWS Resource Groups 身分型政策範例

使用身分來驗證

身分驗證是使用身分登入資料登入 AWS 的方式。您必須以 AWS 帳戶根使用者、IAM 使用者身分，或擔任 IAM 角色進行 驗證 (登入至 AWS)。

您可以使用透過身分來源提供的憑證，以聯合身分登入 AWS。AWS IAM Identity Center(IAM Identity Center) 使用者、貴公司的單一登入身分驗證和您的 Google 或 Facebook 憑證都是聯合身分的範例。當您以聯合身分登入時，您的管理員先前已設定使用 IAM 角色的聯合身分。當您 AWS 藉由使用聯合進行存取時，您會間接擔任角色。

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

如果您是以程式設計的方式存取 AWS，AWS 提供了軟體開發套件 (SDK) 和命令行介面 (CLI)，以便使用您的憑證透過密碼編譯方式簽署您的請求。如果您不使用 AWS 工具，您必須自行簽署請求。如需使用建議的方法自行簽署請求的詳細資訊，請參閱《IAM 使用者指南》中的簽署 AWS API 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) 來提高帳戶的安全。如需詳細資訊，請參閱《AWS IAM Identity Center 使用者指南》中的多重要素驗證和《IAM 使用者指南》中的在 AWS 中使用多重要素驗證 (MFA)。

AWS 帳戶 根使用者

如果是建立 AWS 帳戶，您會先有一個登入身分，可以完整存取帳戶中所有 AWS 服務 與資源。此身分稱為 AWS 帳戶 根使用者，使用建立帳戶時所使用的電子郵件地址和密碼即可登入並存取。強烈建議您不要以根使用者處理日常作業。保護您的根使用者憑證，並將其用來執行只能由根使用者執行的任務。如需這些任務的完整清單，了解需以根使用者登入的任務，請參閱《IAM 使用者指南》中的需要根使用者憑證的任務。

IAM 使用者和群組

IAM 使用者是您 AWS 帳戶 中的一種身分，具備單一人員或應用程式的特定許可。建議您盡可能依賴暫時性憑證，而不是擁有建立長期憑證 (例如密碼和存取金鑰) 的 IAM 使用者。但是如果特定使用案例

需要擁有長期憑證的 IAM 使用者，建議您輪換存取金鑰。如需詳細資訊，請參閱 IAM 使用者指南中的為需要長期憑證的使用案例定期輪換存取金鑰。

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

使用者與角色不同。使用者只會與單一人員或應用程式建立關聯，但角色的目的是在由任何需要它的人員取得。使用者擁有永久的長期憑證，但角色僅提供臨時憑證。若要進一步了解，請參閱《IAM 使用者指南》中的建立 IAM 使用者 (而非角色) 的時機。

IAM 角色

IAM 角色是您 AWS 帳戶 中的一種身分，具備特定許可。它類似 IAM 使用者，但不與特定的人員相關聯。您可以在 AWS Management Console 中透過切換角色來暫時取得 IAM 角色。您可以透過呼叫 AWS CLI 或 AWS API 操作，或是使用自訂 URL 來取得角色。如需使用角色的方法詳細資訊，請參閱《IAM 使用者指南》中的使用 IAM 角色。

使用臨時性憑證的 IAM 角色在下列情況中非常有用：

- 聯合身分使用者存取 – 若要向聯合身分指派許可，請建立角色，並為角色定義許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並獲授予由角色定義的許可。如需有關聯合角色的詳細資訊，請參閱 IAM 使用者指南中的為第三方身分供應商建立角色。如果您使用 IAM Identity Center，則需要設定許可集。為控制身分驗證後可以存取的內容，IAM Identity Center 將許可集與 IAM 中的角色相關聯。如需有關許可集的資訊，請參閱 AWS IAM Identity Center 使用者指南中的許可集。
- 暫時 IAM 使用者許可：使用者可以擔任 IAM 角色或角色來暫時針對特定任務採用不同的許可。
- 跨帳戶存取：您可以使用 IAM 角色，允許不同帳戶中的某人 (信任的委託人) 存取您帳戶的資源。角色是授予跨帳户存取權的主要方式。但是，針對某些 AWS 服務，您可以將政策直接連接到資源 (而非使用角色作為代理)。若要了解跨帳戶存取角色和資源型政策間的差異，請參閱《IAM 使用者指南》中的 IAM 角色與資源類型政策的差異。
- 跨服務存取：有些 AWS 服務 會使用其他 AWS 服務 中的功能。例如，當您在服務中進行呼叫時，該服務通常會在 Amazon EC2 中執行應用程式或將物件存放在 Amazon Simple Storage Service (Amazon S3) 中。服務可能會使用呼叫委託人的許可、使用服務角色或使用服務連結角色來執行此作業。
  - 轉發存取工作階段 (FAS)：當您使用 IAM 使用者或角色在 AWS 中執行動作時，系統會將您視為主體。當您使用某些服務時，您可能會執行一個動作，而該動作之後會在不同的服務中啟動另一個動作。FAS 使用主體的許可呼叫 AWS 服務，搭配請求 AWS 服務 以向下游服務

發出請求。只有在服務收到需要與其他 AWS 服務或資源互動才能完成的請求之後，才會提出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出 FAS 請求時的政策詳細資訊，請參閱《轉發存取工作階段》https://docs.aws.amazon.com/IAM/latest/UserGuide/access_forward_access_sessions.html。

- 服務角色 – 服務角色是服務擔任的 IAM 角色，可代表您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需詳細資訊，請參閱《IAM 使用者指南》中的建立角色以委派許可給 AWS 服務 服務。
- 服務連結角色：服務連結角色是一種連結到 AWS 服務 的服務角色類型。服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的 AWS 帳戶 中，並由該服務所擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

- 在 Amazon EC2 上執行的應用程式：針對在 EC2 執行個體上執行並提出 AWS CLI 和 AWS API 請求的應用程式，您可以使用 IAM 角色來管理臨時性憑證。這是在 EC2 執行個體內存放存取金鑰的較好方式。若要指派 AWS 角色給 EC2 執行個體並提供其所有應用程式使用，您可以建立連接到執行個體的執行個體設定檔。執行個體設定檔包含該角色，並且可讓 EC2 執行個體上執行的程式取得臨時性憑證。如需詳細資訊，請參閱《IAM 使用者指南》中的利用 IAM 角色來授予許可給 Amazon EC2 執行個體上執行的應用程式。

若要了解是否要使用 IAM 角色或 IAM 使用者，請參閱《IAM 使用者指南》中的建立 IAM 角色 (而非使用者) 的時機。

使用政策管理存取權

您可以透過建立政策並將其連接到 AWS 身分或資源，在 AWS 中控制存取。政策是 AWS 中的一個物件，當其和身分或資源建立關聯時，便可定義其許可。AWS 會在主體 (使用者、根使用者或角色工作階段) 發出請求時評估這些政策。政策中的許可，決定是否允許或拒絕請求。大部分政策以 JSON 文件形式存放在 AWS 中。如需 JSON 政策文件結構和內容的詳細資訊，請參閱《IAM 使用者指南》中的 JSON 政策概觀。

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

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

IAM 政策定義該動作的許可，無論您使用何種方法來執行操作。例如，假設您有一個允許 `iam:GetRole` 動作的政策。具備該政策的使用者便可以從 AWS Management Console、AWS CLI 或 AWS API 取得角色資訊。

身分型政策

身分型政策是可以附加到身分 (例如 IAM 使用者、使用者群組或角色) 的 JSON 許可政策文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。若要了解如何建立身分類型政策，請參閱《IAM 使用者指南》中的建立 IAM 政策。

身分型政策可進一步分類成內嵌政策或受管政策。內嵌政策會直接內嵌到單一使用者、群組或角色。受管政策則是獨立的政策，您可以將這些政策連接到 AWS 帳戶 中的多個使用者、群組和角色。受管政策包含 AWS 受管政策和由客戶管理之政策。若要了解如何在受管政策及內嵌政策間選擇，請參閱《IAM 使用者指南》中的在受管政策和內嵌政策間選擇。

資源型政策

資源型政策是連接到資源的 JSON 政策文件。資源型政策的最常見範例是 Amazon Simple Storage Service (Amazon S3) 儲存貯體政策和 IAM 角色信任政策。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，政策會定義指定的委託人可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中指定委託人。委託人可以包括帳戶、使用者、角色、聯合身分使用者或 AWS 服務。

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

存取控制清單 (ACL)

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

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

其他政策類型

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

- 許可界限：許可界限是一種進階功能，可供您設定身分型政策能授予 IAM 實體 (IAM 使用者或角色) 的最大許可。您可以為實體設定許可界限。所產生的許可會是實體的身分型政策和其許可界限的交集。會在 `Principal` 欄位中指定使用者或角色的資源型政策則不會受到許可界限限制。所有這類政策中的明確拒絕都會覆寫該允許。如需許可邊界的詳細資訊，請參閱《IAM 使用者指南》中的 IAM 實體許可邊界。

- 服務控制政策 (SCP)：SCP 是 JSON 政策，可指定 AWS Organizations 中組織或組織單位 (OU) 的最大許可。AWS Organizations 服務可用來分組和集中管理您企業所擁有的多個 AWS 帳戶。若您啟用組織中的所有功能，您可以將服務控制政策 (SCP) 套用到任何或所有帳戶。SCP 會限制成員帳戶中實體的許可，包括每個 AWS 帳戶根使用者。如需 Organizations 和 SCP 的詳細資訊，請參閱《AWS Organizations 使用者指南》中的 SCP 運作方式。
- 工作階段政策：工作階段政策是一種進階政策，您可以在透過編寫程式的方式建立角色或聯合身分使用者的暫時工作階段時，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 使用者指南》中的工作階段政策。

多種政策類型

將多種政策類型套用到請求時，其結果形成的許可會更為複雜、更加難以理解。若要了解 AWS 在涉及多種政策類型時如何判斷是否允許一項請求，請參閱《IAM 使用者指南》中的政策評估邏輯。

Resource Groups 如何搭配 IAM 運作

在您使用 IAM 管理 Resource Groups 的存取權之前，您應該先了解可與 Resource Groups 搭配使用的 IAM 功能有哪些。若要取得 Resource Groups 和其他AWS服務如何使用 IAM 的詳細資訊，請參閱《IAM 使用者指南》中的使用 IAM 的AWS服務。

主題

- Resource Groups 以身分為基礎的政策
- 資源型政策
- 根據資 Resource Groups 的授權
- Resource Groups IAM 角色

Resource Groups 以身分為基礎的政策

使用 IAM 身分型政策，您可以指定允許或拒絕的動作和資源，以及在何種條件下允許或拒絕動作。Resource Groups 支援特定動作、資源和條件金鑰。若要了解您在 JSON 政策中使用的所有元素，請參閱《IAM 使用者指南》中的 JSON 政策元素參考。

動作

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

JSON 政策的 Action 元素描述您可以用來允許或拒絕政策中存取的動作。政策動作的名稱通常會和相關聯的 AWS API 操作相同。有一些例外狀況，例如沒有相符的 API 作業的僅限許可動作。也有一些作業需要政策中的多個動作。這些額外的動作稱為相依動作。

政策會使用動作來授予執行相關聯操作的許可。

Resource Groups 中的政策動作會在動作之前使用下列前綴：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，若要授予某人使用 Resource GroupsCreateGroup API 操作建立 Resource Groups 的許可，請在其政策中加入resource-groups:CreateGroup動作。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任務。

若要在單一陳述式中指定多個 Resource Groups 和標籤編輯器動作，請用逗號分隔，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《IAM 使用者指南》AWS Resource Groups中的動作、資源和條件金鑰。

資源

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

Resource JSON 政策元素可指定要套用動作的物件。陳述式必須包含 Resource 或 NotResource 元素。最佳實務是使用其 Amazon Resource Name (ARN) 來指定資源。您可以針對支援特定資源類型的動作 (稱為資源層級許可) 來這麼做。

對於不支援資源層級許可的動作 (例如列出作業)，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。群組資源有以下格式的 ARN：

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

如需 ARN 格式的詳細資訊，請參閱 Amazon Resource Name (ARN) 和 AWS 服務命名空間。

例如，若要在您的陳述式中指定my-test-group資源群組，請使用以下 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/*"
```

有些資源動作無法對特定資源執行，例如用來建立資源的動作，例如用來建立資源的動作。在這些情況下，您必須使用萬用字元 (*)。

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

有些 Resource Groups 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項資源，請使用逗號分隔 ARN。

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

若要查看 Resource Groups 型及其 ARN 的清單，並了解您可以透過哪些動作來指定每項資源的 ARN，請參閱《IAM 使用者指南》AWS Resource Groups中的動作、資源和條件金鑰。

條件金鑰

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個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 元素中指定多個金鑰，AWS 會使用邏輯 AND 操作評估他們。若您為單一條件索引鍵指定多個值，AWS 會使用邏輯 OR 操作評估條件。必須符合所有條件，才會授予陳述式的許可。

您也可以在指定條件時使用預留位置變數。例如，您可以只在使用者使用其 IAM 使用者名稱標記時，將存取資源的許可授予該 IAM 使用者。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM 政策元素：變數和標籤。

AWS 支援全域條件索引鍵和服務特定的條件索引鍵。若要查看 AWS 全域條件金鑰，請參閱《IAM 使用者指南》中的 AWS 全域條件內容金鑰。

Resource Groups 會定義自己的一組條件金鑰，也支援一些全域條件金鑰的使用。若要查看 AWS 全域條件索引鍵，請參閱《IAM 使用者指南》中的 AWS 全域條件內容金鑰。

若要查看 Resource Groups 條件金鑰清單，並了解您可以透過哪些動作和資源來使用條件金鑰，請參閱《IAM 使用者指南》AWS Resource Groups中的動作、資源和條件金鑰。

範例

若要檢視 Resource Groups 以身分為基礎的政策範例，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。

根據資 Resource Groups 的授權

您可以將標籤連接至 Resource Groups 中的群組，或是在請求中將標籤傳遞至 Resource Groups。若要根據標籤控制存取，請使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 條件索引鍵，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。

若要檢視身分型原則範例，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 帳戶中具備特定許可的實體。Resource Groups 沒有或不使用服務角色。

將暫時性憑證與 Resource Groups 搭配

在 Resource Groups 中，您可以使用暫時登入資料登入聯合、擔任 IAM 角色，或是擔任跨帳戶角色。您取得暫時安全憑證的方式是透過呼叫AWS STS API 操作，例如AssumeRole或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

變更	描述	日期
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
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 AWS Resource Groups 和標籤編輯器的權限中的。

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。

對 AWS Resource Groups 身分與存取進行疑難排解

請使用以下資訊來協助您診斷和修復使用 Resource Groups 和 IAM 時可能遇到的常見問題。

主題

- 我未獲授權，不得在 Resource Groups 中執行動作
- 我未獲授權，不得執行 iam:PassRole
- 我想允許AWS帳戶外的人員存取我的 Resource Groups

我未獲授權，不得在 Resource Groups 中執行動作

若 AWS Management Console 告知您並未獲得執行動作的授權，您必須聯絡您的管理員以取得協助。您的管理員是提供您的登入憑證。

以下範例錯誤會在使用者`mateojackson`嘗試使用主控台檢視群組的詳細資訊，但卻沒有`resource-groups:ListGroups`許可時發生。

```
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。

我未獲授權，不得執行 iam:PassRole

如果您收到錯誤，告知您未獲授權執行`iam:PassRole`動作，您的政策必須更新，允許您將角色傳遞給 Resource Groups。

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

以下範例錯誤會在名為的 IAM 使用者`marymajor`嘗試使用主控台在 Resource Groups 中執行動作時，發生。但是，動作要求服務具備服務角色授予的許可。Mary 沒有將角色傳遞至該服務的許可。

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

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

如需任何協助，請聯絡您的 AWS 管理員。您的管理員提供您的登入憑證。

我想允許AWS帳戶外的人員存取我的 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對象取得該角色。針對支援基於資源的政策或存取控制清單 (ACL) 的服務，您可以使用那些政策來授予人員存取您資源的許可。

若要進一步了解，請參閱以下內容：

- 若要了解 Resource Groups 是否支援這些功能，請參閱Resource Groups 如何搭配 IAM 運作。

- 若要了解如何存取您擁有的所有 AWS 帳戶 所提供的資源，請參閱《IAM 使用者指南》中的將存取權提供給您所擁有的另一個 AWS 帳戶 中的 IAM 使用者。
- 若要了解如何將資源的存取權提供給第三方 AWS 帳戶，請參閱《IAM 使用者指南》中的將存取權提供給第三方擁有的 AWS 帳戶。
- 若要了解如何透過聯合身分提供存取權，請參閱《IAM 使用者指南》中的將存取權提供給在外部進行身分驗證的使用者 (聯合身分)。
- 若要了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱《IAM 使用者指南》中的 IAM 角色與資源型政策的差異。

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

要瞭解 AWS 服務 是否在特定法規遵循方案範圍內，請參閱法規遵循方案範圍內的 AWS 服務，並選擇您感興趣的法規遵循方案。如需一般資訊，請參閱 AWS 法規遵循方案。

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

您使用 AWS 服務 時的法規遵循責任取決於資料的敏感度、您的公司的合規目標，以及適用的法律和法規。AWS 提供以下資源協助您處理法規遵循事宜：

- 安全與合規快速入門指南 – 這些部署指南討論在 AWS 上部署以安全及合規為重心的基準環境的架構考量和步驟。
- Amazon Web Services 的 HIPAA 安全與法規遵循架構：本白皮書說明公司可如何運用 AWS 來建立符合 HIPAA 規定的應用程式。

> **Note**
>
> 並非全部的 AWS 服務 都符合 HIPAA 資格。如需詳細資訊，請參閱 HIPAA 資格服務參照。

- AWS 法規遵循資源：這組手冊和指南可能適用於您的產業和位置。
- AWS 客戶合規指南：透過合規角度瞭解共同的責任模式。這份指南總結了多個架構 (包括美國國家標準技術研究所 (NIST)、支付卡產業安全標準委員會 (PCI) 和國際標準化組織 (ISO)) 中，保護 AWS 服務並符合安全控制指引的最佳實務。
- AWS Config 開發人員指南中的使用規則評估資源：AWS Config 服務可評估資源組態對於內部實務、業界準則和法規的合規狀態。
- AWS Security Hub – 此 AWS 服務 可供您全面檢視 AWS 中的安全狀態。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。
- AWS Audit Manager – 此 AWS 服務 可協助您持續稽核 AWS 使用情況，以簡化管理風險與法規與業界標準的法規遵循方式。

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。

資源群組的基礎結構安全

沒有其他方法可隔離資源群組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 VPC 中使用資源群組 API 和主控台來協助最大化隱私權和基礎架構安全性。

作為託管服務，AWS Resource Groups受到AWS全球網絡安全的保護。如需有關 AWS 安全服務以及 AWS 如何保護基礎設施的詳細資訊，請參閱 AWS 雲端安全。若要使用基礎設施安全性的最佳實務來設計您的 AWS 環境，請參閱安全性支柱 AWS 架構良好的框架中的基礎設施保護。

您可以使用AWS已發佈的 API 呼叫透過網路存取資源群組。用戶端必須支援下列項目：

- Transport Layer Security (TLS)。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 具備完美轉送私密 (PFS) 的密碼套件，例如 DHE (Ephemeral Diffie-Hellman) 或 ECDHE (Elliptic Curve Ephemeral Diffie-Hellman)。現代系統 (如 Java 7 和更新版本) 大多會支援這些模式。

此外，請求必須使用存取索引鍵 ID 和與 IAM 主體相關聯的私密存取索引鍵來簽署。或者，您可以使用 AWS Security Token Service (AWS STS) 來產生暫時安全憑證來簽署請求。

資源群組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) 內的限制。您可以對一部分限制請求提高限制。若要要求提高限制，請前往 Service Quotas 主控台。如需可變更之限制的相關資訊，請參閱 Service Quotas。

> **Note**
>
> 下列定義適用於下列配額中的說明：
>
> - 資源群組 — 全部位於相同的AWS資源集合AWS 區域，且符合群組查詢中指定的條件。

資源	預設值限制
每AWS 帳戶個資源群組的最大數目 AWS 區域	100

AWS Resource Groups 參考

使用本節中的主題來尋找的各個層面的參考資訊AWS Resource Groups。

Resource Groups 的服務配額

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。

> **Note**
>
> 您可以使用 Service Quotas 主控台中的AWS Resource Groups頁面來要求變更標示為可調整的配額。

可搭配 AWS Resource Groups 使用的 AWS 受管政策

AWS-受管 IAM 許可政策可讓您將預先設定的許可授予帳戶中的 IAM 主體，例如角色和使用者。 AWS 受管理的原則會經過測試，並遵守最佳實務建議，因此您可以在定義的案例中可靠地使用它們。當資源群組的成員支援新資源類型時，當新資源類型支援標記時，會AWS自動更新這些策略以支援這些策略。你不需要做任何事情。

下表列出可供您用來授與許可的 AWS-managed IAM 權限政策。AWS Resource Groups

策略名稱和 ARN	描述
AWSResourceGroupsReadOnlyAccess	授與AWS Resource Groups管理主控台的唯讀存取權。它包括檢視資源詳細資訊的權限，包括附加標籤清單。此原則不會授與對資源群組或標籤進行任何變更的權限。

策略名稱和 ARN	描述
arn:aws:iam::aws:policy/AWSResourceGroupsReadOnlyAccess	
ResourceGroupsandTagEditorReadOnlyAccess arn:aws:iam::aws:policy/ResourceGroupsandTagEditorReadOnlyAccess	授與AWS Resource Groups管理主控台的唯讀存取權，包括標籤編輯器。它包括檢視資源詳細資料 (包括其標籤) 的權限。您可以使用標籤編輯器檢視與標籤查詢相符的資源。此原則不會授與對資源群組或標籤進行任何變更的權限。
ResourceGroupsandTagEditorFullAccess arn:aws:iam::aws:policy/ResourceGroupsandTagEditorFullAccess	授與管AWS Resource Groups理主控台的完整管理存取權。它包括檢視、建立和修改資源群組的權限。它還包括檢視、設定和修改標籤編輯器支援之任何資源之標籤的權限。

AWS Resource Groups 文件歷程記錄

變更	描述	日期
已更新AWS管理的政策ResourceGroupsandTagEditorFullAccess和ResourceGroupsandTagEditorReadOnly存取	資源群組更新了兩個AWS受管理的政策以新增其他AWS CloudFormation權限。	2023年8月10日
資源群組服務配額	您現在可以使用服務配額檢視資源群組配額限制。	2023 年 6 月 29 日
IAM 最佳做法更新	更新了指南以符合 IAM 最佳實務。如需詳細資訊，請參閱 IAM 中的安全最佳實務。	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亞馬遜密鑰空間的資源（阿帕奇卡桑德拉）	AWS Resource Groups現在支持包括資源組亞馬遜密鑰空間（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::RoboMaker::Fleet` ，以及`AWS::RoboMaker::DeploymentJob` 。	2022年5月17日
新AWS受管理策略-ResourceGroupsServiceRolePolicy	資源群組新增AWS受管理的政策AWS Identity and Access Management(IAM) 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	資源群組現在可以在 Amazon 中產生事件CloudWatch在資源群組發生變更時提醒您的事件。	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網路流量AWS資源。	您可以使用AWS Resource Groups，以指定您網路存取需求的來源和目的地。	2021 年 12 月 3 日
增加了對資源的支持AWS韌性樞紐	AWS Resource Groups現在支持包括資源AWS資源群組中的恢復中樞。	2021 年 11 月 18 日
增加了對亞馬遜精確定位資源的支持	AWS Resource Groups現在支援在資源群組中包含 Amazon 精確定位的資源。	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之資源之資源之服務組態的資源群組AWS Service Catalog AppRegistry。如需詳細資訊，請參閱服務組態在AWS Resource GroupsAPI 參考資料。	2021 年 9 月 15 日
增加了對亞馬遜的資源支持OpenSearch服務	AWS Resource Groups現在支持包括亞馬遜的資源OpenSearch資源群組中的服務。	2021 年 8 月 11 日
增加了對資源的支持AWS布拉基特	AWS Resource Groups現在支持包括資源AWS在資源群組中佈局。	2021 年 6 月 30 日
增加了對亞馬遜 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

增加了對額外的資源支持AWS服務	AWS Resource Groups現在支援在資源群組中包含下列服務的資源：AmazonCodeGuru審閱者、Amazon 彈性推論、亞馬遜預測、Amazon 詐騙偵測器和服務配額。	2021 年 2 月 25 日
新增有關安全性與合規性的章節。	討論資源群組如何保護您的資訊並遵守法規標準。	2020 年 7 月 30 日
已新增對設定的資源群組的支援AWS服務	您現在可以建立與AWS服務，並配置服務如何與組中的資源進行交互。在此第一版功能中，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，請參閱使用容量保留群組在亞馬遜 EC2 Linux 執行個體使用者指南。	2020 年 7 月 29 日
增加了支持AWS IoT Greengrass資源。	現在支援更多資源類型AWS Resource Groups和標籤編輯器。	2020 年 3 月 25 日

檢視 AWS Resource Groups 的操作資料	在AWS Systems Manager控制台，AWS Resource Groups頁面會在四個頁籤上顯示所選群組的作業資料：詳情,配置,CloudTrail,OpsItems。在資源群組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。如需詳細資訊，請參閱檢視的作業資料 AWS Resource Groups在AWS Systems Manager使用者指南。	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
支援更多資源類型	現在支援更多資源類型AWS Resource Groups和標籤編輯器。	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，特別是對於基於AWS CloudFormation堆疊。	2019 年 8 月 5 日

支援的新資源類型AWS Resource Groups	亞馬遜 API 網關休息 API，亞馬遜CloudWatch活動事件和 Amazon SNS 主題現在支援的資源類型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
支援的新資源類型AWS Resource Groups和標籤編輯器	超過 50 種新的資源類型已添加到AWS Resource Groups和標籤編輯器支持。	2019 年 6 月 6 日
AWS Resource Groups和標籤編輯器控制台移出AWS Systems Manager安慰	該AWS Resource Groups和標籤編輯器主控台現在獨立於系統管理員主控台。雖然你仍然可以找到指向AWS Resource Groups主控台位於 Systems Manager 左側導覽列中，您可以直接從左上角的下拉式功能表開啟資源群組和標籤編輯器主控台AWS Management Console。	2019 年 6 月 5 日
新增資源群組授權和存取控制功能	資源群組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
舊版的舊版資源群組和標籤編輯器工具不再可用	舊版、傳統或舊版資源群組和標籤編輯器的提及已移除；這些工具不再可用於AWS。使用AWS Resource Groups和標籤編輯器代替。	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為 CSV	您可以在 Find Resources to tag (尋找要加標籤的資源) 頁面上，將查詢的結果匯出為 CSV 格式的檔案。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」小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
資源群組中群組支援的新資源類型	已新增資源群組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資源群組查詢的使用者	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已新增至資源群組的堆疊式查詢支援	您可以建立資源群組，其中的查詢是根據 AWS CloudFormation 堆疊。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
資源群組和CloudTrail	資源群組現在提供AWS CloudTrail支持。您可以在以下位置檢視和使用所有資源群組 API 呼叫的記錄CloudTrail。	2018 年 6 月 29 日

- API 版本：2017-11-27
- 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 AWS Resource Groups 的初始版本	2017 年 11 月 29 日

AWS 詞彙表

如需最新的 AWS 術語，請參閱《AWS 詞彙表 參考》中的 AWS 詞彙表。

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。