使用者指南

AWS 資源總管

AWS 資源總管: 使用者指南

Table of Contents

什麼是 AWS 資源總管？

AWS 資源總管 是一項資訊搜尋和探索服務。使用資源總管，您可以使用類似網際網路搜尋引擎的體驗來探索資源，例如 Amazon 彈性運算雲端執行個體、Amazon Kinesis 串流或 Amazon DynamoDB 表。您可以使用資源中繼資料 (例如名稱、標籤和 ID) 來搜尋資源。資源總管AWS 區域在您的帳戶中運作，以簡化跨區域的工作負載。

資源總管使用服務建立和維護的索引，提供快速回應您的搜尋查AWS 資源總管詢。資源總管使用各種資料來源來收集AWS 帳戶. 資源總管將該資訊儲存在索引中，以供資源瀏覽器搜尋。

> 我們希望您對此文件的意見反應
>
> 我們的目標是幫助您從資源瀏覽器中獲得所有可能的一切。如果本指南可以幫助您做到這一點，請告訴我們。如果指南對您沒有幫助，那麼我們希望收到您的來信，以便我們解決此問題。使用每個頁面右上角的「意見反應」連結。這將您的評論直接發送給本指南的作者。我們審查每一個提交，尋找改進文檔的機會。預先感謝您的幫助！

主題

您是第一次使用資源總管的使用者嗎？

如果您是資源總管的第一次使用者，建議您先閱讀 [開始使用] 區段中的下列主題：

- 資源總管的術語和概念
- 使用快速設定設定資源總管

資源瀏覽器的功能

資源總管提供下列功能：

- 使用者可以搜尋其中的資源，AWS 區域或在其中跨區域搜尋資源AWS 帳戶。
- 使用者可以使用關鍵字、搜尋運算子和標籤等屬性，將搜尋結果篩選為僅符合資源。
- 當使用者在搜尋結果中找到資源時，他們可以立即前往資源的原生主控台以使用該資源。
- 管理員可以建立檢視，以定義搜尋結果中可用的資源。管理員可以根據使用者的工作，為不同群組的使用者建立不同的檢視，並僅將檢視權限授予需要檢視的使用者。
- 像許多其他資源管理器一樣AWS 服務，最終是一致的。資源總管透過在全球 Amazon 資料中心內的多個伺服器上複寫資料，以達到高可用性。如果變更一些資料的請求成功完成，則該變更經認可並安全儲存。但是，必須在資源總管之間複製變更，這可能需要一些時間。例如，這包括「資源總管」在一個區域中尋找資源，然後將其複寫到包含帳戶彙總器索引的「區域」。

相關 AWS 服務

以下是AWS 服務其主要目的是幫助您管理AWS資源的另一個：

AWS Resource Access Manager (AWS RAM)

與其他人共享一AWS 帳戶個資源AWS 帳戶。如果您的帳戶由管理AWS Organizations，您可AWS RAM以使用與組織單位中的帳號或組織中的所有帳號共用資源。共用資源適用於這些帳戶中的使用者，就像在本機帳戶中建立時一樣。

AWS Resource Groups

為您的AWS資源建立群組。然後，您可以將每個組作為一個單元使用和管理，而不必單獨引用每個資源。您的群組可以包含屬於相同AWS CloudFormation堆疊一部分的資源，或使用相同標籤加上標籤的資源。某些資源類型也支援將配置套用至資源群組，以影響該群組中的所有相關資源。

標籤編輯器和 AWS Resource Groups Tagging API

標籤是客戶定義的中繼資料，您可以附加至資源。您可以根據成本分配和基於屬性的訪問控制等目的對資源進行分類。

存取資源總管

您可以透過下列方式與資源總管互動：

資源總管主控台

資源總管提供了一個基於 Web 的用戶界面，即資源總管控制台。如果您已註冊AWS 帳戶，則可以登入AWS Management Console並從主控台首頁選擇 [資源總管]，以存取 [資源總管] 主控台。

您也可以直接在瀏覽器中導覽至 [資源總管] 儀表板頁面或 [資源搜尋] 頁面。如果您尚未登入，系統會要求您在主機出現之前進行登入。

> **Note**
>
> 資源瀏覽器控制台是一個AWS 區域全局控制台，這意味著您不必選擇要在其中工作。但是，當您使用資源總管來建立索引或檢視時，您需要指定索引或檢視儲存在哪個區域。當您使用資源總管進行搜尋時，您可以選擇您有權存取的任何檢視。結果會自動來自與所選視圖相關聯的「區域」。如果檢視來自包含彙總器索引的「區域」，則結果會包含您在其中建立資源總管索引之所有區域的資源。

AWS Management Console統一搜索

在每個頁面的頂部AWS Management Console，有一個搜索欄。您可以將資源總管配置為參與統一搜尋。然後，您的使用者可以在統一搜尋文字方塊中使用 Resource Explorer 搜尋查詢語法，並在這些搜尋結果中查看相符的資源。開啟此功能後，使用者可以從任何控制台搜尋資源，AWS 服務而不必先切換至 Resource Explorer 主控台。

> **Important**
>
> 統一搜尋一律會使用包含彙總器索引的AWS 區域預設檢視進行搜尋。

中的資源總管命令AWS CLI和適用於 Windows 的工具 PowerShell

PowerShell 提供直接存取資源總管公用 API 作業的AWS CLI和工具。這些工具可在視窗、macOS 和 Linux 上運作。若要取得有關入門的更多資訊，請參閱《AWS Command Line Interface使用指南》或《AWS Tools for Windows PowerShell使用指南》。如需資源總管之命令的相關資訊，請參閱命AWS CLI令參考或 C AWS Tools for Windows PowerShellmdlet 參考。

AWSSDK 中的資源總管作業

AWS為廣泛的程式設計語言提供 API 命令。如需有關入門的更多相關資訊，請參閱 搭 AWS 資源總管 配 AWS SDK 使用。

查詢 API

如果您不使用其中一種支援的程式設計語言，資源總管 HTTPS 查詢 API 可讓您以程式設計方式存取資源總管。使用資源總管 API，您可以直接向服務發出 HTTPS 要求。當您使用資源總管 API

時，您必須包含可以使用您的AWS認證以數位方式簽署要求的程式碼。如需詳細資訊，請參閱 AWS 資源總管 API 參考。

定價

使用搜尋資源無須支付任何費用AWS 資源總管，包括建立檢視表、開啟「區域」或搜尋資源。在建立資源清查的過程中，資源總管會代表您呼叫 API，這可能會產生費用。與您在搜尋結果中找到的資源互動可能會產生使用費用，這取決於資源類型及其資源類型AWS 服務。如需有關正常使用特定資源類型如何計AWS費的詳細資訊，請參閱該資源類型擁有服務的說明文件。

開始使用資源總管

使用本節中的主題可基本瞭解所使用的概念和術語AWS 資源總管。瞭解成功使用資源總管必須滿足的必要條件，以及如何在AWS 帳戶.

主題

- 資源總管的術語和概念
- 使用資源總管的先決條件
- 設定和設定資源總管

資源總管的術語和概念

AWS 資源總管 是一項資訊搜尋和探索服務。使用資源總管，您可以使用類似網際網路搜尋引擎的體驗來探索您的資源。您可以使用資源中繼資料 (例如名稱、標籤和 ID) 來搜尋資源，例如 Amazon 彈性運算雲端執行個體、Amazon Kinesis 串流或 Amazon DynamoDB 表。資源總管AWS 區域在您的帳戶中運作，以簡化跨區域的工作負載。

資源總管使用服務建立和維護的索引，提供快速回應您的搜尋查AWS 資源總管詢。資源總管使用各種資料來源來收集AWS 帳戶. 資源總管將該資訊儲存在索引中，以供資源瀏覽器搜尋。

您應該瞭解下列概念，才能成功管理和設定您AWS 資源總管的使用者。

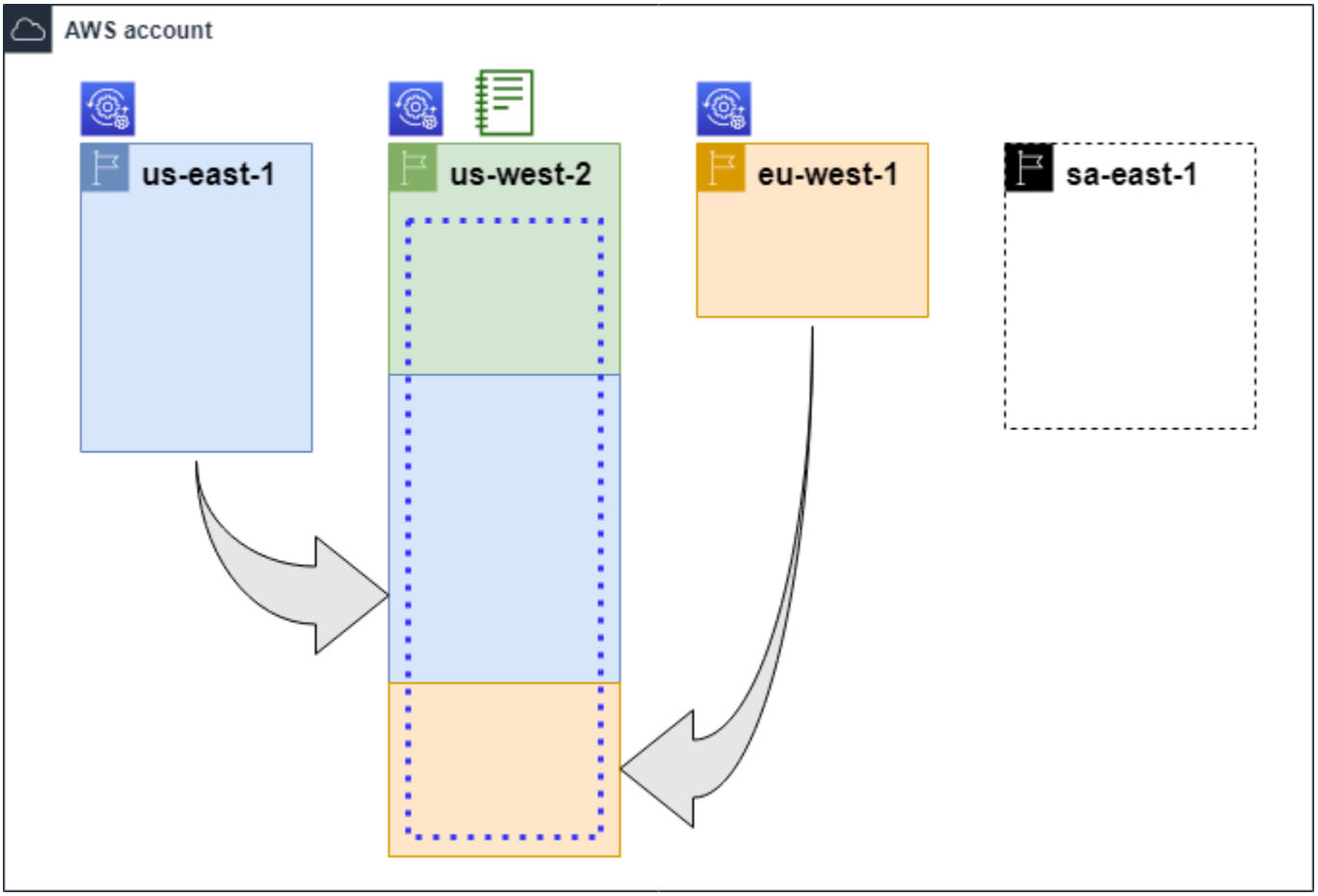
概念

- 資源總管管理員
- 資源總管使用者
- 索引
- 檢視
- 資源
- 在統一搜索 AWS Management Console
- 多帳戶搜尋

下圖顯示管理員開啟「資源總管」的三AWS 區域個，以及一個管理員選擇不開啟的「區域」。未開啟資源總管的區域沒有索引。因此，資源總管查詢無法搜尋其資源。

在此範例案例中，系統管理員選擇美國西部 (奧勒岡us-west-2) 區域 () 來包含帳戶的彙總索引。您開啟的所有區域會使用彙總索引，將其區域索引複寫到「區域」。

資源總管創建的默認視圖沒有任何過濾器。因此，使用此檢視進行搜尋的結果可能會包含已開啟資源總管之帳號中所有區域中任何類型的資源。



傳奇	
	資源瀏覽器已在此處打開AWS 區域，有關該區域資源的信息存儲在該區域的本地索引中。每個區域的區域索引也會複寫 (以箭頭表示) 到包含彙總器索引的「區域」。
	其中的索引設定AWS 區域為帳戶的彙總索引。Resource Explorer 會將已開啟資源總管之所有其他區域的本機索引中收集的資源資訊複製到此區域的彙總器索引中。在此區域中進行的搜尋可以包含帳戶中所有區域的結果。
	「快速設定」所建立的預設檢視表包含所有資源AWS 區域。

資源總管管理員

資源總管管理員是 AWS Identity and Access Management (IAM) 主體，具有管理資源總管及其在整個組織AWS 帳戶。資源總管管理員可以配置以下功能：

- 透過在這些區域中建立索引，為AWS 區域中AWS 帳戶的個人開啟資源總管。這可讓 Resource Explorer 探索資源，並將這些資源的相關資訊填入索引，以便使用者可以搜尋該區域中的資源。
- 在一個更新索引類型，AWS 區域使其成為其AWS 帳戶聚合索引。此區域中的彙總器索引會從已開啟資源總管的帳號中的所有其他區域接收資源資訊的複製副本。
- 建立定義使用者可在資源總管中搜尋和探索索引資訊子集的檢視。
- 雖然不是「資源總管」動作的一部分，但資源總管管理員還必須能夠將搜尋權限授與帳號中的主參與者。管理員可以將相關許可新增至現有 IAM 權限政策，或使用 Resource Explorer 唯讀AWS受管政策，將這些權限授與主體。

  若要提供存取權，請新增權限至您的使用者、群組或角色：

  - AWS IAM Identity Center 中的使用者和群組：

    建立權限合集。請遵循 AWS IAM Identity Center 使用者指南 的 建立權限合集 中的指示。
  - 透過身分提供者在 IAM 中管理的使用者：

    建立聯合身分的角色。請遵循 IAM 使用者指南 的 為第三方身分提供者 (聯合) 建立角色 中的指示。
  - IAM 使用者：
    - 建立您的使用者可擔任的角色。請遵循 IAM 使用者指南 的 為 IAM 使用者建立角色 中的指示。
    - (不建議) 將政策直接連接至使用者，或將使用者新增至使用者群組。請遵循 IAM 使用者指南 的 新增權限至使用者 (主控台) 中的指示。

管理員通常擁有所有資源總管資源管理器資源的所有資源總管權限 (`resource-explorer-2:*`)，包括索引和檢視。您可以使用 [資源總管] 完整存取AWS受管理的原則來授與這些權限。

資源總管使用者

資源總管使用者是 IAM 主體，具有執行下列一或多項工作的權限：

- 使用檢視查詢資源總管來執行資源搜尋。資源總管使用者想要探索和尋找AWS資源，通常使用資源總Search管主控台，或 AWS SDK 或. AWS CLI

角色或使用者可以使用 IAM 取得權限，透過以下兩種方法之一進行搜尋：

- 資源總AWS管對 IAM 角色、群組或使用者的唯讀受管政策。
- IAM 許可政策，其中包含對 IAM 角色、群組或使用者的下列最低許可的陳述式。

```
{
    "Effect": "Allow",
    "Action": [
        "resource-explorer-2:Search",
        "resource-explorer-2:GetView",
    "Resource": "<ARN of the view>"
}
```

- 雖然通常被視為管理員工作，但您可以將定義建立檢視的能力委派給信任的使用者。為此，管理員可以授予權限，以`resource-explorer-2:CreateView`便在附加到相關角色、群組或使用者的 IAM 權限政策中呼叫作業。如果檢視需要特定許可，則必須為相關使用者進行佈建，以新增或修改 IAM 政策。

如需如何使用資源總管搜尋資源的相關資訊，請參閱使用AWS 資源總管搜尋資源。

索引

索引是資源瀏覽器維護的有關所有AWS資源的信息的AWS 區域集合AWS 帳戶。資源總管會在您開啟「資源總管」的每個「區域」中維護索引。當您在中建立和刪除資源時，資源總管會自動更新索引AWS 帳戶。在先前的圖表中，AWS 區域名稱下的方塊代表每個索引中維護的資源總管索引AWS 區域。區域中的索引是在該區域中創建的任何視圖的信息來源。使用者無法直接查詢索引。相反，他們必須始終使用視圖進行查詢。

索引有兩種類型：

本地索引

在每個您開啟資源總管的每一個區域索引AWS 區域中都有一個區域索引。本機索引僅包含相同區域中資源的相關資訊。

聚合索引

資源總管管理員也可以將索引中AWS 區域的索引指定為的彙總索引AWS 帳戶。彙總器索引會針對在帳戶中開啟資源總管的其他每個區域接收並儲存索引的副本。聚合器索引還會在自己的區域中接收並存儲有關資源的信息。在先前的圖表中，「地區」us-west-2 包含帳戶的彙總器索引。為帳

戶指定彙總器索引的主要原因是，您可以建立可包含帳戶中所有區域資源的檢視表。一個中只能有一個彙總索引 AWS 帳戶

當您開啟 [資源總管] 時，您可以指定要AWS 區域包含彙總器索引的內容。您也可以稍後變更AWS 區域用於彙總索引的。如需有關如何升級區域索引以使其成為其彙總索引的資訊AWS 帳戶，請參閱透過建立彙總索引開啟跨區域搜尋。

索引是具有 Amazon 資源名稱（ARN）的資源。不過，您只能在權限原則中使用此 ARN，以授與直接與索引互動之作業的存取權。透過這些作業，您可以建立檢視並將其設定為 [區域] 中的預設檢視、開啟或關閉 [區域] 中的 [資源總管]，以及為帳戶建立彙總器索引。索引的 ARN 看起來類似下列範例：

```
arn:aws:resource-explorer-2:us-east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-
abcd11111111
```

檢視

視圖是用於查詢索引中列出的資源的機制。此檢視會定義索引中的哪些資訊可見，以及可用於搜尋和探索目的。使用者永遠不會直接查詢資源總管索引。相反，查詢必須始終通過一個視圖，該視圖創建者可以限制用戶可以在搜索結果中查看的資源。

建立檢視表時，您可以指定篩選條件，以限制搜尋結果中包含哪些資源。例如，您可以選擇僅包含少數指定資源類型的資源，這些資源類型可供您授與此檢視的存取權限的使用者使用。使用者使用檢視進行的查詢結果一律會自動篩選，以僅包含符合檢視條件的資源。

若要授與使用檢視的存取權限，您可以使用下列其中一種方法來使用指派權限。

若要提供存取權，請新增權限至您的使用者、群組或角色：

- AWS IAM Identity Center 中的使用者和群組：

  建立權限合集。請遵循 AWS IAM Identity Center 使用者指南 的 建立權限合集 中的指示。
- 透過身分提供者在 IAM 中管理的使用者：

  建立聯合身分的角色。請遵循 IAM 使用者指南 的 為第三方身分提供者 (聯合) 建立角色 中的指示。
- IAM 使用者：
  - 建立您的使用者可擔任的角色。請遵循 IAM 使用者指南 的 為 IAM 使用者建立角色 中的指示。
  - (不建議) 將政策直接連接至使用者，或將使用者新增至使用者群組。請遵循 IAM 使用者指南 的 新增權限至使用者 (主控台) 中的指示。

授予權限以允許您的角色、群組或使用者在由其 Amazon 資源名稱 (ARN) 識別的檢視上叫用`resource-explorer-2:GetView`和`resource-explorer-2:Search`操作。或者，您可以針對需要使用檢視進行搜尋的所有主參與者使用 Resource Explorer 唯讀AWS受管理的原則。您可以建立具有不同篩選器和範圍的多個檢視，從而傳回資源資訊的不同子集。然後，您可以將每個檢視的權限授與需要查看該檢視結果所包含資訊的使用者。

若要使用資源總管進行搜尋，每個使用者都必須具有至少使用一個檢視的權限。如果不使用檢視，就無法在資源總管中執行搜尋。

視圖存儲在每個區域的基礎上。視圖只能訪問其中的資源瀏覽器索引AWS 區域。若要存取整個帳戶的搜尋結果，您必須使用「地區」中包含帳戶彙總索引的檢視。快速設定選項會在中建立預設檢視，並使AWS 區域用包含帳戶所AWS 區域使用之全部資源中所有資源的篩選器。

若要取得有關如何建立視圖的資訊，請參閱管理資源總管檢視以提供搜尋存取權。若要取得有關如何在查詢中使用檢視的資訊，請參閱〈〉使用AWS 資源總管搜尋資源。

每個檢視都有一個 Amazon 資源名稱 (ARN)，您可以在權限政策中參考該名稱，以授予對個別檢視的存取權。您還可以將視圖的 ARN 作為參數傳遞給與視圖交互的任何 API 或AWS CLI操作。檢視的 ARN 看起來類似下列範例。

```
arn:aws:resource-explorer-2:us-east-1:123456789012:view/My-View-
Name/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111
```

> **Note**
>
> 每個視圖 ARN 在最後都包含一個AWS生成的 UUID。這有助於確保可能有權存取已刪除之特定名稱之檢視的使用者無法自動存取以相同名稱建立的新檢視。

資源

資源是您可以AWS使用的實體。AWS 服務當您使用服務的功能時，會建立資源。範例包括 Amazon EC2 執行個體、Amazon S3 儲存貯體或AWS CloudFormation堆疊。某些資源類型可以包含客戶資料。所有資源類型都有屬性或中繼資料來描述資源，包括名稱、說明以及您用來唯一參照資源的 Amazon 資源名稱 (ARN)。大多數資源類型也支援標籤。標籤是您可以基於各種目的附加至資源的自訂中繼資料，例如帳單中的成本分配、使用以屬性為基礎的存取控制的安全授權，或支援其他分類需求。

資源瀏覽器的主要目的是幫助您找到AWS 帳戶. 資源總管使用各種技術來發現您的所有資源，並將有關它們的信息放在索引中。然後，您可以透過管理員提供給您的任何檢視來查詢索引。

> **Important**
>
> 資源總管故意排除那些包含會暴露客戶資料的資源類型。下列資源類型不會由資源總管建立索引，因此不會在搜尋結果中傳回。
>
> - 儲存貯體中包含的 Amazon S3 物件
> - Amazon DynamoDB 格項目
> - 屬性值

在統一搜索 AWS Management Console

在的頂部AWS Management Console，在每個AWS 服務，有一個搜索欄，您可以使用它來搜索各種AWS相關的事物。您可以搜尋服務和功能，並直接取得該服務主控台中相關頁面的連結。您也可以搜尋與搜尋字詞相關的文件和部落格文章。

在您開啟資源總管並建立彙總器索引和預設檢視之後，統一搜尋也可以在搜尋結果中包含您帳戶的資源。統一搜尋會自動使用包AWS 區域含帳戶彙總索引的預設檢視。這可讓您從中的任何頁面搜尋資源AWS Management Console，而不必先開啟資源總管。如果您未將本機索引提升為帳戶的彙總索引，或者未在彙總器索引 Region 中建立預設檢視表，則統一搜尋不會在其搜尋結果中包含資源。此外，執行搜尋的任何主參與者都必須擁有使用「地區」(Region) 中包含彙總器索引的預設檢視的權限，否則統一搜尋不會在其搜尋結果中包含資源。

> **Important**
>
> 統一搜尋會在字串中第一個關鍵字的結尾自動插入萬用字元 (*) 運算子。這意味著統一的搜索結果包括匹配以指定關鍵字開頭的任何字符串的資源。
> [資源總管] 主控台中 [資源搜尋] 頁面上的 [查詢] 文字方塊執行的搜尋不會自動附加萬用字元。您可以在搜尋字串中的任何字詞之後*手動插入。

如需統一搜尋及其與資源總管整合的詳細資訊，請參閱在中使用統一搜尋 AWS Management Console。

多帳戶搜尋

透過多帳戶搜尋，您可以透過單一關鍵字搜尋來搜尋AWS Organizations和AWS 區域探索資源。

如需有關多帳號搜尋以及如何針對資源總管啟用此搜尋的詳細資訊，請參閱開啟多帳戶搜尋。

使用資源總管的先決條件

第一次使AWS 資源總管用前，請根據需要完成以下任務。

任務

- 註冊 AWS 帳戶
- 建立管理使用者

註冊 AWS 帳戶

如果您還沒有 AWS 帳戶，請完成以下步驟建立新帳戶。

註冊 AWS 帳戶

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

   部分註冊程序需接收來電，並在電話鍵盤輸入驗證碼。

   註冊 AWS 帳戶時，會建立 AWS 帳戶根使用者。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。

註冊程序完成後，AWS 會傳送一封確認電子郵件給您。您可以隨時登錄 https://aws.amazon.com/ 並選擇 我的帳戶，以檢視您目前的帳戶活動並管理帳戶。

建立管理使用者

當您註冊 AWS 帳戶 之後，請保護您的 AWS 帳戶根使用者，啟用 AWS IAM Identity Center，並建立管理使用者，讓您可以不使用根使用者處理日常作業。

保護您的 AWS 帳戶根使用者

1. 選擇 根使用者 並輸入您的 AWS 帳戶電子郵件地址，以帳戶擁有者身分登入 AWS Management Console。在下一頁中，輸入您的密碼。

   如需使用根使用者登入的說明，請參閱 AWS 登入使用者指南中的以根使用者身分登入。
2. 若要在您的根使用者帳戶上啟用多重要素驗證 (MFA)。

如需指示，請參閱《IAM 使用者指南》中的為 AWS 帳戶根使用者啟用虛擬 MFA 裝置 (主控台)。

建立管理使用者

1. 啟用 IAM Identity Center。

   如需指示，請參閱 AWS IAM Identity Center 使用者指南中的啟用 AWS IAM Identity Center。
2. 在 IAM Identity Center 中，將管理權限授予管理使用者。

   若要取得有關使用 IAM Identity Center 目錄 做為身分識別來源的教學課程，請參閱《使用 AWS IAM Identity Center 使用者指南中的以預設 IAM Identity Center 目錄 設定使用者存取權限。

以管理員的身分登入

- 若要使用您的 IAM 身分中心使用者登入，請使用建立 IAM 身分中心使用者時傳送至您電子郵件地址的登入 URL。

  如需有關如何使用 IAM Identity Center 使用者登入的說明，請參閱《AWS 登入 使用者指南》中的登入 AWS存取入口網站。

設定和設定資源總管

在您可以設定和設定之前 AWS 資源總管，請先確定您符合先決條件。之後，以 IAM 角色或具有執行資源總管操作所需許可的使用者身分登入，以執行下列程序。

您可以使用此設定和組態程序，在現有帳號以及新增至組織的任何新帳號中設定資源總管。

有兩種方法可以設定資源總管：

- 快速設定
- 進階設定

> **Important**
>
> 如果您選擇使用任何顯示 AWS 區域「全部」的選項來設定 Resource Explorer，它只會啟動 AWS 區域 已存在且在執行程序時已啟用的選項。 AWS 帳戶資源總管不會在 future AWS 添加的任何 AWS 區域 內容中自動打開。 AWS 引入新的 [區域] 時，您可以選擇在 [資源

總管] 主控台的 [設定] 頁面中顯示 [資源總管] 時，手動開啟 [區域] 中的 [資源總管]，或呼叫CreateIndex作業。

> **Note**
>
> 設定資源總管也可以使用上的統一搜尋列來開啟搜尋資源的功能 AWS Management Console。若要讓使用者在統一搜尋結果中查看資源，您必須使用跨區域彙總器索引和預設檢視來設定資源總管。如需詳細資訊，請參閱下列程序。您還必須確保您的搜尋使用者具有使用包含彙總索引的 AWS 區域 預設檢視的權限。如需詳細資訊，請參閱 在中使用統一搜尋 AWS Management Console。

使用快速設定設定資源總管

如果您選擇 [快速設定] 選項，[資源總管] 會執行下列動作：

- 在您的每 AWS 區域 個 AWS 帳戶.
- 更新您指定為帳戶彙總索引之區域中的索引。
- 在彙總索引區域中建立預設檢視。此檢視沒有篩選條件，因此會傳回索引中找到的所有資源。

最低許可

若要執行下列程序中的步驟，您必須具備下列權限：

- 動作：`resource-explorer-2:*`— 資源：沒有特定資源（*）
- 動作：`iam:CreateServiceLinkedRole`— 資源：沒有特定資源（*）

AWS Management Console

使用快速設定設定資源總管

1. 在開啟AWS 資源總管 主控台https://console.aws.amazon.com/resource-explorer。
2. 選擇 [開啟資源總管]。
3. 在 [開啟資源總管] 頁面上，選擇 [快速設定]。
4. 選擇 AWS 區域 您要包含彙總索引的索引。您應該為使用者選取適合地理位置的區域。
5. 在頁面底部，選擇 [開啟資源總管]。

6. 在 [進度] 頁面上，您可以在資源總管建立其索引時監視每個 AWS 區域 項目。此頁面會顯示建立彙總器索引和建立預設檢視的狀態。

在所有步驟都顯示成功完成後，您和您的使用者可以導覽至 [資源搜尋] 頁面並開始搜尋資源。

> **Note**
>
> 索引本機的標記資源會在幾分鐘內出現在搜尋結果中。未標記的資源通常需要不到兩個小時的時間才能顯示，但需求繁忙時可能需要更長的時間。從所有現有的本機索引完成對新彙總器索引的初始複寫作業最多可能需要一小時的時間。

後續步驟：您必須先授與使用者使用您剛才建立的預設檢視進行搜尋的權限，使用者才能進行搜尋。如需詳細資訊，請參閱 授與資源總管檢視的存取權以進行搜尋。

AWS CLI

根據定義，在您 AWS 帳戶 的中設定資源總管，等同於 [進階設定] 選項。 AWS CLI 這是因為資源總管 CLI 作業不會像資源總管主控台那樣自動為您執行任何步驟。請參閱上的 AWS CLI 索引標籤，使用進階設定設定來設定資源總管 以瞭解與使用主控台相同的指令。

使用進階設定設定來設定資源總管

如果您選擇 [進階設定] 選項，您可以執行下列動作：

- 選擇要 AWS 區域 在其中開啟資源總管的。
- 選擇是否使用彙總索引設定一個「區域」。如果這樣做，您可 AWS 區域 以指定要放置它的。此索引可讓您建立檢視，其中包含帳戶中所有區域的資源。如需詳細資訊，請參閱透過建立彙總索引來開啟跨區域搜尋。
- 選擇是否要建立預設檢視表。該視圖允許自動搜索您在其中打開 AWS 資源總管的區域中的任何資源。您必須確保需要使用預設檢視在 Resource Explorer 中搜尋的任何主參與者都具有檢視的權限。如需詳細資訊，請參閱 授與資源總管檢視的存取權以進行搜尋。

> **Note**
>
> 您可以將資源總管配置為在上統一搜尋功能提供的搜尋結果中包含您的資源 AWS Management Console。若要開啟此功能，您必須使用彙總器索引和預設檢視來設定 Resource

Explorer，讓所有角色和使用者都可以使用搜尋。[快速設定] 選項會同時建立彙總索引和預設檢視，並且是我們建議您開啟 [資源總管] 的方式。

最低許可

若要執行下列程序中的步驟，您必須具備下列權限：

- 動作：`resource-explorer-2:*`— 資源：沒有特定資源（*）
- 動作：`iam:CreateServiceLinkedRole`— 資源：沒有特定資源（*）

AWS Management Console

使用進階設定開啟資源總管

1. 在開啟AWS 資源總管 主控台https://console.aws.amazon.com/resource-explorer。
2. 選擇 [開啟資源總管]。
3. 在 [開啟資源總管] 頁面上，選擇 [進階設定]。
4. 在 [區域 AWS 區域] 下方塊中，選擇您要開啟 [全部] 中的 [資源總管] AWS 區域，還是只開啟特定區域。

   如果您只在此帳號中指定 AWS 區域 的選項中選擇「開啟資源總管」，請選取您要將其資源包含在搜尋結果中的每個區域。
5. 針對彙總索引，選擇是否要建立彙總索引。如果您選擇建立彙總索引，其他所有其他都會將其索引 AWS 區域 複製到此區域。這可讓使用者在中搜尋所有選取區域的資源 AWS 帳戶。選擇包 AWS 區域 含彙總器索引的。我們建議您指定使用者花費大部分時間的地區，或者至少您希望他們執行大部分資源搜尋的地區。
6. 在「預設」檢視方塊中的「視圖建立」下，選擇是否要建立預設視圖。只有在您選擇建立彙總索引時，才能使用此選項。如果您選擇建立預設檢視，資源總管會將此檢視置於與彙總器索引 AWS 區域 相同的檢視中。這可讓預設檢視包含您 AWS 區域 在其中註冊資源總管的所有結果。每當用戶使用默認視圖在「區域」中執行搜索時，並且沒有明確指定視圖時，搜索都會使用該區域的默認視圖。

> **Note**
>
> 在您的使用者可以使用檢視進行搜尋之前，您必須授與他們使用該檢視的權限。如需詳細資訊，請參閱 授與資源總管檢視的存取權以進行搜尋。

7. 選擇 [啟動資源總管]。

> **Note**
>
> 索引本機的標記資源會在幾分鐘內出現在搜尋結果中。未標記的資源通常需要不到兩個小時的時間才能顯示，但需求繁忙時可能需要更長的時間。從所有現有的本機索引完成對新彙總器索引的初始複寫作業最多可能需要一小時的時間。

AWS CLI

使用進階設定設定來設定資源總管

資源總管主控台會根據您所做的選擇代表您執行許多 API 作業呼叫。下列範例 AWS CLI 命令說明如何使用控制台外部執行相同的基本程序 AWS CLI。

Example 步驟 1：通過在所需的索引中創建索引來打開資源瀏覽器 AWS 區域

在您要啟動資源總管 AWS 區域 的每個命令中執行下列命令。下列範例命令會在預設的 AWS 區域 中開啟資源總管 AWS CLI。

```
$ aws resource-explorer-2 create-index
{
    "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "CreatedAt": "2022-07-27T16:17:12.130000+00:00",
    "State": "CREATING"
}
```

Example 步驟 2：將索引更新為 AWS 區域 帳戶的聚合索引

在您希望資源總管將本機索引更新為帳戶彙總器索引的 AWS 區域 中執行下列命令。下列範例命令會更新美國東部 (維吉尼亞北部) (us-east-1) 中的彙總器索引。

```
$ aws resource-explorer-2 update-index-type \
```

```
    --arn arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111 \
    --type AGGREGATOR
{
    "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "LastUpdatedAt": "2022-07-27T16:29:49.231000+00:00",
    "State": "UPDATING",
    "Type": "AGGREGATOR"
}
```

Example 步驟 3：在包含彙總索 AWS 區域 引的中建立檢視

在您建立彙總索引的 AWS 區域 中執行下列命令。下列範例命令會建立與 Resource Explorer 主控台安裝程序所建立的檢視相同的檢視。這個新檢視包括作為索引資訊一部分附加至資源的標籤，並支援依標籤索引鍵或值搜尋資源。

```
$ aws resource-explorer-2 create-view \
    --view-name My-New-View \
    --included-properties Name=tags
{
    "View": {
        "Filters": {
            "FilterString": ""
        },
        "IncludedProperties": [
            {
                "Name": "tags"
            }
        ],
        "LastUpdatedAt": "2022-07-27T16:34:14.960000+00:00",
        "Owner": "123456789012",
        "Scope": "arn:aws:iam::123456789012:root",
        "ViewArn": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/My-New-
View/1a2b3c4d-5d6e-7f8a-9b0c-abcd22222222"
    }
}
```

Example 步驟 4：將新檢視設定為其預設檢視 AWS 區域

下列範例會將您在上一個步驟中建立的檢視設定為「區域」(Region) 的預設檢視。您必須在其中創建默認視圖 AWS 區域 的相同命令運行以下命令。

```
$ aws resource-explorer-2 associate-default-view \
    --view-arn arn:aws:resource-explorer-2:us-east-1:123456789012:view/My-New-
View/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111
{
    "ViewArn": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/My-New-
View/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
}
```

在您的使用者可以使用檢視進行搜尋之前，您必須授與他們使用該檢視的權限。如需詳細資訊，請參閱 授與資源總管檢視的存取權以進行搜尋。

執行這些命令之後，資源總管會在您的 AWS 帳戶. 資源總管在每個區域中構建和維護索引，其中包含位於該處的資源的詳細信息。資源總管會將每個個別區域索引複寫到指定區域中的彙總器索引。該區域還包含一個檢視，允許帳戶中的任何 IAM 角色或使用者搜尋所有索引區域的資源。

> **Note**
>
> 索引本機的標記資源會在幾分鐘內出現在搜尋結果中。未標記的資源通常需要不到兩個小時的時間才能顯示，但需求繁忙時可能需要更長的時間。從所有現有的本機索引完成對新彙總器索引的初始複寫作業最多可能需要一小時的時間。

管理資源總管以支援搜尋資源

在您的至少一個AWS 資源總管AWS 區域中開啟之後AWS 帳戶，您可能需要偶爾執行一些管理工作。本節說明維護和組態工作，這些工作可協助您讓 Resource Explorer 以您希望的方式隨著您AWS 帳戶和資源使用情況的發展進行運作。

主題

檢查哪個AWS 區域已開啟資源瀏覽器

你可以找出哪個AWS 區域有AWS 資源總管透過檢查哪些區域包含資源總管索引來啟用。若要檢視哪些區域具有索引，請使用此頁面上的程序。

> **Important**
>
> 使用者可以搜尋資源只要那些已開啟資源總管的區域。您也可以在一個區域中建立彙總器索引，以支援搜尋所有區域中的資源。資源總管會使用來自包含資源總管索引之所有其他區域的彙總器索引，將資源資訊複製到「區域」。使用者無法使用資源總管探索沒有索引的區域中的資源。

檢查區域中的資源總管狀態

您可以檢查哪些區域具有資源總管的索引，方法是使用AWS Management Console，透過使用中的指令AWS Command Line Interface(AWS CLI)，或透過在AWSSDK。

AWS Management Console

若要檢查哪些區域具有資源總管的索引

1. 打開設定資源瀏覽器控制台中的頁面。
2. 中的列表索引區段僅包含那些包含資源總管索引的區域。中的值类型列指示索引是否為本地其地區的索引，或聚合器索引AWS 帳戶。
3. 若要查看哪些區域不包含資源總管，請選擇建立索引。如果「區域」不存在，則「區域」不包含「資源總管」。

AWS CLI

若要檢查哪些區域具有資源總管的索引

運行以下命令以查看哪個AWS 區域有資源瀏覽器的索引。

```
$ aws resource-explorer-2 list-indexes
{
    "Indexes": [
        {
            "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
            "Region": "us-east-1",
            "Type": "AGGREGATOR"
        },
        {
            "Arn": "arn:aws:resource-explorer-2:us-
west-2:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd22222222",
            "Region":"us-west-2",
            "Type":"LOCAL"
        }
    ]
}
```

開啟多帳戶搜尋

透過多帳戶搜尋，您可以在您 AWS Organizations 或組織單位 (OU) 中具有作用中索引的帳號之間搜尋資源。

主題

必要條件

若要為您的組織啟用多帳戶搜尋，請完成下列步驟：

- 建立管理使用者。
- 使`aws iam create-service-linked-role --aws-service-name resource-explorer-2.amazonaws.com`用在管理員帳戶中建立服務連結角色。
- 在中啟用受信任的存取 AWS Organizations。這可讓您與資源總管完全整合，以列出組織中所有帳號的資源。
- 指派委派的管理員 (建議)。如需詳細資訊，請參閱《AWS Organizations 使用指南》中的「委派管理員」以瞭解與 Organizations 合作的 AWS 服務。
  - 資源總管僅支援 1 位委派管理員，他們執行與管理帳戶類似的動作。
  - 移除或變更組織的委派系統管理員會導致移除其帳戶中建立的所有多帳戶檢視。

啟用多帳戶搜尋

若要搜尋並探索組織帳戶中的資源，您必須完成下列步驟：

1. 在您的. AWS 資源總管 中的一個或多個帳戶中啟用 AWS Organizations.
2. 註冊一個區域以包含彙總器索引。
3. 選擇要在其中建立彙總索引的區域。此區域必須在您的 AWS Organizations.
4. 建立範圍為您 AWS Organizations 或組織單位的資源總管檢視。在上一個步驟的彙總器「區域」中建立此檢視表。
5. 與整個組織的帳戶共用檢視。

多帳戶快速設定

使用 [快速設定] 在組織中的多個帳號上啟用資源總管。

> **Note**
>
> 此程序不會在管理帳戶中部署任何資源。如果您使用的是管理帳戶，且想要在帳號中建立索引，則必須使用 Resource Explorer 上線流程手動新增這些索引。

1. 導覽至系統管理員主控台中資源總管的快速設定。
2. 選擇您的彙總索引區域。這可讓您搜尋位於所選目標帳號之所有區域中的資源。如果任何選取的目標帳戶已在其他區域中設定彙總索引，則現有的彙總器索引將自動取代為此新區域。
3. 選擇您的帳戶目標。您可以為整個組織或特定組織單位 (OU) 啟用資源總管。

   > **Note**
   >
   > 您一次最多可以部署 50,000 個堆疊。如果您的大型組織跨越多個區域，您應該以較小的批次在 OU 層級部署。

4. 在選擇「建立」之前，請先閱讀確認摘要。

在中打開資源瀏覽器AWS 區域以索引您的資源

當您最初開啟時AWS 帳戶，您會AWS 資源總管在一或多個中建立服務的索引AWS 區域。如果您使用快速設定選項，資源總管會自動在您的AWS 帳戶.AWS 區域 資源總管服務也會將指定區域中的索引提升為帳號的彙總器索引。如果您使用「進階」設定選項，則指定了要在其中建立索引的「區域」。

若要在其他區域中開啟資源總管，請使用本主題中的程序。

當您在中開啟資源總管時AWS 區域，服務會執行下列動作：

- 當您在第一個區域中啟動資源總管時AWS 帳戶，資源總管會在名為的帳號中建立服務連結角色AWSServiceRoleForResourceExplorer。此角色授與使用服務 (例如和標記服務)，讓 Resource Explorer 探索您帳戶中的資源AWS CloudTrail並建立索引的權限。只有當您AWS 區域在帳戶中註冊第一個角色時，才會建立服務連結角色。資源總管會針對您稍後新增的所有區域，使用相同的服務連結角色。
- 資源總管在指定的區域中創建索引，以存儲有關該區域資源的詳細信息。
- Resource Explorer 會開始探索指定區域中的資源，並將找到的資源相關資訊新增至該區域的索引。
- 如果您的帳戶已經包含不同區域中的彙總器索引，Resource Explorer 會開始將資訊從新區域的索引複製到彙總器索引，以支援跨區域搜尋。

完成這些步驟後，使用者就可以探索有關資源的資訊。他們可以使用在相同區域或包含聚合器索引的區域中定義的其中一個檢視來進行搜尋。

在區域中建立資源總管索引

您可以使用AWS Command Line Interface (AWS CLI) 中的命令AWS Management Console，或在AWS SDK 中使用 API 作業來建立其他AWS 區域資源總管索引。您只能在 East 中建立一個索引。

最低許可

若要執行以下程序中的步驟，您必須擁有下列許可：

- 動作：`resource-explorer-2:*`— 資源：沒有特定資源（*）
- 動作：`iam:CreateServiceLinkedRole`— 資源：沒有特定資源（*）

AWS Management Console

在中建立資源總管索引的步驟AWS 區域

1. 在 [資源總管設定] 頁面上。
2. 在「索引」區段中，選擇「建立索引」。
3. 在 [建立索引] 頁面上，選取您要AWS 區域在其中建立索引以支援搜尋該地區資源的索引旁邊的核取方塊。不可用的核取方塊表示已包含資源總管索引的區域。
4. (選擇性) 在「標籤」區段中，您可以指定索引的標籤鍵和值配對。
5. 選擇 [建立索引]。

   Resource Explorer 會在頁面頂端顯示綠色橫幅以表示成功，如果在一或多個選取的區域中建立索引時發生錯誤，則會顯示紅色橫幅。

> **Note**
>
> 索引本機的標記資源會在幾分鐘內出現在搜尋結果中。未標記的資源通常需要不到兩個小時的時間才能顯示，但需求繁忙時可能需要更長的時間。從所有現有的本機索引完成對新彙總器索引的初始複寫作業最多可能需要一小時的時間。

下一步 — 如果您已經建立彙總索引，則新的 Region 會自動開始將其索引資訊複製到彙總索引。如果這是您的使用者進行所有搜尋的地方，則新區域中的資源會顯示在這些搜尋結果中，而您就完成了。

不過，如果您希望使用者只能搜尋新建索引的「地區」中的資源，則您也必須為該區域中的使用者建立檢視，並將該檢視的權限授與使用者。如需如何建立視圖的詳細資訊，請參閱管理資源總管檢視以提供搜尋存取權。

AWS CLI

在中建立資源總管索引的步驟AWS 區域

針對您要AWS 區域在其中建立索引以支援搜尋該地區資源的每個執行下列命令。以下範例命令是在 US East (N. Virginia) 中註冊資源總管 (維吉尼亞北部us-east-1)。

```
$ aws resource-explorer-2 create-index \
    --region us-east-1
{
    "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "CreatedAt": "2022-11-01T20:00:59.149Z",
    "State": "CREATING"
}
```

針對您要在其中開啟「資源總管」的每個「區域」重複此指令，以適當的「區域」代碼取代--region參數。

因為 Resource Explorer 會在背景中以非同步工作的形式執行某些索引建立CREATING，因此回應可以是，表示背景處理程序尚未完成。

> **Note**
>
> 索引本機的標記資源會在幾分鐘內出現在搜尋結果中。未標記的資源通常需要不到兩個小時的時間才能顯示，但需求繁忙時可能需要更長的時間。從所有現有的本機索引完成對新彙總器索引的初始複寫作業最多可能需要一小時的時間。

您可以通過運行以下命令並檢查ACTIVE狀態來檢查最終完成。

```
$ aws resource-explorer-2 get-index \
    --region us-east-1
```

```
{
    "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "CreatedAt": "2022-07-12T18:59:10.503000+00:00",
    "LastUpdatedAt": "2022-07-13T18:41:58.799000+00:00",
    "ReplicatingFrom": [],
    "State": "ACTIVE",
    "Tags": {},
    "Type": "LOCAL"
}
```

下一步 — 如果您已經建立彙總索引，則新的 Region 會自動開始將其索引資訊複製到彙總索引。如果這是您的使用者進行所有搜尋的地方，則新區域中的資源會顯示在這些搜尋結果中，而您就完成了。

不過，如果您希望使用者只能搜尋新建索引的「地區」中的資源，則您也必須為該區域中的使用者建立檢視，並將該檢視的權限授與使用者。如需如何建立視圖的詳細資訊，請參閱管理資源總管檢視以提供搜尋存取權。

AWS 選擇加入區域的考量

選擇加入區域的安全要求高於商業區域，因為它與透過選擇加入區域中的帳戶共用 IAM 資料有關。透過 IAM 服務管理的所有資料都會被視為身分資料。

您可以使用AWS 資源總管 主控台啟用選擇加入區域。如需詳細資訊，請參閱在中 AWS 區域 開啟資源總管以建立資源索引。

退出行為

選擇退出選擇加入區域之前，請考慮下列行為：

> **Important**
>
> 在您選擇退出具有彙總索引的區域之前，建議您刪除彙總索引或將其降級為本機索引。資源總管支援分割區內所有區域的一個彙總器索引。

- 您的索引不會被刪除，只會停用。如果您選擇稍後再次選擇加入，您的設定將會回復。
- IAM 會停用對該區域中資源的 IAM 存取權。

- 資源總管會停用已選擇退出區域的索引，並停止擷取資料。該 `ListIndexes` API 將不再顯示區域索引。
- 如果您的彙總器索引位於不同的區域，Resource Explorer 會停止從選擇退出的區域進行資料複寫，並在 24 小時內清除資料。
- 如果您選擇退出彙總索引區域，則必須再次選擇加入才能刪除或降級索引。
- 如果您再次選擇加入「區域」，「資源總管」會重新啟用索引並開始擷取資料。
- 選擇加入區域狀態的任何變更都需要大約 24 小時才會生效。

透過建立彙總索引開啟跨區域搜尋

主題

關於彙總索引

AWS 資源總管AWS 區域將其收集的有關資源的資訊儲存在資源總管在該區域中建立和維護的本機索引中。例如，假設您在美國西部 (奧勒岡) 區域有一個 Amazon EC2 執行個體。資源總管會將該資源的詳細資料儲存在美國西部 (奧勒岡) 區域的本機索引中。

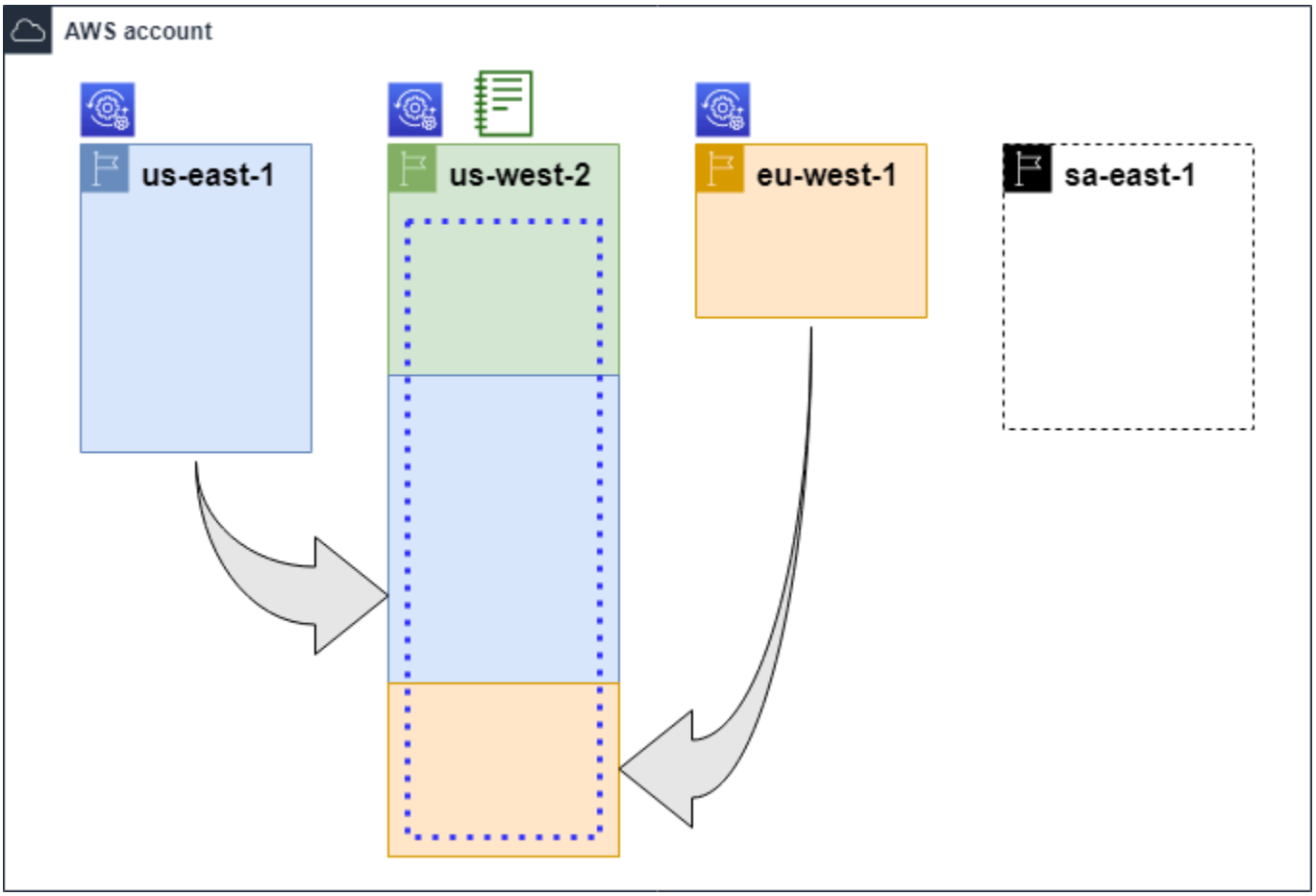
若要支援在帳戶AWS 區域中搜尋所有資源，您可以將一個區域中的本機索引轉換為帳戶的彙總索引。

在您開啟資源總管的每個其他區域中，彙總器索引包含本機索引的複寫副本。這可讓您在 [區域] 中建立包含彙總器索引的檢視，其結果可以包含帳戶AWS 區域中所有資源的彙總器索引。

下圖顯示了聚合器索引是如何工作的一個例子。在此範例中AWS 帳戶，系統管理員會執行下列動作：

- 透過在這些區域中建立索引 `us-east-1`、`us-west-2`、和`eu-west-1` (、和) 中開啟資源總管。每個區域都包含自己的區域索引。
- 選擇不在「`sa-east-1`區域」中建立索引。使用者無法在中執行搜尋`sa-east-1`，且搜尋結果中也不會顯示該區域的資源。
- 為`us-west-2`區域中的帳戶建立彙總索引。這會導致資源總管將資源總管開啟的所有其他區域中的本機索引中的資訊複製到彙總器索引。這允許在中執行`us-west-2`的搜尋包括開啟「資源總管」的所有三個區域的資源。

此組態表示使用者只能在中執行跨區域搜尋us-west-2，其中包含彙總器索引。只有該區域的檢視才能傳回帳戶中所有區域的結果。



傳奇	
	資源瀏覽器在此打開AWS 區域，其資源被編目為該區域中的索引。此區域的索引也會複寫 (以箭頭表示) 到包AWS 區域含彙總索引的。
	這AWS 區域包含聚合器索引。資源總管會將在所有其他資源中收集到的資源資訊複製AWS 區域到此區域中。
	「快速設定」所建立的預設檢視表包含所有資源AWS 區域。

將本機索引提升為帳戶的彙總索引

首次設定AWS 區域時，您可以選擇在其中一個建立彙總器索引AWS 資源總管。如需詳細資訊，請參閱 設定和設定資源總管。如果您在初始設定時未執行，則此程序是關於將其中一個本機索引提升為帳戶的彙總索引。

> **Important**
>
> - 您只能有一個彙總索引AWS 帳戶。如果帳戶已有彙總索引，您必須先將其降級為本機索引或刪除。
> - 刪除或變更包含彙總器索引的地區之後，您必須等待 24 小時，才能將另一個索引提升為彙總器索引。

AWS Management Console

將本機索引提升為帳戶的彙總索引

1. 開啟 [資源總管設定] 頁面。
2. 在 [索引] 區段中，選取您要升級之索引旁的核取方塊，然後選擇 [變更索引類型]。
3. 在 [變更 < 區域名稱 > 的索引類型] 對話方塊中，選擇 [彙總索引]，然後選擇 [儲存變更]。

AWS CLI

將本機索引提升為帳戶的彙總索引

下列範例命令會將指定AWS 區域的索引 in type 更新LOCAL為類型AGGREGATOR。您必須從要包含彙總器索引的作業呼叫作業。AWS 區域

```
$ aws resource-explorer-2 update-index-type \
    --arn arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111 \
    --type AGGREGATOR \
    --region us-east-1
{
    "Arn":"arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "LastUpdatedAt":"2022-07-13T18:41:58.799Z",
    "State":"UPDATING",
```

```
    "Type":"AGGREGATOR"
}
```

作業會以非同步方式運作，並從State設定為開始UPDATING。若要檢查作業是否已完成，您可以執行下列命令，並在State回應欄位ACTIVE中尋找值。您必須在 [包含要檢查的索引的區域] 中執行此命令。

```
$ aws resource-explorer-2 get-index --region us-east-1
{
    "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "CreatedAt": "2022-10-12T21:31:37.277000+00:00",
    "LastUpdatedAt": "2022-10-12T21:31:37.677000+00:00",
    "ReplicatingFrom": [
        "us-west-2",
        "us-east-2",
        "us-west-1"
    ],
    "State": "ACTIVE",
    "Tags": {},
    "Type": "AGGREGATOR"
}
```

將彙總索引降級為本機索引

您可以將彙總索引降級為本機索引，例如當您想要將彙總索引移至其他索引時。AWS 區域

當您將彙總器索引降級為本機索引時，資源總管會停止從其他索引複寫索引。AWS 區域它也會啟動非同步背景工作，從其他區域刪除任何複製的資訊。在非同步工作完成之前，某些跨區域結果可能會繼續出現在搜尋結果中。

備註

- 降級彙總器索引之後，您必須等待 24 小時，才能提升不同區域中的相同索引或索引，使其成為帳戶的新彙總索引。
- 降級彙總索引之後，背景程序最多可能需要 36 小時才能完成，而且來自其他區域的所有資源資訊會從此區域執行的搜尋結果中消失。
- 如果您在整個組織檢視中降級成員帳號，該成員可能會從多帳號搜尋中移除。

您可以檢視「設定」頁面上的索引清單或使用作業，來檢查背景工GetIndex作的狀態。非同步工作完成時，索引中的Status欄位會從變更UPDATING為ACTIVE。當時，只有來自本地區域的結果才會顯示在查詢結果中。

AWS Management Console

將彙總索引降級為本機索引

1. 開啟 [資源總管設定] 頁面。
2. 在 [索引] 區段中，選取包含您要降級為區域索引之彙總器索引的 [區域] 旁邊的核取方塊，然後選擇 [變更索引類型]。
3. 在 [變更 < 區域名稱 > 的索引類型] 對話方塊中，選擇 [區域索引]，然後選擇 [儲存變更]。

AWS CLI

將彙總索引降級為本機索引

下列範例會將指定的彙總器索引降階為本機索引。您必須呼叫目前包含彙總器索引的作業。AWS 區域

```
$ aws resource-explorer-2 update-index-type \
    --arn arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111 \
    --type LOCAL \
    --region us-east-1
{
    "Arn":"arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "LastUpdatedAt":"2022-07-13T18:41:58.799Z",
    "State":"UPDATING",
    "Type":"LOCAL"
}
```

作業會以非同步方式運作，並從State設定為開UPDATING始。若要檢查作業是否已完成，您可以執行下列命令，並在State回應欄位ACTIVE中尋找值。您必須在 [包含要檢查的索引的區域] 中執行此命令。

```
$ aws resource-explorer-2 get-index --region us-east-1
{
    "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
```

```
    "CreatedAt": "2022-10-12T21:31:37.277000+00:00",
    "LastUpdatedAt": "2022-10-12T21:31:37.677000+00:00",
    "ReplicatingFrom": [
        "us-west-2",
        "us-east-2",
        "us-west-1"
    ],
    "State": "ACTIVE",
    "Tags": {},
    "Type": "LOCAL"
}
```

支援統一搜尋AWS Management Console

在每AWS Management Console個控制台頁面的頂部都有一個搜索欄。這為所有人提供了統一的搜索體驗AWS 服務。統一的搜索結果可以包括以下內容：

- AWS 服務和功能控制台頁面。
- AWS文檔頁面。
- AWS部落格與知識庫文章
- 如果您依照下列步驟操作，請依照您的帳戶進行。

若要在整合搜尋結果中查看帳戶的資源，您必須執行下列步驟。您可以在初始設定期間執行此操作AWS 資源總管。如果您使用 [快速設定] 選項，這一切都會自動發生。

- 您必須在一個中建立彙總器AWS 區域索引AWS 帳戶。
- 您必須在包含彙總索引AWS 區域的中建立預設檢視。
- 您必須授與所有需要在統一搜尋列中搜尋資源的主參與者使用該預設檢視進行搜尋的權限。

統一搜尋一律會使用包含彙總器索引AWS 區域的預設檢視來執行所有搜尋。

帳號動作對資源總管多帳號搜尋的影響

> **Note**
>
> 從多帳戶搜尋結果中移除帳號和資源最多需要 24 小時。

帳號動作對AWS 資源總管多帳號搜尋有下列影響。

資源總管已停用

當您停用某個帳號的資源總管時，只有在您停用該帳號時選取AWS 區域的帳號才會停用該帳號。

您必須在每個已啟用資源總管的區域中個別停用資源總管。

24 小時後，此帳號的資源將不會顯示在搜尋結果中。

不會移除其他資源總管資料和設定。

已從組織中移除成員帳戶

從組織中移除成員帳號時，Resource Explorer 管理員帳號會失去檢視成員帳戶中資源的權限。

如果移除的帳戶是系統管理員或委派的管理員帳戶，也會移除先前由這些帳戶建立的所有多帳戶檢視。

資源總管會繼續在這兩個帳號中執行。

資源搜尋結果不再包含此帳號的資源。

帳戶被暫停

在中暫停帳號時AWS，帳號將失去在資源總管中檢視資源的權限。暫停帳戶的管理員帳戶可以檢視現有資源。

對於組織帳戶，成員帳戶狀態也可以變更為 [帳戶已暫停]。如果帳戶在系統管理員帳戶嘗試啟用帳戶的同時遭到暫停，就會發生這種情況。帳戶已暫停帳戶的系統管理員帳戶無法檢視該帳戶的資源。

否則，暫停狀態不會影響會員帳戶狀態。

90 天後，帳戶會停用或重新啟用。重新啟動帳號後，其資源總管權限會還原。如果成員帳戶狀態為 [帳戶已暫停]，則系統管理員帳戶必須手動啟用帳戶。

帳戶已關閉

關閉AWS帳號時，資源總管會回應關閉，如下所示：

- 資源總管會保留帳號的資源 90 天，從帳號關閉的有效日期算起。在 90 天期限結束時，資源總管會永久刪除該帳號的所有資源。

- 若要保留資源超過 90 天，您可以使用自訂動作搭配 EventBridge 規則，將資源存放在 Amazon S3 儲存貯體中。只要資源總管保留資源，當您重新開啟已關閉的帳號時，資源總管會還原該帳號的資源。
- 如果帳號是資源總管管理員帳號，則會以系統管理員身分移除該帳號，並移除所有成員帳號。如果帳號是成員帳號，則該帳號會取消關聯，並以成員身份從資源總管管理員帳號中移除。
- 如需詳細資訊，請參閱關閉帳戶。

退出帳戶

如果帳戶選擇退出某個區域，您仍然可以在 24 小時內在搜尋結果中看到他們的資源。

24 小時後，此帳號的資源將不會顯示在搜尋結果中。如需詳細資訊，請參閱 退出行為。

在中關閉資源瀏覽器 AWS 區域

當您不再需要搜尋特定資源時AWS 區域，只能在該區域AWS 資源總管中刪除其索引來關閉該地區。執行此操作時，資源總管會停止掃描該區域中的新資源或更新資源。如果您的帳戶包含彙總索引，則會停止從已刪除索引的複寫，且已刪除索引中的資訊會從彙總器索引中移除，並停止出現在搜尋結果中。刪除索引中的所有資源最多可能需要 24 小時才會從具有彙總器索引的區域中的搜尋結果中消失。

> **Note**
>
> 當您註冊第一個時AWS 區域，資源總管會建立名為AWSServiceRoleForResourceExplorer的服務連結角色 (SLR)。AWS 帳戶資源總管不會自動刪除此 SLR。刪除帳戶中每個區域中的資源總管索引後，如果以後不使用資源總管，則可以使用 IAM 主控台刪除 SLR。如果您確實刪除角色，然後選擇在至少一個角色中再次開啟資源總管AWS 區域，則 Resource Explorer 會自動重新建立服務連結的角色。

您可以使用 AWS Command Line Interface (AWS CLI) 中AWS 區域的命令或在 AWS Management Console AWS SDK 中使用 API 作業來關閉中的資源總管。

如果您關閉成員帳號的資源總管，且該成員處於全組織檢視中，則該成員將從多帳號搜尋結果中移除。

如果您不再希望支援在您帳戶中的一或多個資源搜尋，請執行下列程序中的步驟。AWS 區域

> **Note**
>
> 如果您刪除的索引是的彙總索引AWS 帳戶，則必須等待 24 小時，才能將另一個本機索引升級為帳戶的彙總索引。在設定另一個彙總器索引之前，使用者無法使用資源總管執行全帳戶搜尋。

AWS Management Console

若要刪除資源總管索引 AWS 區域

1. 開啟 [資源總管設定] 頁面。
2. 在 [索引] 區段中，選取要刪除之索引旁AWS 區域的核取方塊，然後選擇 [刪除]。
3. 在 [刪除索引] 頁面上，確認您只選取要刪除的索引。**delete**在 [確認] 文字方塊中輸入，然後選擇 [刪除索引]。

   Resource Explorer 會在頁面頂端顯示綠色橫幅以表示成功，如果一或多個選取的區域發生錯誤，則會顯示紅色橫幅。

AWS CLI

若要刪除資源總管索引 AWS 區域

如果您不再希望支援在您帳戶中的一或多個搜尋資源，請執行下列命令。AWS 區域

針對您要刪除之索引的每個區域執行下列命令。您必須使用要刪除的索引在 [區域] 中執行命令。下列範例命令會刪除美國西部 (奧勒岡) (us-west-2) 中的資源總管索引。

```
$ aws resource-explorer-2 delete-index \
    --arn arn:aws:resource-explorer-2:us-
west-2:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd22222222 \
    --region us-west-2
{
    "Arn": "arn:aws:resource-explorer-2:us-
west-2:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd22222222",
    "State": "DELETING"
}
```

由於 Resource Explorer 會在背景中以非同步工作的形式執行部分刪除清除工作，因此回應可能會指出作業為DELETING。此狀態表示背景處理程序尚未完成。您可以執行下列命令，並檢查State要變更為的來檢查最終完成DELETED。

```
$ aws resource-explorer-2 get-index \
    --region us-west-2
{
    "Arn": "arn:aws:resource-explorer-2:us-
west-2:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "CreatedAt": "2022-07-12T18:59:10.503000+00:00",
    "LastUpdatedAt": "2022-07-13T18:41:58.799000+00:00",
    "ReplicatingFrom": [],
    "State": "DELETED",
    "Tags": {},
    "Type": "LOCAL"
}
```

全部關閉資源瀏覽器AWS 區域

AWS 資源總管，。

> **Note**
>
> 當您在第一個帳號 AWSServiceRoleForResourceExplorer 中建立索引時，資源總管會建立在帳號中名AWS 區域為的服務連結角色。資源總管不會自動刪除此服務連結的角色。刪除每個區域中的資源總管索引之後，如果您確定將 future 不會再次使用資源總管，則可以使用 IAM 主控台刪除角色。如果您確實刪除角色，然後選擇在至少一個角色中啟動資源總管AWS 區域，則 Resource Explorer 會重新建立服務連結角色。

全部關閉資源瀏覽器AWS 區域

您可以使用AWS Management Console、使用AWS Command Line Interface (AWS CLI) 中的命令或在AWS SDK 中使用 API 作業來關閉資源總管。

AWS Management Console

如果您不再希望支援在中搜尋任何AWS 區域資源AWS 帳戶，請執行下列程序中的步驟。

若要全部關閉資源總管AWS 區域

1. 開啟 [資源總管設定] 頁面。
2. 在 [索引] 區段中，選取所有已註冊旁的核取方塊AWS 區域，然後選擇 [刪除]。

> **Tip**
>
> 您可以核取「索引」旁邊表格標題列中的核取方塊，以在單一步驟中核取所有區域的核取方塊。

3. 在 [刪除索引] 頁面上，確認您要刪除所有索引。**delete**在 [確認] 文字方塊中輸入，然後選擇 [刪除索引]。

   Resource Explorer 會在頁面頂端顯示綠色橫幅以表示成功，如果一或多個選取的區域發生錯誤，則會顯示紅色橫幅。

AWS CLI

若要全部關閉資源總管AWS 區域

如果您不想再支援搜尋帳戶中的任何AWS 區域資源，請執行下列命令，以尋找先前已開啟「資源總管」之每個AWS 區域索引的 ARN。

```
$ aws resource-explorer-2 list-indexes --query Indexes[*].Arn[
"arn:aws:resource-explorer-2:us-east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
"arn:aws:resource-explorer-2:us-west-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd22222222",
"arn:aws:resource-explorer-2:us-west-2:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd33333333"
]
```

針對每個回應，執行下列命令以刪除該區域中的資源總管索引。

```
$ aws resource-explorer-2 delete-index \
    --arn arn:aws:resource-explorer-2:us-east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111 \
    --region us-east-1
{
    "Arn": "arn:aws:resource-explorer-2:us-east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
```

```
    "State": "DELETING"
}
```

在每個其他「區域」中重複上一個指令。

由於資源總管在背景中以非同步工作的形式執行部分清理，因此回應可能會指出作業為DELETING。此狀態表示背景處理程序尚未完成。您可以執行下列命令，並檢查要變更為的狀態，以檢查最終完成DELETED。

```
$ aws resource-explorer-2 get-index \
    --region us-east-1
{
    "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "CreatedAt": "2022-07-12T18:59:10.503000+00:00",
    "LastUpdatedAt": "2022-07-13T18:41:58.799000+00:00",
    "ReplicatingFrom": [],
    "State": "DELETED",
    "Tags": {},
    "Type": "LOCAL"
}
```

將資源總管部署到組織中的帳號

透過使用 AWS CloudFormation StackSets，您可以定義並部署至組織中管理的所有帳戶AWS Organizations。當您定義堆疊集時，您可以指定您要在所指定的所有目標帳戶AWS 區域和跨越所有目標帳戶建立的AWS資源。當所有帳戶都屬於同一組織時，您可以利用與組 Organizations AWS CloudFormation 整合的優勢，並讓這些服務處理跨帳戶角色的建立。您可以在組織中啟用自動部署，這會自動將堆疊執行個體部署到 future 可能新增至目標組織或組織單位 (OU) 的新帳戶。如果您從組織中移除帳號，則AWS CloudFormation會自動刪除任何部署為組織堆疊執行個體一部分的資源。若要取得有關的更多資訊 StackSets，請參閱使用指南AWS CloudFormation StackSets中的〈AWS CloudFormation使用〉。

您可AWS CloudFormation StackSets 以使用在組織中的所有帳戶AWS 資源總管中開啟和設定、在每個已啟用的區域中建立索引，以及在需要的位置建立檢視表。

> **Important**
>
> 如果您嘗試在區域中設定彙總器索引，則必須確定該帳戶在任何其他區域中都沒有現有的彙總器索引。將彙總器索引降級為本機索引之後，您必須等待 24 小時，才能將另一個索引升級為帳戶的新彙總索引。

先決條件

若要用AWS CloudFormation StackSets 來將 Resource Explorer 部署到組織中的帳號，您或組織的管理員必須先執行下列步驟，才能啟用具有服務管理權限的堆疊：

1. 組織必須啟用所有功能。如果組織僅啟用合併帳單功能，您就無法建立具有服務管理權限的堆疊集。
2. 開啟AWS CloudFormation和 Organizations 之間的信任存取。這會AWS CloudFormation授與建立組織管理帳戶中所需角色的權限，且成員帳號AWS CloudFormation將部署 Resource Explorer 索引和檢視。

現在您可以建立具有服務管理權限的堆疊集。

> **Important**
>
> 您必須在組織的管理帳戶中建立堆疊集。 AWS CloudFormation是一項地區服務，因此您只能從原先建立的區域中檢視和管理您建立的堆疊集。

建立資源總管的堆疊集

完全部署資源總管，您必須部署兩個堆疊集。

- 第一個堆疊集會建立彙總器索引和預設檢視，讓使用者搜尋帳戶中所有區域的資源。

  只將此堆疊集部署到您要在其中建立彙總索引的單一區域。
- 第二個堆棧集創建一個本地索引和默認視圖。本機索引會將其內容複寫至彙總索引。

  將此堆疊集部署到帳戶中每個已啟用的區域 (包含彙總器索引的區域除外)。請勿選擇您部署堆疊的帳戶中未啟用的任何區域。如果這樣做，部署就會失敗。

下一節介紹了每個範本的範例。如需如何使用這些範本建立堆疊集的指 step-by-step示，請參閱使用指南中的建立具有服務管理權限的AWS CloudFormation堆疊集。

將這些堆疊集部署到您的組織之後，您所選範圍內的每個帳戶 (組織或組織單位) 都會在指定的區域中具有彙總索引，而且每個其他區域都有本機索引。

AWS CloudFormation範例範本

下列範例範本會建立帳戶的彙總索引和預設檢視，以便在您部署索引的帳戶中，跨所有區域搜尋資源。

YAML

```
Description: >-
  CFN Stack setting up ResourceExplorer with an Aggregator Index, and a new Default
 View.
Resources:
  Index:
    Type: 'AWS::ResourceExplorer2::Index'
    Properties:
      Type: AGGREGATOR
      Tags:
        Purpose: ResourceExplorer CFN Stack
  View:
    Type: 'AWS::ResourceExplorer2::View'
    Properties:
      ViewName: DefaultView
      IncludedProperties:
        - Name: tags
      Tags:
        Purpose: ResourceExplorer CFN Stack
    DependsOn: Index
  DefaultViewAssociation:
    Type: 'AWS::ResourceExplorer2::DefaultViewAssociation'
    Properties:
      ViewArn: !Ref View
```

JSON

```
{
    "Description": "CFN Stack setting up ResourceExplorer with an Aggregator Index,
 and a new Default View.",
    "Resources": {
```

```
        "Index": {
            "Type": "AWS::ResourceExplorer2::Index",
            "Properties": {
                "Type": "AGGREGATOR",
                "Tags": {
                    "Purpose": "ResourceExplorer CFN Stack"
                }
            }
        },
        "View": {
            "Type": "AWS::ResourceExplorer2::View",
            "Properties": {
                "ViewName": "DefaultView",
                "IncludedProperties": [{
                    "Name": "tags"
                }],
                "Tags": {
                    "Purpose": "ResourceExplorer CFN Stack"
                }
            },
            "DependsOn": "Index"
        },
        "DefaultViewAssociation": {
            "Type": "AWS::ResourceExplorer2::DefaultViewAssociation",
            "Properties": {
                "ViewArn": {
                    "Ref": "View"
                }
            }
        }
    }
}
```

下列範例範本會在除彙總器索引以外的所有帳戶中，在每個已啟用的區域中建立本機索引。它也會建立預設檢視，讓使用者只能搜尋該區域中的資源。使用者必須在彙總器「區域」中使用檢視進行搜尋，才能在所有區域中搜尋資源。

YAML

```
Description: >-
  CFN Stack setting up ResourceExplorer with a Local Index, and a new Default View.
Resources:
```

```
  Index:
    Type: 'AWS::ResourceExplorer2::Index'
    Properties:
      Type: LOCAL
      Tags:
        Purpose: ResourceExplorer CFN Stack
  View:
    Type: 'AWS::ResourceExplorer2::View'
    Properties:
      ViewName: DefaultView
      IncludedProperties:
        - Name: tags
      Tags:
        Purpose: ResourceExplorer CFN Stack
    DependsOn: Index
  DefaultViewAssociation:
    Type: 'AWS::ResourceExplorer2::DefaultViewAssociation'
    Properties:
      ViewArn: !Ref View
```

JSON

```
{
    "Description": "CFN Stack setting up ResourceExplorer with a Local Index, and a
 new Default View.",
    "Resources": {
        "Index": {
            "Type": "AWS::ResourceExplorer2::Index",
            "Properties": {
                "Type": "LOCAL",
                "Tags": {
                    "Purpose": "ResourceExplorer CFN Stack"
                }
            }
        },
        "View": {
            "Type": "AWS::ResourceExplorer2::View",
            "Properties": {
                "ViewName": "DefaultView",
                "IncludedProperties": [{
                    "Name": "tags"
                }],
                "Tags": {
```

```
                    "Purpose": "ResourceExplorer CFN Stack"
                }
            },
            "DependsOn": "Index"
        },
        "DefaultViewAssociation": {
            "Type": "AWS::ResourceExplorer2::DefaultViewAssociation",
            "Properties": {
                "ViewArn": {
                    "Ref": "View"
                }
            }
        }
    }
}
```

管理資源總管檢視以提供搜尋存取權

檢視是搜尋資源的關鍵。每個AWS 資源總管搜索操作都必須使用一個視圖。

檢視是系統管理員可用來控制您的資源相關資訊存取的方法AWS 帳戶。

只有具有使用該檢視權限的主體 (IAM 角色或使用者) 才能存取檢視。若要使用資源總管成功搜尋，主參與Allow者必須擁有檢視 ARN 上resource-explorer-2:GetView與resource-explorer-2:Search作業的存取權。

檢視包含內建篩選器，管理員可以使用這些篩選器將結果限制為只有感興趣的項目。例如，您可以建立僅包含與特定專案相關資源的檢視表。不需要查看其他專案相關資訊的使用者可以使用此檢視來僅查看感興趣的資源。

檢視表是區域資源。該視圖被創建並存儲在一個特定的，AWS 區域並在其結果中返回僅來自該地區索引的信息。若要在帳戶中包含來自所有區域的結果，檢視表必須位於包含彙總器索引的「區域」中。該區域包含帳戶中所有其他區域的索引複本。

如需有關建立和使用檢視的詳細資訊，請參閱下列主題。

主題

- 關於資源總管
- 建立用於搜尋的資源總管檢視
- 授與資源總管檢視的存取權以進行搜尋
- 在中設定預設檢視AWS 區域
- 對檢視新增標籤
- 共用資源瀏覽器檢視
- 在資源總管中刪除視圖

關於資源總管

AWS 資源總管在後台索引您的資源，然後使該索引可供您查詢。您可以使用本指南中說明的資源總管 API 或使用資源總管主控台執行資源搜尋查詢。資源瀏覽器使用其 API 來提供交互式圖形界面，否則只能以編程方式訪問的 API。本主題中描述的概念同時適用於 API 和主控台。

視圖存儲在，AWS 區域並返回僅從該地區的索引的結果。

由於管理員可能想要限制對資源索引中包含的資訊的存取，因此無法直接存取索引本身。相反地，所有搜尋都必須經過使用者必須具有搜尋權限的檢視。

每個視圖都有幾個關鍵元素：

許可

您可以使用標準AWS權限原則來控制可以使用每個檢視的使用者。這是由附加到主參與者的基於身份的權限原則提供，這些原則可讓您精細控制誰可以查看每個檢視所提供的資訊。例如，您可以授與Production-resources檢視的存取權，以便僅允許操作您生產服務的工程師進行搜尋。然後，您可以授予Pre-production-resources檢視的不同權限，以允許開發人員搜尋生產前資源。

如果您使用以主參AWSResourceExplorerReadOnlyAccess與者命名的AWS受管理策略，它會授與他們使用帳戶中的任何檢視進行搜尋的能力。

或者，您可以建立自己的許可

- resource-explorer-2:GetView
- resource-explorer-2:Search

若要提供存取權，請新增許可到您的使用者、群組或角色：

- AWS IAM Identity Center 中的使用者和群組：

  建立許可集合。請遵循《AWS IAM Identity Center 使用者指南》的建立許可集合中的指示。
- 透過身分提供者在 IAM 中管理的使用者：

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

如許可授與資源總管檢視的存取權以進行搜尋

篩選搜尋

視圖作為一個虛擬窗口，通過該窗口，用戶可以看到帳戶中的資源。您可以建立多個檢視，每個檢視都會呈現大圖的不同檢視。例如，您可以建立一個檢視，僅允許搜尋與生產前環境相關聯的資

源，如附加至資源的標籤所識別。然後，您可以創建一個單獨的視圖，允許根據標籤中的不同值僅搜索生產環境中的資源。如果您使用不同的FilterString值設定多個檢視表，則不必每次搜尋時重新輸入這些查詢參數。

檢視也可以指定要包含在結果中的資源相關的選擇性資訊。默認字段列表始終包括在結果中。除了預設清單之外，您還可以要求檢視表也包含附加至資源的任何盤點單。

搜尋範圍

- 區域範圍 — 當您在 [資源總管] 中進行搜尋時，結果只能包含在該區域中編製索引的資源。AWS 區域大多數區域中的索引都會加上標籤，LOCAL因為它只包含該區域內的資源相關資訊。這些區域中的搜尋只能傳回這些資源。
- 帳戶範圍 — 您可以將一個本機索引升級為帳戶的彙總索引。當您執行此操作時，開啟「資源總管」的所有其他區域會將其索引資訊複寫到具有彙總器索引的「區域」。如果您在該區域中進行搜尋，則這些結果會包含帳戶中所有區域的資源。當您使用 [快速設定] 選項來設定伺服器時，資源總管會自動在您指定的 [區域] 中建立彙總器索引。此外，「快速設定」選項會在該區域中建立預設檢視表，以支援跨所有區域搜尋帳戶中的所有資源。

預設視圖

如果使用者嘗試在未明確指定檢視的情況下進行搜尋，Resource Explorer 會使用為該檢視定義的預設檢視AWS 區域。

如果該區域的預設檢視表不存在，且使用者未指定要使用的檢視表，則搜尋會失敗並產生例外狀況。

資源總管會自動建立預設檢視，如下所示：

- 如果您使用AWS Management Console並選擇 [快速設定] 選項來開啟 [資源總管]，則必須指定哪個區域包含帳戶的彙總器索引。資源總管會在指定的聚合器索引區域中自動創建默認視圖。
- 如果您使用註冊資源總管，AWS Management Console並選擇 [進階設定] 選項，您可以選擇性地選擇為指定區域中的帳號建立彙總器索引。如果您這麼做，資源總管會在彙總器索引區域中自動建立預設檢視。
- 如果您使用主控台註冊資源總管，並選擇不註冊彙總器索引區域，則 Resource Explorer 會為每個區域中的本機索引建立預設檢視。
- 如果您使用AWS CLI或 API 作業註冊資源總管，資源總管不會自動建立預設檢視。相反地，您必須針對預期使用者搜尋的每個「區域」手動設定預設檢視。

建立用於搜尋的資源總管檢視

所有搜尋都必須使用檢視。檢視會定義篩選器，以決定使用檢視的查詢可傳回哪些資源。檢視也會控制誰可以搜尋資源。

檢視會儲存在 AWS 區域，而且只會傳回該 Region 索引的搜尋結果。如果「地區」包含彙總器索引，則檢視會傳回帳戶中每個「區域」中索引的搜尋結果。

多帳戶檢視可讓您搜尋整個組織帳號中的資源。您希望搜索的任何帳戶都需要索引。只有管理帳戶或組織的委派管理員可以建立多帳戶檢視。

AWS 資源總管 如果您在 Systems Manager 主控台的資源總管的快速設定或進階設定中選擇相關選項，則可在初始設定期間為您建立預設檢視。稍後，您可以為不同的使用者集建立具有不同篩選器的其他檢視。

您可以使用或在 AWS SDK 中執行 AWS CLI 命令 AWS Management Console 或其等效 API 作業來建立檢視表。

最低許可

若要執行此程序，您必須具備下列權限：

- 動作：`resource-explorer-2:CreateView`

  資源：這可以是*允許在帳戶中的任何視圖 AWS 區域 中創建視圖。

AWS Management Console

建立視圖的步驟

1. 開啟 [資源總管] 主控台 [檢視] 頁面，然後選擇 [建立
2. 在「建立檢視表」頁面上，為「名稱」輸入檢視表的名稱。

   名稱長度不得超過 64 個字元，且可包含字母、數字和連字號 (-) 字元。名稱在其中必須是唯一的 AWS 區域。
3. 選擇您要 AWS 區域 在其中建立視圖的。若要建立從帳戶中所有區域傳回資源的檢視，請選擇包 AWS 區域 含彙總器索引的檢視。
4. (選擇性) 在「範圍」中，選擇搜尋傳回多帳戶資源，還是僅傳回您帳戶的資源。帳戶層級範圍是預設值。

只有管理帳戶或委派管理員才能看到建立多帳戶檢視的選項。

5. 選擇是否篩選結果。

   - 包含所有資源

     不包括任何查詢篩選器。與檢視相關聯的索引中的所有資源都可以在搜尋結果中傳回。

   - 僅包含符合指定篩選條件的資源

     打開 [資源篩選器] 核取方塊，您可以在其中選擇篩選名稱和運算子。如需每個可用篩選器名稱和運算子的說明，請參閱篩選條件。

   - 選擇要包含在此檢視結果中的選擇性資源屬性。選取「標籤」旁邊的核取方塊，可讓使用者根據其標籤鍵名稱和值搜尋資源。如果您未在檢視中包含標籤，則使用者無法提出使用標籤鍵和值的搜尋請求來進一步篩選結果。
   - 或者，您可以將標籤貼附至視圖。展開「標籤」方塊，最多可輸入 50 個標籤鍵/值組。您可以使用標籤來分類資源，或做為以屬性為基礎的存取控制 (ABAC) 安全性權限策略的一部分。如需詳細資訊，請參閱 對檢視新增標籤。
   - 選擇「建立視圖」。

   主控台會返回「搜尋」頁面，您可以在此頁面使用新的檢視來執行搜尋。

   下一步：授與您帳戶中的主體使用新檢視進行搜尋的權限。如需更多資訊，請參閱 授與資源總管檢視的存取權以進行搜尋

AWS CLI

建立視圖的步驟

執行下列命令，以在指定的中建立檢視表 AWS 區域。下列範例會建立一個檢視，該檢視僅傳回與使用`Stage`金鑰和值標記的 Amazon EC2 服務相關資源`prod`。

```
$ aws resource-explorer-2 create-view \
    --region us-west-2 \
    --view-name "My-EC2-Prod-Resources" \
    --filters FilterString="service:ec2 tag:stage=prod" \
    --included-properties Name=tags
{
    "View": {
        "Filters": {
```

```
            "FilterString": "service:ec2 tag:stage=prod"
        },
        "IncludedProperties": [
            {
                "Name": "tags"
            }
        ],
        "LastUpdatedAt": "2022-08-03T16:13:37.625000+00:00",
        "Owner": "123456789012",
        "Scope": "arn:aws:iam::123456789012:root",
        "ViewArn": "arn:aws:resource-explorer-2:us-west-2:123456789012:view/My-EC2-
Prod-Resources/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
    }
}
```

若要建立組織層次檢視表

下列範例會建立可從整個組織傳回資源的檢視表。這必須由組織的管理帳戶或委派的管理員帳戶執行。

1. 執行命aws organizations describe-organization令以取得您的組織 ARN。
2. 執行下列命令以建立指定組織的檢視表。

```
$ aws resource-explorer-2 create-view \
    --region us-west-2 \
    --view-name entire-org-view \
    --scope "arn:aws:organizations::111111111111:organization/o-exampleorgid"
{
    "View": {
        "Filters": {
            "FilterString": ""
        },
        "IncludedProperties": [],
        "LastUpdatedAt": "2022-08-03T16:13:37.625000+00:00",
        "Owner": "111111111111",
        "Scope": "arn:aws:organizations::111111111111:organization/o-
exampleorgid",
        "ViewArn": "arn:aws:resource-explorer-2:us-west-2:111111111111:view/
entire-org-view/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
    }
}
```

若要建立組織單位層級檢視

下列範例會建立一個檢視，該檢視會傳回此組織單位所有成員的資源。此檢視的行為與組織層級檢視類似。這必須由組織的管理帳戶或委派的管理員帳戶執行。

1. 執行命`aws organizations describe-organizational-unit`令以取得您的組織 ARN。
2. 執行下列命令，為指定的組織單位建立檢視表。

```
$ aws resource-explorer-2 create-view \
    --region us-west-2 \
    --view-name entire-ou-view \
    --scope "arn:aws:organizations::222222222222:ou/o-exampleorgid/ou-
exampleouid"
{
    "View": {
        "Filters": {
            "FilterString": ""
        },
        "IncludedProperties": [],
        "LastUpdatedAt": "2022-08-03T16:13:37.625000+00:00",
        "Owner": "222222222222",
        "Scope": "arn:aws:organizations::222222222222:ou/o-exampleorgid/ou-
exampleouid",
        "ViewArn": "arn:aws:resource-explorer-2:us-west-2:222222222222:view/
entire-ou-view/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
    }
}
```

下一步：授與您帳戶中的主體使用新檢視進行搜尋的權限。如需詳細資訊，請參閱 授與資源總管檢視的存取權以進行搜尋

授與資源總管檢視的存取權以進行搜尋

您必須須須須須須須須須須須須須須須須須須須須須須須須須須須須須須須AWS 資源總管 若要這麼做，請對需要使用檢視進行搜尋的AWS Identity and Access Management (IAM) 主體使用以身分識別為基礎的權限原則。

若要提供存取權，請新增許可到您的使用者、群組或角色：

- AWS IAM Identity Center 中的使用者和群組：

  建立許可集合。請遵循《AWS IAM Identity Center 使用者指南》的建立許可集合中的指示。

- 透過身分提供者在 IAM 中管理的使用者：

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

- IAM 使用者：
  - 建立您的使用者可擔任的角色。請遵循《IAM 使用者指南》的為 IAM 使用者建立角色中的指示。
  - (不建議) 將政策直接連接至使用者，或將使用者新增至使用者群組。請遵循《IAM 使用者指南》的新增許可到使用者 (主控台)中的指示。

您可以使用下列任一方法：

- 使用現有的AWS受管理策略。資源總管提供數個預先定義的AWS受管理策略供您使用。如需所有可用AWS受管理策略的詳細資訊，請參閱AWS 資源總管 的 AWS 受管政策。

  例如，您可以使用`AWSResourceExplorerReadOnlyAccess`策略將搜尋權限授與帳戶中的所有檢視。

- 建立您自己的權限原則，並將其指派給主參與者。如果您建立自己的政策，可以透過在政策陳述式的`Resource`元素中指定每個檢視的 Amazon 資源名稱 (ARN)，以限制對單一檢視或可用檢視子集的存取。例如，您可以使用下列範例原則，授與該主參與者僅使用該檢視進行搜尋的能力。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "resource-explorer-2:Search",
                "resource-explorer-2:GetView"
            ],
            "Resource": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/
MyTestView/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111
        }
    ]
}
```

使用 IAM 主控台建立權限政策，並將其與需要這些權限的主體搭配使用。如需有關 IAM 許可的詳細資訊，請參閱下列主題：

- IAM 中的政策和許可
- 新增和移除 IAM 身分許可
- 了解政策授予的許可

使用基於標籤的授權來控制對視圖的存取權

如果您選擇使用僅傳回特定資源結果的篩選器來建立多個檢視表，則您可能還想要將這些檢視的存取限制為只有需要查看這些資源的主參與者。您可以使用以屬性為基礎的存取控制 (ABAC) 策略，為帳戶中的檢視提供這種類型的安全性。ABAC 使用的屬性是附加到試圖在其中執行作業的主參與者AWS和他們嘗試存取的資源的標籤。

ABAC 使用附加到主體的標準 IAM 許可政策。只有當附加到請求主參與者的標籤和附加到受影響資源的標籤都符合策略中的需求時，策略才會使用策略陳述式中的Condition元素來允許存取。

例如，您可以在支援公司生產應用程式的所有AWS資源上附加標籤"Environment" = "Production"。若要確保只有獲得授權可存取生產環境的主參與者才能看到這些資源，請建立使用該標籤作為篩選器的 Resource Explorer 檢視。然後，若要將檢視的存取限制為只有適當的主參與者，您可以使用條件類似下列範例元素的原則來授與權限。

```
{
    "Effect": "Allow",
    "Action": [ "service:Action1", "service:Action2" ],
    "Resource": "arn:aws:arn-of-a-resource",
    "Condition": { "StringEquals": {"aws:ResourceTag/Environment":
 "${aws:PrincipalTag/Environment}"} }
}
```

Condition在前面的範例中，指定只有當附加至發出請求之主參與者的Environment標籤符合附加至請求中指定之資源的Environment標籤時，才允許此請求。如果這兩個標籤不完全匹配，或者缺少任何一個標籤，則資源總管拒絕該請求。

> **Important**
>
> 若要成功使用 ABAC 來保護對資源的存取，您必須先限制對新增或修改附加至主參與者和資源之標籤的能力的存取。如果使用者可以新增或修改附加AWS主參與者或資源的標籤，則該使用

者可以影響這些標籤所控制的權限。在安全的 ABAC 環境中，只有核准的安全性管理員有權新增或修改附加至主體的標籤，而且只有安全性管理員和資源擁有者可以新增或修改附加至資源的標籤。

如需如需如需如需如需如需如需如需如需如需如需如需如需如需有關如需如需如需如需如需如需如需如需如需如

- IAM 教學課程：根據標籤定義存取AWS權限
- 使用標籤控制對AWS資源的存取權

在您有必要的 ABAC 基礎結構之後，您可以使用 [開始使用標記] 控制誰可以使用您帳戶中的 [資源總管] 檢視進行搜尋。如需說明此原則的政策，請參閱下列範例：

- 根據標籤授予檢視的存取權
- 授予根據標籤建立檢視的存取權

在中設定預設檢視AWS 區域

在中AWS 資源總管，您可以在中定義許多檢視AWS 區域，其中每個檢視都會滿足不同的搜尋需求。建議您在每個「區域」中設定一個檢視作為該「區域」的預設檢視。

每當使用者執行搜尋且未明確指定要使用的檢視時，Resource Explorer 就會使用預設檢視。 每個AWS Management Console頁面頂端的統一搜尋列也會自動使用 [地區] 中包含彙總器索引的預設檢視，以尋找符合使用者搜尋查詢的資源。

您只能選取「區域」中存在的檢視作為該「區域」的預設檢視表。如果另一個「區域」具有您要使用的視圖，則必須先在「區域」中建立該視圖的副本，以使其成為預設檢視。

> **Tip**
>
> 沒有複製視圖操作。您必須在目標「區域」中建立視圖，然後將設定從既有視圖複製到新視圖。

您可以使用或在AWS SDK 中執行AWS CLI命令AWS Management Console或等效 API 作業，將檢視表指定為「地區」的預設值。

AWS Management Console

設定預設檢視的步驟

1. 在 [資源總管檢視] 頁面上，選擇要設為 [區域] 預設值的檢視旁邊的選項按鈕。
2. 選擇「動作」，然後選擇「設為預設值」。

AWS CLI

設定預設檢視的步驟

執行下列命令，將指定的檢視設定為 [Region]。下列範例會將指定的檢視設定為在 us-east-1 區域中執行的所有搜尋的預設檢視。該檢視表必須存在於您執行命令的「區域」中。

```
$ aws resource-explorer-2 associate-default-view \
    --region us-east-1 \
    --view-arn arn:aws:resource-explorer-2:us-east-1:123456789012:view/
MyViewName/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111
{
    "ViewArn": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/
MyViewName/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
}
```

對檢視新增標籤

您可以對檢視新增標籤來對其進行分類。標籤是客戶提供的中繼資料，採用金鑰名稱字串和相關選用值字串的形式。有關標記AWS資源的一般AWS資訊，請參閱在 Amazon Web Services 一般參考.

對檢視新增標籤

您可以使用或在AWS SDK 中執行AWS CLI命令AWS Management Console或等效 API 作業，將標籤新增至 [資源總管] 檢視。

AWS Management Console

對視圖新增標籤

1. 開啟 [資源總管檢視] 頁面，並選擇要標記以顯示其 [詳細資料] 頁面的檢視名稱。
2. 在 Tags (標籤) 下，選擇 Manage tags (管理標籤)。

3. 若要新增標記，請選擇「新增標籤」，然後輸入標籤鍵名稱和選用值。

> **Note**
>
> 您也可以選擇標籤旁邊的 X 來刪除標籤。

您可以在資源中連接最多 50 個使用者定義的標籤。任何由自動建立和管理的標籤都AWS不會計入此配額。

4. 完成所有標籤變更後，請選擇 [儲存變更]。

AWS CLI

對視圖新增標籤

執行以下命令，對檢視新增標籤。下列範例會將含有索引鍵名稱`environment`和值的標籤新增`production`至指定檢視。

```
$ aws resource-explorer-2 tag-resource \
    --resource-id arn:aws:resource-explorer-2:us-east-1:123456789012:view/
MyViewName/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111 \
    --tags environment=production
```

上述命令如果成功就不會產生輸出。

> **Note**
>
> 若要從視圖中移除既有標籤，請使用`untag-resource`指令。

使用標籤控制權限

標籤的關鍵用途是支援屬性型存取控制 (ABAC) 的標籤策略。ABAC 可讓您標記資源，協助簡化權限管理。然後，您將權限授予使用者以特定方式標記的資源。

例如，考量這項情境。對於稱為的視圖`ViewA`，您可以貼附標籤`environment=prod` (鍵名稱 = 值)。另一個`ViewB`可能會被標記`environment=beta`。您可以根據每個角色或使用者應該能夠存取的環境，使用相同的標籤和值來標記角色和使用者。

然後，您可以為 IAM 角色、群組和使用者指派AWS Identity and Access Management (IAM) 許可政策。只有當發出搜尋請求的角色或使用者具有與檢視附加的標籤值相同的environment標籤時，原則才會授與使用檢視存取environment和搜尋的權限。

這種方法的好處是它是動態的，不需要您維護誰可以訪問哪些資源的列表。而是確保所有資源 (您的檢視) 和主體 (IAM 角色和使用者) 都已正確標記。然後，權限會自動更新，而您不必變更任何原則。

在 ABAC 政策中引用標籤

標記檢視之後，您可以選擇使用這些標記來動態控制對這些檢視的存取。下列範例政策假設您的 IAM 主體和檢視都使用標籤金鑰environment和某些值標記。完成時，您可以下範例政策至您的主參與者。然後，您的角色和使用者可以Search使用environment標籤值標記的任何檢視，這些檢視與附加至主參與者的environment標籤完全相符。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "resource-explorer-2:GetView",
                "resource-explorer-2:Search"
            ],
            "Resource": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:ResourceTag/environment": "${aws:PrincipalTag/environment}"
                }
            }
        }
    ]
}
```

如果主參與者和檢視都有標environment籤，但值不相符，或者如果其中一個缺少environment標籤，則 Resource Explorer 會拒絕搜尋要求。

如需使用 ABAC 安全地授予資源存取權的詳細資訊，請參閱 ABAC 的用途為何AWS？

共用資源瀏覽器檢視

中的檢視AWS 資源總管主要使用以資源為基礎的政策來授與存取權 與 Amazon S3 儲存貯體政策類似，這些政策會附加到檢視，並指定誰可以使用該檢視。這與 AWS Identity and Access Management (IAM) 身分型政策形成鮮明對比。IAM 身分型政策會指派給角色、群組或使用者，並指定角色、群組或使用者可存取的動作和資源。您可以將任一類型的原則與資源總管檢視搭配使用，如下所示：

- 在擁有資源的管理帳戶或委派管理員帳戶中，只要沒有其他原則明確拒絕存取該主體的檢視，就可以使用其中一種原則類型來授與存取權。
- 跨帳戶，您必須同時使用這兩種策略類型。附加至共用帳戶中檢視的以資源為基礎的政策會開啟與另一個消費帳戶共用。不過，該原則不會將存取權授與個別使用者或使用帳戶中的角色。消費帳戶中的系統管理員還必須將以身分識別為基礎的策略指派給消費帳戶中所需的角色和使用者。該政策授予對檢視之 Amazon 資源名稱 (ARN) 的存取權。

若要與其他帳戶共用檢視表，您必須使用 AWS Resource Access Manager (AWS RAM)。 AWS RAM為您處理以資源為基礎的政策的複雜性。您必須先依照下列步驟開啟多帳戶搜尋，才能分享。

若要共用檢視，您必須是組織的管理帳戶或委派的管理員。您可以指定要與其共用資源的帳號或身分識別。 AWS RAM完全支持資源瀏覽器視圖。 AWS RAM根據您選擇與之共用的主參與者類型，使用與下列各節中所述相似的原則。如需有關如何共用資源的指示，請參閱AWS Resource Access Manager使用指南中的「共用AWS資源」。

系統管理員和委派的系統管理員可以建立和共用 3 種檢視類型：組織範圍檢視、組織單位 (OU) 範圍檢視，以及帳戶層級範圍檢視。他們可以與組織、OU 或帳戶共用。當帳戶加入或離開組織時，AWS RAM會自動授予或撤銷共用檢視。

與之共用檢視的權限原則 AWS 帳戶

下列範例原則顯示如何讓檢視可供兩種不同AWS 帳戶的主參與者使用：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": [ "111122223333", "444455556666" ]
            },
            "Action": [
                "resource-explorer-2:Search",
```

```
                "resource-explorer-2:GetView",
            ],
            "Resource": "arn:aws:resource-explorer-2:us-
east-1:123456789012:view/policy-name/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
            "Condition": {"StringEquals": {"aws:PrincipalOrgID": "o-123456789012"},
                "StringNotEquals": {"aws:PrincipalAccount": "123456789012"}
            }
        }
    ]
    }"
}
```

現在，每個指定帳戶中的管理員都必須透過將以身分識別為基礎的權限原則附加到角色、群組和使用者，來指定哪些角色和使用者可以存取檢視。帳號 111122223333 或 444455556666 的管理員可以建立下列範例策略。然後，他們可以將策略指派給那些帳戶中的角色、群組和使用者，這些帳戶將允許使用從原始帳戶共用的檢視進行搜尋。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "resource-explorer-2:Search",
                "resource-explorer-2:GetView",
            "Resource": "arn:aws:resource-explorer-2:us-
east-1:123456789012:view/policy-name/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
        }
    ]
}
```

您可以將這些 IAM 身分型政策用作屬性型存取控制 (ABAC) 安全策略的一部分。在這種範例中，您可以確保您的所有資源和所有身份都被標記。然後，您可以在策略中指定哪些標籤鍵和值必須在身份和資源之間匹配才能允許訪問。如需有關在帳戶中標記檢視的資訊，請參閱對檢視新增標籤。如需有關以屬性為基礎的存取控制的詳細資訊，請參閱 ABAC 的用途為何？AWS 以及在 IAM 使用者指南中使用標籤控制AWS資源的存取權限。

在資源總管中刪除視圖

，Delete ()。AWS 資源總管您可以使用AWS Management Console或在AWS SDK 中執行AWS CLI命令或其等效 API 作業來刪除檢視表。

> **Note**
>
> 您無法刪除目前指定為其預設檢視的檢視表AWS 區域。若要刪除檢視，您必須移除視圖做為預設檢視。 ，DisassociateDefaultViewAPI API ()。

最低許可

，。

- 動作： `resource-explorer-2:DeleteView`

  資源：要刪除之檢視的 ARN

AWS Management Console

刪除視圖

1. ，Delete () ，() ，() ，() ，() ，()。
2. 選擇 Actions (動作)，然後選擇 Delete (刪除)。
3. ，Delete () ，Delete ()。

AWS CLI

刪除視圖

，Amazon Resource Name (ARN)。

```
$ aws resource-explorer-2 delete-view \
    --view-arn arn:aws:resource-explorer-2:us-east-1:123456789012:view/
MyViewName/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111
{
    "ViewArn": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/
MyViewName/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
}
```

使用AWS 資源總管搜尋資源

啟用的主要目的AWS 資源總管在您的AWS 帳戶是允許您的使用者搜尋帳戶中的資源。使用AWS Management Console或AWS Command Line Interface(AWS CLI) 以使用資源總管搜尋資源。

以下是資源總管搜尋的一些主要特性。

- 每次搜尋都必須使用檢視。

  檢視是資源總管用來判斷誰有權查看哪些資源的權限。若要在資源總管搜尋作業中使用檢視，使用者必須具有Allow上的resource-explorer-2:Search指定視圖的操作。此權限來自以身分為基礎的權限原則附於提出請求的主體。

  檢視可以包含篩選條件，以限制哪些資源可以包含在結果中。透過建立使用篩選器的不同檢視，並授與不同主參與者對不同檢視的存取權，您可以配置每個使用者群組只能檢視與其相關資源的環境。

  如需檢視的詳細資訊，請參閱〈管理資源總管檢視以提供搜尋存取權。
- 資源瀏覽器使用異步後台進程來維護其索引。

  Resource Explorer 可能需要一些時間，以便其索引程序探索新建立或修改的資源，並將其新增至本機索引。資源總管將本機索引中的變更複寫到彙總器索引可能需要額外的時間。

  這同樣適用於您刪除的資源。刪除索引程序會探索該刪除的資源，以及要從本機索引中移除該資源的資訊之後，可能需要一些時間。資源總管需要額外的時間，才能將該刪除從本機索引複製到帳戶的彙總索引。

  新增、修改和刪除資源最多可能需要 36 小時的時間，資源總管才能在您啟動資源總管的所有區域中顯示搜尋結果中的變更。
- 資源總管中的搜索發生在AWS 區域。

  您開啟資源總管的每個區域都只包含儲存在該區域中的資源的索引。視圖也與區域相關聯，並且只能返回該地區索引中找到的資源。其中一個例外是彙總器索引，它會接收所有本機索引的複寫副本，以支援在帳戶中的所有區域中進行搜尋。
- 跨區域搜尋需要帳戶的彙總索引。

  讓使用者搜尋所有資源的步驟AWS 區域，管理員必須指定一個 [區域]，以包含帳戶的彙總器索引。每個本機索引的副本會自動複寫到彙總索引。

  因此，只有彙總索引 Region 中的檢視才能傳回包含所有資源的結果AWS 區域在帳戶中。

- 查詢包含任意數量的自由格式文字關鍵字和篩選器。

  自由格式關鍵字會使用邏輯合併在查詢中**OR**運營商。使用資源總管定義篩選器名稱的篩選器使用邏輯組合在查詢中**AND**運營商。請看下面的例子查詢。

  ```
  test instance service:EC2 region:us-west-2
  ```

  這是由資源總管評估如下。

  ```
  test OR instance AND service:EC2 AND region:us-west-2
  ```

  此查詢要求相符資源必須是美國西部 (奧勒岡) 區域的 Amazon EC2 資源，且至少要有一個關鍵字 (測試,實例) 以某種方式附加，例如在名稱、描述或標籤中。

  > **Note**
  >
  > 因為隱含的AND，對於只能有一個與資源關聯的值的屬性，您只能成功使用一個篩選器。例如，資源只能是一個資源的一部分AWS 區域。因此，下列查詢不會傳回任何結果。
  >
  > ```
  > region:us-east-1 region:us-west-1
  > ```
  >
  > 這個限制不套用至可同時具有多個值之屬性的篩選條件，例如`tag:`,`tag.key:`，以及`tag.value:`。

- 搜尋只能傳回前 1,000 個結果。

  此需求包括含有符合所有資源的空白查詢字串的搜尋。若要查看空白查詢字串傳回超過 1,000 的資源，您必須使用查詢將相符結果限制為您要查看的結果，並將相符項目數限制在 1,000 以下。

- 您可以執行的搜尋作業數量有每個帳戶的配額。

  配額限制您每秒可進行的查詢次數，以及每個月可以進行的查詢次數。如需特定配額數量，請參閱資源總管的配額。

AWS Management Console

使用資源總管搜尋資源的步驟

1. 在「」資源搜尋頁面上，首先選擇您要使用的檢視表。您可以從您有權存取的檢視中進行選擇。
2. 對於查詢，輸入搜尋字詞，然後過濾器識別您想要查看的資源。如需有關所有可用語法選項的資訊，請參閱〈資源總管的搜尋查詢語法參考。
3. 新闻輸入提交您的查詢。

   資源總管顯示符合兩者的所有結果Filter在視圖中定義，查詢您提供的。結果會依相關性排序，符合較多查詢字詞的資源會在清單中顯示較高，而符合較少字詞的資源則會顯示在清單下方。
4. 選擇資源的標識符以導航到該資源類型的本機控制台，您可以在其中以該服務支持的所有方式與資源進行交互。

AWS CLI

使用資源總管搜尋資源的步驟

執行下列命令，以使用指定的檢視來搜尋資源。該檢視表必須存在於您執行作業的「區域」中。下列範例會搜尋已標記的 Amazon EC2 執行個體env=production在美國東部 (俄亥俄州) (美國東部-2)。如需有關所有可用語法選項的資訊query-string參數，請參閱資源總管的搜尋查詢語法參考。

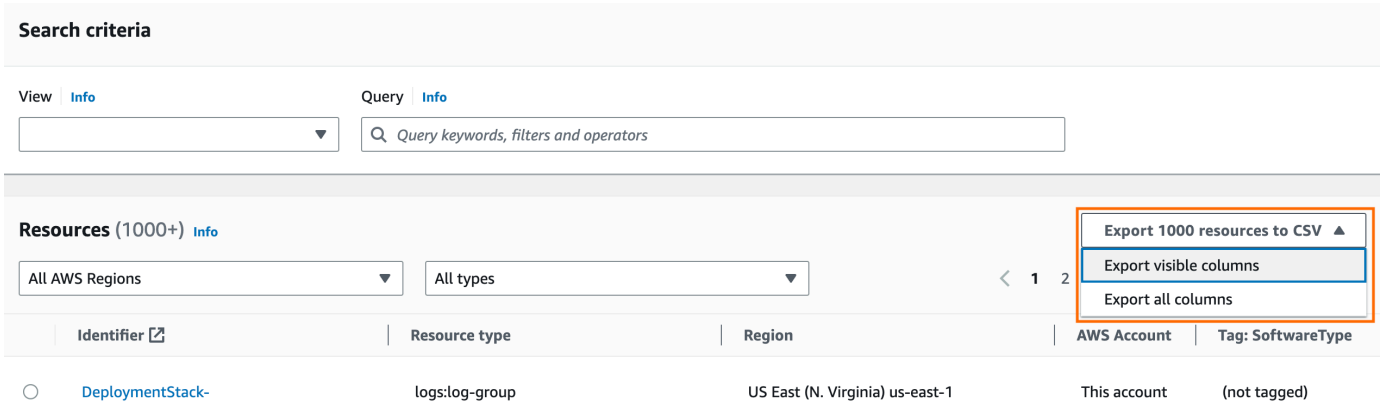
```
$ aws resource-explorer-2 search \
    --region us-east-1 \
    --query-string "resourcetype:AWS::EC2::Instance tag:env=production"
    --view-arn arn:aws:resource-explorer-2:us-east-2:123456789012:view/My-Resources-View/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111
```

將搜尋結果匯出至 .csv 檔案

您可以匯出的結果資源搜尋查詢至逗號分隔值 (.csv) 檔案。.csv 檔案包含識別碼、資源類型、區域、AWS 帳戶、標籤的總數，以及集合中每個唯一標籤鍵的欄。.csv 檔案可協助您設定您的AWS組織中的資源，或判斷跨資源標記時，哪些地方有重疊或不一致。

1. 在您的結果中資源搜尋查詢，選擇將資源匯出為 CSV。

您可以選擇只匯出目前可以看到的資料欄的結果，或匯出所有可用欄。



2. 當瀏覽器出現提示時，請選擇開啟 .csv 檔案，或將檔案儲存到方便的位置。

資源總管的搜尋查詢語法參考

AWS 資源總管 幫 AWS 助您在 AWS 帳戶. 為了協助您找到您要尋找的確切資源，Resource Explorer 接受支援本主題所述語法的搜尋查詢字串。如需示範如何使用此處所述功能的查詢範例，請參閱範例資源總管搜尋查詢。

> **Note**
>
> 目前，連接到 AWS Identity and Access Management (IAM) 資源的標籤 (例如角色或使用者) 不會建立索引。

查詢在資源總管中的工作方式

搜索查詢始終使用視圖。如果您沒有明確指定，Resource Explorer 會使用指定為您正在使 AWS 區域用的預設檢視。

檢視表決定哪些資源可供您查詢。您可以建立不同的檢視表，每個檢視都會傳回不同的資源集。

例如，您可以建立一個檢視，其中只包含那些使用索引鍵`Environment`和值標記的資源`Production`。然後，您可以選擇將該檢視的存取權授與只有具有業務理由的使用者才能檢視這些資源。需要檢視這些資源的不同使用者可以存取包含`Alpha`或`Beta`環境資源的個別檢視。如需控制誰可存取哪些檢視的資訊，請參閱授與資源總管檢視的存取權以進行搜尋。

查詢字串語法

本節提供有關查詢語法、篩選器和篩選運算子的基本層面資訊。

基本概念

最基本的是，a `QueryString` 是一組由邏輯**OR**運算符隱含連接的自由格式文本關鍵字。使用空格將每個關鍵字與其他關鍵字分隔開來，如下列範例所示：

```
ec2 billing test gamma
```

資源瀏覽器評估此關鍵字列表意味著：

```
ec2 OR billing OR test OR gamma
```

資源總管會依相關性來排序結果，對符合大量搜尋字詞的資源提供較高的偏好設定。不符合一或多個字詞的資源不會從結果中排除。但是，資源瀏覽器認為它們的相關性較低，並在搜索結果中將它們推向下。

如果您為QueryString參數指定空字串，則查詢會傳回前 1,000 個資源，這些資源可透過用於作業的檢視使用。任何查詢可傳回的資源數目上限為 1,000。

> **Note**
>
> AWS 保留更新評估自由格式文本關鍵字的匹配邏輯和相關性算法的權利，以便我們可以為客戶提供最相關的結果。因此，針對使用任意格式文字關鍵字的相同查詢傳回的結果可能會隨著時間而改變。如果您需要更具決定性的結果，我們建議您使用篩選器。過濾器匹配邏輯不會隨著時間而改變。

篩選條件

您可以透過包含篩選條件來更嚴格地限制查詢結果。與文字關鍵字不同，篩選器會使用 AND 運算子在查詢中評估。例如，請考慮下列查詢，其中包含兩個任意格式關鍵字和兩個篩選器：

```
test instance service:EC2 region:us-west-2
```

此查詢的評估方式如下：

```
( test OR instance ) AND service:EC2 AND region:us-west-2
```

篩選器一律使用 AND 邏輯運算子進行評估。如果資源與篩選器不符，則結果中不會包含該資源。範例查詢的結果包括任何與 Amazon EC2 相關聯且位於美國西部 (奧勒岡) 的資源， AWS 區域 且至少以某種方式附加了一個關鍵字。

> **Note**
>
> 由於隱含的原因AND，您只能針對只能有一個與資源關聯的值的屬性成功使用一個篩選器。例如，資源只能是一個資源的一部分 AWS 區域。因此，下列查詢不會傳回任何結果。
>
> ```
> region:us-east-1 region:us-west-1
> ```
>
> 此限制不適用於可同時具有多個值之屬性的篩選器，例如tag:tag.key:、和tag.value:。

下表列出您可以在資源總管搜尋查詢中使用的可用篩選器名稱。

篩選器名稱	說明與範例
id:	個別資源的識別碼，以 Amazon 資源名稱 (ARN) 表示。 id:arn:aws:license-manager: us-east-1 :123456789012:license-configuration:lic-ecbd5574fd92cb0d312baea26EXAMPLE
accountid:	擁 AWS 帳戶 有資源的。資源總管在結果中僅包含指定帳號所擁有的資源。 accountid:123456789012
region:	資源所 AWS 區域 在的位置。資源總管在結果中僅包含位於指定的資源 AWS 區域。 region:us-east-1 **Note** 只輸入區域碼 (不含篩選器，例如us-east-1) 不會傳回與region:us-east-1 。這個結果是因為，作為非篩選條件的自由格式文字關鍵字，Region 程式碼會細分為其個別部分。例如us-east-1 ，搜尋為useast、和1。當您使用region:前綴時，不會發生這種細分為組件。
region:global	region:篩選器的一種特殊情況，您可以使用此情況來尋找與個人無關聯 AWS 區域 但被視為全域範圍內的資源。 region:global **Note** 只輸入關鍵字不global會傳回相同的結果，region:global 因為常值單字「global」未附加至全域資源。輸入global為關鍵字只會傳回具有該常值字串與資源相關聯的資源。

篩選器名稱	說明與範例
service:	與 AWS 服務 資源類型相關聯的。資源總管在結果中僅包含由指定服務建立和管理的資源。 service:ec2
resourcetype:	*service*:*type*符號中的資源類型。資源總管在結果中僅包含指定類型的資源。 resourcetype:ec2:instance
application:	此篩選可讓您搜尋具有awsApplication 標籤鍵和資源群組值的資源。您可以依應用程式名稱或應用程式資源群組 ARN 進行搜尋。 application:MyApplicationName arn:aws:resource-groups: us-east-1 :123456789012:group/MyApplicationName **Note** 若要使用此篩選器，您的檢視必須具有標記資料的存取權。
tag:	標籤鍵/值配對表示為。<key>=<value> Resource Explorer 只會在結果中包含具有標籤且具有相符索引鍵和指定值的資源。 tag:environment=production
tag:none	tag:篩選器的一種特殊情況，可讓您搜尋沒有附加任何使用者建立標籤的資源。 **Note** 具有AWS 服務建立標籤的資源仍會顯示在此篩選器的結果中。
tag.key:	標籤鍵。資源總管在結果中僅包含具有匹配鍵的標籤的資源，而不管值如何。 tag.key:environment

篩選器名稱	說明與範例
tag.value:	標籤值。資源總管在結果中僅包含具有匹配值的標籤的資源，而不考慮密鑰名稱。 tag.value:production

篩選運算子

您可以將下表中顯示的其中一個運算子作為字串的一部分，來修改關鍵字和篩選器。

運算子	說明與範例
"*multiple word phrase*" 或 「以*#####*的短語」	用雙引號字元 (" ") 圍住應該被視為單一關鍵字的多字詞語。資源總管僅包括那些符合整個片語的資源，以及所有單詞在一起，並按指定的順序。 如果您不使用雙引號，Resource Explorer 會以空格或連字號將片語分解為其元件，並包含符合個別元件的資源，即使它們不在一起或以不同的順序也一樣。報價應該是操作員之後的所有內容。 "This matches only resources with the whole sentence." This matches resources with any of the words. "us-east-1" — 僅匹配與該確切區域相關聯的資源。 us-east-1 — 匹配任何包含「us」或「東」或「1」的資源。 -tag:"enviornment=production"
*keyword**	前綴通配符匹配。您只能在字串的結尾放置萬用字元 (星號*)。資源總管在結果中僅包括具有以前綴文本開頭的值的資源*。下列範例會符合所有 AWS 區域 以開頭的範例us-east。 region:us-east*

運算子	說明與範例
	Important 統一搜尋會在字串中第一個關鍵字的結尾自動插入萬用字元 (*) 運算子。這意味著統一的搜索結果包括匹配以指定關鍵字開頭的任何字符串的資源。 [資源總管] 主控台中 [資源搜尋] 頁面上的 [查詢] 文字方塊執行的搜尋不會自動附加萬用字元。您可以在搜尋字串中的任何字詞之後*手動插入。

運算子	說明與範例

-keyword	Not運營商。您可以在關鍵字或篩選條件的開頭加上連字號 (-)，以反轉搜尋結果。資源總管會從結果中排除符合此運算子後面的關鍵字或篩選器的任何資源。下列範例會將與 Amazon EC2 服務相關聯的所有資源排除在結果之外。
	
	`-service:ec2`
	
	Important
	如果您使用 AWS CLI `search`指令，且`--query-string` 參數值以`-`運算子做為第一個字元，則必須使用等號字元 (=) 來分隔參數名稱與其值，而不是一般的空格字元。如果您使用空格字元，CLI 會誤解字串。例如，下列查詢會失敗。
	
	`aws resource-explorer-2 search --query-string "-tag:none region:us-east-1"`
	
	以下更正的查詢字符串，=替換空格，按預期工作。
	
	`aws resource-explorer-2 search --query-string =-tag:none region:us-east-1"`
	
	如果您變更查詢字串中篩選器的順序，使得`-`不是參數值中的第一個字元，您可以使用標準空格字元。以下查詢字符串的工作原理。
	
	`aws resource-explorer-2 search --query-string "region:us-east-1 -tag:none"`

運算子	說明與範例
\<*special character*>	您可以轉義必須完全包含的特殊字符，而不是解釋。如果您的文字包含其中一個特殊字元 (* " - : = \)，您必須在該字元前加上反斜線 (\)，以確保字元是按照字面方式使用的。下列範例顯示如何使用包含連字號 () 字元 (-) 的自由格式文字關鍵字。"my-key-word" 此外，若要防止 Resource Explorer 將連字號處的運算式分成三個不同的關鍵字，您可以用雙引號括住整個片語。 "my\-key\-word" 若要插入常值反斜線，請在一列中插入兩個反斜線字元。第一個反斜線會解譯為逸出，而第二個反斜線則是要插入的常值字元。 "some_text\\some_more_text"

> **Note**
>
> 如果檢視包含附加至資源的標籤，則Search作業不會針對搜尋字串擲回驗證錯誤，因為無效的篩選器也可以解譯為自由格式文字搜尋。例如，即使cat:blue看起來像篩選器，Resource Explorer 也無法將其剖析為一個，因為cat:不是有效的定義篩選器之一。相反，Resource Explorer 會將整個字串解譯為自由格式的搜尋字串，以允許它符合標籤索引鍵名稱或 ARN 片段等項目。
> 如果符合下列任一條件，作業確實會擲回驗證錯誤：
>
> - 檢視不包含標籤的相關資訊
> - 搜尋查詢明確使用標籤篩選器 (tag.key:tag.value:、或tag:)

範例資源總管搜尋查詢

下列範例顯示您可以在中使用的常見查詢類型的語法AWS 資源總管。

> **Important**
>
> 如果您使用AWS CLIsearch指令，且--query-string參數值以-運算子做為第一個字元，則必須使用等號字元 (=) 來分隔參數名稱與其值，而不是一般的空格字元。如果您使用空格字元，CLI 會誤解字串。例如，下列查詢會失敗。
>
> ```
> aws resource-explorer-2 search --query-string "-tag:none region:us-east-1"
> ```
>
> 下列已修正的查詢會取=代空間，如預期般運作。
>
> ```
> aws resource-explorer-2 search --query-string="-tag:none region:us-east-1"
> ```
>
> 如果您變更查詢字串中篩選器的順序，使得-不是參數值中的第一個字元，您可以使用標準空格字元。下面的查詢工作。
>
> ```
> aws resource-explorer-2 search --query-string "region:us-east-1 -tag:none"
> ```

搜尋未標記的資源

如果您想要在帳戶中使用以屬性為基礎的存取控制 (ABAC)、使用以成本為基礎的配置，或針對資源執行以標籤為基礎的自動化，您必須知道帳戶中哪些資源可能遺失標籤。下列範例查詢使用特殊大小寫篩選標籤：none 可傳回缺少使用者產生標籤的所有資源。

tag:none篩選條件僅適用於使用者建立的標籤。由產生和維護的標籤AWS會從此篩選器中排除，且仍會顯示在結果中。

```
tag:none
```

()。AWS查詢字串中的第一個元素會篩選掉所有使用者建立的標籤，複製前一個範例。 AWS創建的系統標籤始終以字母開頭aws。因此，您可以使用邏輯 NOT 運算子 (-) 搭配 tag.key 篩選器，也可以排除任何具有以索引鍵名稱開頭之標籤的資源aws。

```
tag:none -tag.key:aws*
```

搜尋已標記的資源

若要尋找具有任何類型標籤的所有資源，您可以使用邏輯 NOT 運算子 (-) 搭配特殊大小寫標籤：none篩選，如下所示。

```
-tag:none
```

搜尋缺少特定標籤的資源

同樣與 ABAC 相關，您可能想要搜索所有沒有具有指定密鑰的標籤的資源。下列範例會使用邏輯 NOT運算子，傳-回缺少具有索引鍵名稱之標籤的所有資源Department。

```
-tag.key:Department
```

搜尋具有無效標籤值的資源

基於符合性原因，您可能想要搜尋重要標籤上標籤值遺漏或拼錯的所有資源。下列範例會傳回含有索引鍵名稱之標籤的所有資源environment。不過，查詢會篩選出任何具有有效值prodinteg、或的資源dev。此查詢中出現的任何結果都有其他值，您應該調查並更正。

> **Important**
>
> 資源瀏覽器搜索不區分大小寫，無法區分僅與其大寫方式不同的鍵名稱和值。例如，下列範例中的值符合PROD、prodPrOd、或任何變化。不過，有些應用程式會以區分大小寫的方式使用標籤。建議您標準化組織的大小寫策略，例如僅使用小寫的標籤關鍵字名稱和值。一致的方法可以幫助避免由於標籤的大寫不同而可能導致的混淆。

```
tag.key:environment -tag:environment=prod -tag:environment=integ -tag:environment=dev
```

搜尋下列子集中的資源AWS 區域

使用'*'萬用字元運算子來比對世界特定區域中的所有區域。下列範例會傳回位於歐洲 (EU) 區域的所有資源。

```
region:eu-*
```

全球

使用region:篩選條件的特殊大小寫global值來尋找被視為全域且與個別區域無關聯的資源。

```
region:global
```

搜索位於特定地區的特定類型的資源

當您使用多個篩選器時，Resource Explorer 會結合前置詞與隱含邏輯AND運算子來評估運算式。Amazon EC2 ()AND。

```
region:ap-east-1 resourcetype:ec2:instance
```

> **Note**
>
> 由於隱含的原因AND，您只能針對只能有一個與資源相關聯的值的屬性成功使用一個篩選器。例如，資源只能是一個資源的一部分AWS 區域。因此，下列查詢不會傳回任何結果。
>
> ```
> region:us-east-1 region:us-west-1
> ```
>
> 此限制不適用於可同時具有多個值之屬性的篩選器，例如tag:tag.key:、和tag.value:。

搜尋具有多字詞彙的資源

以雙引號 (") 括住多字詞詞彙，只會傳回以指定順序排列整個字詞的結果。如果沒有雙引號，資源總管會傳回符合任何組成字詞的個別字詞的資源。例如，下列查詢會使用雙引號，只傳回符合該字詞的資源"west wing"。查詢不符合us-west-2AWS 區域 (或其程式碼中包含的任何其他區域)west 中的資源，或符合「wing」一詞而不含「west」一詞的資源。

```
"west wing"
```

搜尋屬於指定 CloudFormation堆疊一部分的資源

當您將資源創建為AWS CloudFormation堆棧的一部分時，它們都會自動標記為堆棧的名稱。下列範例會傳回建立為指定堆疊一部分的所有資源。

```
tag:aws:cloudformation:stack-name=my-stack-name
```

在中使用統一搜尋 AWS Management Console

在每個AWS控制台頁面的頂部AWS Management Console包括一個搜索欄。此搜尋列可以搜尋AWS服務文件和部落格主題，並直接帶您前往AWS服務主控台頁面。如果您通過打開所需的資源瀏覽器功能打開統一搜索功能AWS 帳戶，它也可以返回您的資源。

透過統一搜尋，您的使用者可以從任何AWS 服務主控台搜尋資源，而不必先瀏覽至主AWS 資源總管控台。

> **Tip**
>
> 如果您想要使用統一的搜尋列特別搜尋資源，請輸入以開始搜尋查詢**`/Resources`**。這會導致AWS資源在搜尋結果中的排名高於不代表資源的結果。

主題

> **Important**
>
> 統一搜尋會在字串中第一個關鍵字的結尾自動插入萬用字元 (*) 運算子。這意味著統一的搜索結果包括匹配以指定關鍵字開頭的任何字符串的資源。
> [資源總管] 主控台中 [資源搜尋] 頁面上的 [查詢] 文字方塊執行的搜尋不會自動附加萬用字元。您可以在搜尋字串中的任何字詞之後*手動插入。

檢查是否已啟用統一搜尋

若要查看您是否已啟用統一搜尋AWS 帳戶，請查看「設定」 頁面頂端。「資源總管」會顯示該處每個需求的目前狀態。具體要求如下：

- 您必須在至少一個中開啟資源總管AWS 區域。只有具有資源總管索引的區域中的資源才能出現在統一的搜尋結果中。
- 您必須在您選擇的「區域」中建立彙總器索引。在此區域中執行的搜尋會傳回帳戶中所有已註冊區域的結果。

- 您必須在包含彙總索引的「區域」中建立預設檢視。所有需要使用統一搜尋資源的使用者都必須擁有使用此預設檢視的權限。
- 使用者必須將 AWS Identity and Access Management (IAM) 許可政策指派給其 IAM 主體，以授與執行`resource-explorer-2:Get*`、`resource-explorer-2:List*`resource-explorer-2:Describe*、`resource-explorer-2:Search`動作的權限。您可以使用自己的自訂 IAM 政策來授予這些許可。這些權限已包含在下列可供您使用的AWS受管理策略中：
  - AWSResourceExplorerReadOnlyAccess
  - AWSResourceExplorerFullAccess

開啟統一搜尋

若要啟用在搜尋結果中包含您帳戶的資源，以便從任何AWS主控台進行統一搜尋，您必須完成下列步驟：

1. AWS 資源總管在您的帳戶中啟用一個或多AWS 區域個項目。
2. 註冊一個區域以包含彙總器索引。
3. 使用彙總器索引在「區域」中建立預設檢視。

用AWS Chatbot來搜尋資源

您可以通過詢問AWS Chatbot自然語言問題來搜索AWS 服務和發現有關以及您的AWS資源的信息。AWS Chatbot透過相關文件和支援AWS文章摘錄，直接在您的聊天頻道中回答與服務相關的問題。AWS Chatbot使用資源總管來搜尋和尋找與資源相關問題的答案。

如需詳細資訊，請參閱什麼是AWS Chatbot？ 在《AWS Chatbot管理員指南》中。

AWS資源問題

AWS Chatbot使用資源總管來搜尋和探索您的資源。 AWS Chatbot將這些搜尋結果顯示在清單中。此清單顯示前五個相符資源，並包含依資源類型、AWS 區域和標籤進一步篩選結果的功能。

必要條件

要提出與AWS Chatbot資源相關的問題，您必須：

- 請確定您的AWS 區域. 索引和視圖允許資源瀏覽器編目和查詢您的資源。如需更多資訊，請參閱資源總管的術語和概念。
- 根據頻道的權限配置，將 AWSResourceExplorerReadOnlyAccess 政策添加到您的頻道角色或每個適當的用戶角色中。
- 請確認您的頻道護欄原則允許使 AWSResourceExplorerReadOnlyAccess 用權限。

常見的資源問題

您可以直接從聊天頻道提出這些問題。用您自己的信息替換紅色文本的單詞。

```
@aws What services am I using in Region?

@aws What are the resources in my account with tags?

@aws What lambda functions do I have?
```

AWS 資源總管 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 與您共同肩負的責任。共同責任模型將其描述為雲端的安全性和雲端中的安全性：

- 雲端本身的安全 – AWS 負責保護在 AWS 雲端 中執行 AWS 服務 的基礎設施。AWS 也提供您可安全使用的服務。第三方稽核人員會定期測試和驗證我們安全性的有效性，作為 AWS 合規計劃的一部分。https://aws.amazon.com/compliance/services-in-scope/
- 雲端內部的安全：您的責任取決於所使用的 AWS 服務。您也必須對其他因素負責，包括資料的機密性、您公司的要求和適用法律和法規

本文件有助於您了解如何在使用 AWS 資源總管 時套用共同責任模型。Resource Explorer。 ，Resource Explorer。AWS 服務

內容

適用於 AWS 資源總管 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。IAM 管理員控制哪些人可以驗證 (登入) 和授權 (具有權限) 以使用資源總管資源管理員資源。IAM 是一種您可以免費使用的 AWS 服務。

主題

- AWS 資源總管 身分型政策範例
- AWS Organizations 和資源總管的服務控制策略示例
- AWS 資源總管 的 AWS 受管政策
- 針對資源總管使用服務連結角色
- 疑難排解AWS 資源總管權

對象

根據您在資源總管中執行的工作而定，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 Explorer 服務執行工作，則管理員會為您提供所需的認證和權限。當您使用更多資源總管功能來完成工作時，您可能需要其他權限。了解存取的管理方式可協助您向管理員請求正確的許可。如果您無法在資源總管中存取圖徵，請參閱疑難排解AWS 資源總管權。

服務管理員 — 如果您負責公司的資源總管資源管理器資源，您可能擁有資源總管的完整存取權。決定您的服務使用者應存取哪些資源總管功能和資源是您的工作。接著，您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搭配資源總管使用 IAM，請參閱資源 Explorer 如何與 IAM 搭配運作。

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資源總管存取權的詳細資訊。若要檢視可在 IAM 中使用的資源總管以身分識別為基礎的政策範例，請參閱。AWS 資源總管 身分型政策範例

使用身分驗證

身分驗證是使用身分憑證登入 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 AWS IAM Identity Center 提供的憑證，以聯合身分登入 AWS。(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。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。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 的更多相關資訊，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 提供軟體開發套件 (SDK) 和命令列介面 (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更多相關資訊，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) 以提高帳戶的安全。如需更多資訊，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。

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。如需更多資訊，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，但角色僅提供暫時憑證。如需進一步了解，請參閱《IAM 使用者指南》中的建立 IAM 使用者（而非角色）的時機。

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更多相關資訊，請參閱《IAM 使用者指南》中的使用 IAM 角色。

使用暫時憑證的 IAM 角色在下列情況中非常有用：

- 聯合身分使用者存取 — 如需向聯合身分指派許可，請建立角色，並為角色定義許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並取得由角色定義的許可。如需有關聯合角色的相關資訊，請參閱 IAM 使用者指南中的為第三方身分提供者建立角色。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 – IAM 使用者或角色可以擔任 IAM 角色來暫時針對特定任務採用不同的許可。
- 跨帳戶存取權 – 您可以使用 IAM 角色，允許不同帳戶中的某人（信任的委託人）存取您帳戶中的資源。角色是授予跨帳戶存取權的主要方式。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權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儲存在 Amazon Simple Storage Service (Amazon S3) 中。服務可能會使用呼叫主體的許可、使用服務角色或使用服務連結角色來執行此作業。
  - 轉發存取工作階段 (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。如需更多資訊，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 角色來管理暫時憑證。這是在 EC2 執行個體內儲存存取金鑰的較好方式。如需指派 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暫時憑證。如需更多資訊，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 文件形式儲存在 AWS 中。如需 JSON 政策文件結構和內容的更多相關資訊，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。

預設情況下，使用者和角色沒有許可。若要授與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 管理政策和客戶管理政策。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 IAM 角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中指定主體。主體可以包括帳戶、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。

AWS 資源總管 不支援資源型政策。

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。

AWS 資源總管 不支援 ACL。

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與您的最大許可。

- 許可界限 – 許可範圍是一種進階功能，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。如需許可範圍的更多相關資訊，請參閱《IAM 使用者指南》中的 IAM 實體許可範圍。
- 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。如需組織和 SCP 的更多相關資訊，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。如需更多資訊，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。

資源 Explorer 如何與 IAM 搭配運作

在您使用 IAM 來管理的存取權之前AWS 資源總管，您應該先了解可與資源總管搭配使用的 IAM 功能有哪些 IAM 功能有哪些。若要取得資源 Explorer 和其他 IAM 如何使AWS 服務用 IAM 的詳細資訊，請參閱AWS 服務 IAM 使用者指南中的可與 IAM 搭配 IAM 運作的 IAM。

主題

- 資源總管以身分為基礎的政策
- 以資源瀏覽器為基礎的授權
- 資源總管 IAM 角色

像任何其他資源管理器一樣AWS 服務，資源總管需要使用其操作與您的資源進行交互的權限。若要搜尋，使用者必須擁有擷取檢視詳細資料的權限，以及使用檢視進行搜尋。若要建立索引或檢視，或修改索引或任何其他資源總管設定，您必須具有其他權限。

指派 IAM 身分型政策，將這些許可授與適當的 IAM 主體。資源總管提供數個預先定義一般使用權限集的受管理策略。您可以將這些指派給 IAM 主體。

資源總管以身分為基礎的政策

使用 IAM 身分型政策，您可以針對特定資源，以及在何種條件下允許或拒絕的動作，以及在何種條件下允許或拒絕這些動作。資源 Explorer 支援特定動作、資源和條件索引鍵。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 IAM 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。

資源總管中的策略動作會在動作之前使用`resource-explorer-2`服務前置詞。例如，若要授予某人使用資源 ExplorerSearch API 操作的許可，請在指派給該主體的政策中包括`resource-explorer-2:Search`動作。政策陳述式必須包含 `Action` 或 `NotAction` 元素。資源 Explorer 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的任務。這些與資源總管 API 操作保持一致。

若要在單一陳述式中指定多個動作，請以逗號分隔它們，如下列範例所示。

```
"Action": [
      "resource-explorer-2:action1",
      "resource-explorer-2:action2"
]
```

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 Describe 文字的所有動作，請包含以下動作：

```
"Action": "resource-explorer-2:Describe*"
```

如需資源總管動作的清單，請參閱AWS服務授權參考AWS 資源總管中定義的動作。

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": "*"
```

檢視

主要資源總管資源類型是檢視表。

資源總管檢視資源有以下 ARN 格式。

```
arn:${Partition}:resource-explorer-2:${Region}:${Account}:view/${ViewName}/${unique-id}
```

下列範例顯示資源總管 ARN 格式。

```
arn:aws:resource-explorer-2:us-east-1:123456789012:view/My-Search-
View/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111
```

> **Note**
>
> 視圖的 ARN 在末尾包括一個唯一的標識符，以確保每個視圖都是唯一的。這有助於確保授予舊版、已刪除檢視存取權的 IAM 政策不會意外地授與新檢視的存取權，而該資料檢視恰好與舊檢視具有相同名稱。每個新視圖最後都會收到一個新的唯一 ID，以確保 ARN 永遠不會重複使用。

如需 ARN 格式的詳細資訊，請參閱 Amazon Resource Name (ARN)。

您可以使用指派給 IAM 主體的 IAM 身分型政策，並將檢視指定為Resource. 這樣做可讓您透過一個檢視將搜尋存取權授與一組主參與者，並透過完全不同的檢視來存取不同的主參與者集。

例如，若要授與 IAM 政策陳述式ProductionResourcesView中指定的單一檢視的權限，請先取得檢視的 Amazon 資源名稱 (ARN)。您可以使用主控台中的「視觀表」頁面來檢視視觀表的詳細資訊，或呼叫ListViews作業來擷取想要的視觀表的完整 ARN。然後，將它包含在策略聲明中，就像下面示例中顯示的那樣，該聲明僅授予修改一個視圖的定義的權限。

```
"Effect": "Allow",
"Action": "UpdateView",
"Resource": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/
ProductionResourcesView/<unique-id>"
```

若要允許對屬於特定帳戶的所有檢視執行動作，請在 ARN 的相關部分中使用萬用字元 (*)。下列範例會將搜尋權限授AWS 區域與指定和帳戶中的所有檢視。

```
"Effect": "Allow",
"Action": "Search",
"Resource": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/*"
```

某些資源總管動作 (例如) 不會針對特定資源執行，因為如下列範例所示，資源尚不存在。CreateView在這種情況下，您必須對整個資源 ARN 使用萬用字元 (*)。

```
"Effect": "Allow",
"Action": "resource-explorer-2:CreateView"
"Resource": "*"
```

如果您指定以萬用字元結尾的路徑，則可以將CreateView作業限制為僅建立具有核准路徑的檢視。下列範例原則部分顯示如何允許主參與者僅在路徑中建立檢視view/ProductionViews/。

```
"Effect": "Allow",
"Action": "resource-explorer-2:CreateView"
"Resource": "arn:aws:resource-explorer-2:us-
east-1:123456789012:view/ProductionViews/*""
```

索引

您可以用來控制對資源 Explorer 功能存取的資源類型是索引。

您與索引互動的主要方式是AWS 區域透過在該區域中建立索引來開啟資源總管。之後，您幾乎可以通過與視圖交互來完成其他所有操作。

您可以使用索引執行的一件事是控制誰可以在每個區域中建立檢視表。

> **Note**
>
> 建立檢視後，IAM 只會針對檢視的 ARN 授權所有其他檢視動作，而非索引。

索引具有 ARN，您可以在權限原則中參考。資源瀏覽器索引 ARN 採用下列格式。

```
arn:${Partition}:resource-explorer-2:${Region}:${Account}:index/${unique-id}
```

請參閱下列資源總管索引 ARN 的範例。

```
arn:aws:resource-explorer-2:us-east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-
abcd22222222
```

某些資源總管動作會針對多種資源類型檢查驗證。例如，CreateView作業會針對索引的 ARN 和檢視的 ARN 進行授權，就像資源總管建立它之後一樣。若要授與管理員管理 Resource Explorer 服務的權限，您可以使用`"Resource": "*"`來授權任何資源、索引或檢視的動作。

或者，您可以將主參與者限制為僅能夠使用指定的「資源總管」資源。例如，若要將動作限制為只有指定區域中的 Resource Explorer 資源，您可以包含同時符合索引和檢視的 ARN 範本，但只會呼叫單一區域。在下列範例中，ARN 只會比對指定帳戶的 [us-west-2區域] 中的索引或檢視表。在 ARN 的第三個欄位中指定 Rework，但在最後一個欄位中使用萬用字元 (*)，以匹配任何資源類型。

```
"Resource": "arn:aws:resource-explorer-2:us-west-2:123456789012:*
```

如需詳細資訊，請參閱AWS服務授權參考AWS 資源總管中的定義資源。若要了解您可以使用哪些動作指定每個資源的 ARN，請參閱 AWS 資源總管 定義的動作。

條件索引鍵

Resource Explorer 不提供任何服務專用條件索引鍵，但它支援使用一些全域條件金鑰。若要查看 AWS 全域條件金鑰，請參閱《IAM 使用者指南》中的 AWS 全域條件內容金鑰。

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。

若要查看可與資源總管搭配使用的條件金鑰清單，請參閱AWS服務授權參考AWS 資源總管中的條件金鑰。若要了解您可以搭配哪些動作和資源使用條件索引鍵的動作和資源，請參閱定義的動作AWS 資源總管。

範例

若要檢視資源總管身分型政策的範例，請參閱AWS 資源總管 身分型政策範例。

以資源瀏覽器為基礎的授權

您可以將標籤連接至資源 Explorer 檢視，或是在請求中將標的標資源傳遞至資源總管。若要根據標籤控制存取，請使用 `resource-explorer-2: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。如需標記資源總管資源的詳細資訊，請參閱對檢視新增標籤。如需在資源總管中使用基於標籤的授權，請參閱使用基於標籤的授權來控制對視圖的存取權。

資源總管 IAM 角色

IAM 角色是您的主體AWS 帳戶，具備特定許可。

將暫時憑證與資源總管使用

您可以搭配聯合使用臨時憑證、擔任 IAM 角色，或是擔任跨帳戶角色。您可以呼叫AWS Security Token Service (AWS STS) API 作業 (例如AssumeRole或) 來取得臨時安全登入資料GetFederationToken。

資源總管支援使用臨時憑證。

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。服務連結角色會顯示在您的 IAM 帳戶中，並由該服務所擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

資源總管使用服務連結角色來執行其工作。如需資源總管服務連結角色的詳細資訊，請參閱針對資源總管使用服務連結角色。

AWS 資源總管 身分型政策範例

預設情況下，AWS Identity and Access Management(IAM) 主體 (如角色、群組和使用者) 沒有建立或修改資源總管資源的許可。他們也無法使用AWS Management Console、AWS Command Line Interface (AWS CLI) 或AWS API 執行工作。IAM 管理員必須建立 IAM 政策必須授予主體授予主體許可，授予主體在指定資源上執行特定 API 操作的所需許可。然後，管理員必須將這些政策指派這些政策指派給需要這些許可的 IAM 主體。

若要提供存取權，請新增許可到您的使用者、群組或角色：

- AWS IAM Identity Center 中的使用者和群組：

  建立許可集合。請遵循《AWS IAM Identity Center 使用者指南》的建立許可集合中的指示。
- 透過身分提供者在 IAM 中管理的使用者：

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

若要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
- 使用資源總管主控台
- 根據標籤授予檢視的存取權
- 授予根據標籤建立檢視的存取權
- 允許主參與者檢視他們自己的許可

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、存取或刪除資源總管理器資源。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 AWS 帳戶中 IAM 使用者或根使用者的情況，請開啟 MFA 提供額外的安全性。若要在呼叫 API 操作時請求 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。

使用資源總管主控台

若要在主AWS 資源總管控台中搜尋主體，他們必須擁有最基本的一組許可。如果您未建立具有最低必要許可的基於身分的政策，則對於帳戶中的主體而言，Resource Explorer 主控台將無法如預期運作。

您可以使用名為AWSResourceExplorerReadOnlyAccess的AWS受管理策略授與使用 Resource Explorer 主控台來使用帳戶中的任何檢視進行搜尋的能力。若要授與僅使用單一檢視進行搜尋的權限授與資源總管檢視的存取權以進行搜尋，請參閱以下兩節中的和範例。

對於僅呼叫 AWS CLI 或 AWS API 的主體，您不需要允許其最基本主控台許可。相反地，您可以選擇僅授與主參與者需要執行之 API 作業相符的動作的存取權。

根據標籤授予檢視的存取權

在此範例中，您想要授予您帳戶中的主體的存取權授AWS 帳戶予您帳戶中的主體。若要這麼做，您可以將 IAM 身分型政策指派給您希望能夠在資源總管中搜尋的主體。下列 IAM 政策範例會授予任何請求的存取權，其中附加至呼叫主體的標Search-Group籤與請求中使用的檢視相同標籤的值完全相符。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "resource-explorer-2:GetView",
                "resource-explorer-2:Search"
            ],
            "Resource": "arn:aws:resource-explorer-2:*:*:view/*",
            "Condition": {
                "StringEquals": {"aws:ResourceTag/Search-Group": "${aws:PrincipalTag/
Search-Group}"}
            }
        }
    ]
}
```

您可以將此政策指派給您帳戶中的 IAM 主體。如果具有標籤的主參與者Search-Group=A嘗試使用「資源總管」檢視進行搜尋，則也必須標記檢視Search-Group=A。如果不是，則主體會被拒絕存取。條件標籤鍵 Search-Group 符合 Search-group 和 search-group，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。

> **Important**
>
> 若要在中的統一搜尋結果中查看您的資源AWS Management Console，主參GetView與者必須同時具有包含彙總索引之AWS 區域預設檢視的和Search權限。授與這些權限的最簡單方法是保留在您使用 [快速] 或 [進階] 設定開啟 [資源總管] 時附加至檢視的預設以資源為基礎的權限。
>
> 在這個案例中，您可以考慮設定預設檢視來篩選出敏感資源，然後設定您授與以標籤為基礎之存取權的其他檢視，如前面的範例所述。

授予根據標籤建立檢視的存取權

在此範例中，您只想要允許標記為與索引相同的主參與者能夠在包含索引的AWS 區域檢視中建立檢視。若要這麼做，請建立以識別為基礎的權限，以允許主參與者使用檢視進行搜尋。

現在您已可以準備授予建立檢視的許可。您可以將此範例中的陳述式新增至您用來授與適當主體Search權限的相同權限原則。根據連接至主參與者 (呼叫檢視要與之相關聯之作業和索引) 的標籤，允許或拒絕動作。下列範例 IAM 政策會拒絕任何建立檢視表的請求，當連接到呼叫者主體的Allow-Create-View標記值與建立檢視的區域中附加至索引的相同標記的值不完全相符時，建立檢視表。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "resource-explorer-2:CreateView",
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {"aws:ResourceTag/Allow-Create-View":
 "${aws:PrincipalTag/Allow-Create-View}"}
            }
        }
    ]
}
```

允許主參與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": "*"
        }
    ]
}
```

AWS Organizations 和資源總管的服務控制策略示例

AWS 資源總管 支援服務控制原則 (SCP)。SCP 是您附加至組織中元素的政策，藉此管理該組織內的許可。SCP 適用於您附加 SCP 的元素下的所有組織 AWS 帳戶 中。SCP 可集中控制組織中所有帳戶可用的許可上限。他們可以幫助您確保您的 AWS 帳戶 逗留在組織的存取控制準則範圍內。如需詳細資訊，請參閱《AWS Organizations 使用者指南》中的服務控制政策。

必要條件

若要使用 SCP，您必須執行下列動作：

- 啟用您組織的所有功能。如需詳細資訊，請參閱 AWS Organizations 使用者指南中的啟用組織中的所有功能。
- 啟用 SCP 以便於您的組織內使用。如需詳細資訊，請參閱《AWS Organizations 使用者指南》中的啟用和停用政策類型。
- 建立您需要的 SCP。如需有關建立 SCP 的詳細資訊，請參閱《AWS Organizations 使用指南》中的〈建立和更新 SCP〉。

服務控制政策的範例

下列範例顯示如何使用以屬性為基礎的存取控制 (ABAC) 來控制對資源總管系統管理作業的存取。除了搜尋所需的兩個權限以外，此範例政策會拒絕存取所有 Resource Explorer 作業`resource-explorer-2:GetView`，`resource-explorer-2:Search`並且除非提出請求的 IAM 主體已加上標籤`ResourceExplorerAdmin=TRUE`。如需將 ABAC 與資源總管搭配使用的更完整討論，請參閱使用基於標籤的授權來控制對視圖的存取權。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "resource-explorer-2:AssociateDefaultView",
        "resource-explorer-2:BatchGetView",
        "resource-explorer-2:CreateIndex",
        "resource-explorer-2:CreateView",
        "resource-explorer-2:DeleteIndex",
        "resource-explorer-2:DeleteView",
        "resource-explorer-2:DisassociateDefaultView",
        "resource-explorer-2:GetDefaultView",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListSupportedResourceTypes",
        "resource-explorer-2:ListTagsForResource",
        "resource-explorer-2:ListViews",
        "resource-explorer-2:TagResource",
        "resource-explorer-2:UntagResource",
```

```
        "resource-explorer-2:UpdateIndexType",
        "resource-explorer-2:UpdateView""
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
          "StringNotEqualsIgnoreCase": {"aws:PrincipalTag/ResourceExplorerAdmin":
 "TRUE"}
      }
    ]
}
```

AWS 資源總管 的 AWS 受管政策

AWS 管理的政策是由 AWS 建立和管理的獨立政策。AWS 管理的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。

請謹記，AWS 管理的政策可能不會授予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 管理的政策中定義的許可。如果 AWS 更新 AWS 管理的政策中定義的許可，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 管理的政策。

如需詳細資訊，請參閱《IAM 使用者指南》中的 AWS 受管政策。

包含資源總AWS管權限的一般受管原則

- AdministratorAccess— 授予對AWS 服務資源的完全訪問權限。
- ReadOnlyAccess— 授予對AWS 服務和資源的唯讀存取權限。
- ViewOnlyAccess— 授予檢視資源和基本中繼資料的權限AWS 服務。

> **Note**
>
> 包含在`ViewOnlyAccess`原則中的 Resource Explorer `Get*` 權限會執行類似`List`權限，雖然它們只會傳回單一值，因為 [區域] 只能包含一個索引和一個預設檢視。

AWS資源總管的受管理策略

- AWSResourceExplorerFullAccess
- AWSResourceExplorerReadOnlyAccess
- AWSResourceExplorerServiceRolePolicy

AWS 受管政策： AWSResourceExplorerFullAccess

您可以將AWSResourceExplorerFullAccess政策指派給您的 IAM 身分。

此原則會授與允許資源總管服務完整系統管理控制權的權限。您可以在帳戶中執行與開啟和管理資源總管相關的AWS 區域所有工作。

許可詳細資訊

此原則包含允許資源總管執行所有動作的權限，包括在中開啟和關閉資源總管AWS 區域、建立或刪除帳號的彙總器索引、建立、更新和刪除檢視，以及搜尋。此原則也包含不屬於資源總管一部分的權限：

- ec2:DescribeRegions-允許資源總管訪問有關您帳戶中區域的詳細信息。
- ram:ListResources— 允許資源總管列出資源屬於資源的資源共用。
- ram:GetResourceShares— 可讓資源總管識別有關您擁有或與您共用之資源共用的詳細資料。
- iam:CreateServiceLinkedRole— 當您透過建立第一個索引來開啟資源總管時，可讓資源總管建立必要的服務連結角色。
- organizations:DescribeOrganization— 允許資源總管存取組織的相關資訊。

若要查看此AWS受管理策略的最新版本，請參閱《AWS受管策略參考指南》*AWSResourceExplorerFullAccess*中的。

AWS 受管政策： AWSResourceExplorerReadOnlyAccess

您可以將AWSResourceExplorerReadOnlyAccess政策指派給您的 IAM 身分。

此原則會授與唯讀權限，允許使用者進行基本搜尋存取權以探索其資源。

許可詳細資訊

此原則包括允許使用者執行 Resource Explorer 的權限 Get*List*，以及檢視資源總管元件和組態設定相關資訊的Search作業，但不允許使用者變更它們。使用者也可以搜尋。此原則也包含兩個不屬於資源總管的權限：

- ec2:DescribeRegions-允許資源總管訪問有關您帳戶中區域的詳細信息。
- ram:ListResources— 允許資源總管列出資源屬於資源的資源共用。
- ram:GetResourceShares— 可讓資源總管識別有關您擁有或與您共用之資源共用的詳細資料。
- organizations:DescribeOrganization— 允許資源總管存取組織的相關資訊。

若要查看此AWS受管理策略的最新版本，請參閱《AWS受管策略參考指南》*AWSResourceExplorerReadOnlyAccess*中的。

AWS 受管政策： AWSResourceExplorerServiceRolePolicy

您無法自行附加AWSResourceExplorerServiceRolePolicy至任何 IAM 實體。此原則只能附加至允許 Resource Explorer 代表您執行動作的服務連結角色。如需詳細資訊，請參閱針對資源總管使用服務連結角色。

此原則會授與資源總管擷取資源相關資訊所需的權限。資源總管填充它在您註冊的每個AWS 區域索引中維護。

若要查看此AWS受管政策的最新版本，請參閱 IAM 主控台AWSResourceExplorerServiceRolePolicy中的。

AWS 受管政策： AWSResourceExplorerOrganizationsAccess

您可以指派AWSResourceExplorerOrganizationsAccess給您的 IAM 身分。

此原則會將系統管理權限授與資源總管，並將唯讀權限授與其他人，AWS 服務以支援此存取。管理 AWS Organizations員需要這些權限才能在主控台中設定和管理多帳戶搜尋。

許可詳細資訊

此原則包含允許系統管理員為組織設定多帳戶搜尋的權限：

- ec2:DescribeRegions— 允許資源瀏覽器訪問有關您帳戶中區域的詳細信息。
- ram:ListResources— 允許資源總管列出資源屬於資源的資源共用。
- ram:GetResourceShares— 允許資源總管識別有關您擁有或與您共用之資源共用的詳細資料。
- organizations:ListAccounts— 允許資源總管識別組織內的帳號。
- organizations:ListRoots— 允許資源總管識別組織內的根帳號。
- organizations:ListOrganizationalUnitsForParent— 允許資源總管識別父組織單位或根目錄中的組織單位 (OU)。

- `organizations:ListAccountsForParent`— 允許資源總管識別組織中指定目標根目錄或 OU 所包含的帳號。
- `organizations:ListDelegatedAdministrators`— 允許資源總管識別在此組織中指定為委派管理員的AWS帳號。
- `organizations:ListAWSServiceAccessForOrganization`— 允許資源總管識別已啟用AWS服務可與您的組織整合的清單。
- `organizations:DescribeOrganization`— 允許資源總管擷取使用者帳號所屬組織的相關資訊。
- `organizations:EnableAWSServiceAccess`— 允許資源總管啟用與 AWS 服務 (由指定的服務`ServicePrincipal`) 的整合AWS Organizations。
- `organizations:DisableAWSServiceAccess`— 允許資源總管停用與 AWS 服務 (由指定的服務 ServicePrincipal) 的整合AWS Organizations。
- `organizations:RegisterDelegatedAdministrator`— 允許資源總管啟用指定的成員帳戶來管理指定AWS服務的組織功能。
- `organizations:DeregisterDelegatedAdministrator`— 允許資源總管以指定的委派管理員 AWS 帳戶身分移除指定的成員AWS 服務。
- `iam:GetRole`— 允許資源總管擷取有關指定角色的資訊，包括角色的路徑、GUID、ARN 以及授與承擔角色之權限的角色信任原則。
- `iam:CreateServiceLinkedRole`— 當您透過建立第一個索引來開啟資源總管時，允許資源總管建立必要的服務連結角色。

若要查看此AWS受管政策的最新版本，請參閱 IAM 主控台`AWSResourceExplorerOrganizationsAccess`中的。

AWS受管理策略的資源總管更新

檢視資源總AWS管受管理策略的詳細資料，因為這項服務開始追蹤這些變更。如需有關此頁面變更的自動警示，請訂閱資源瀏覽器文件歷程記錄頁面上的 RSS 摘要。

變更	描述	日期
新的 受管政策	資源總管新增下列AWS受管理的策略：	2023 年 11 月 14 日

變更	描述	日期
	• AWSResourceExplorerOrganizationsAccess	
已更新 受管政策	資源總管更新了下列AWS受管理的策略，以支援多帳號搜尋： • AWSResourceExplorerFullAccess • AWSResourceExplorerReadOnlyAccess	2023 年 11 月 14 日
AWSResourceExplorerServiceRolePolicy-更新了政策以支持與 Organizations 的多帳戶搜索	Resource Explorer 將權限新增至服務連結角色原則，AWSResourceExplorerServiceRolePolicy_該策略允許資源總管支援 Organizations 的多帳號搜尋： • organizations:ListAWSServiceAccessForOrganization • organizations:DescribeAccount • organizations:DescribeOrganization • organizations:ListAccounts • organizations:ListDelegatedAdministrators	2023 年 11 月 14 日

變更	描述	日期
AWSResourceExplorerServiceRolePolicy-更新了策略以支持其他資源類型	Resource Explorer 將權限新增至服務連結角色原則，AWSResourceExplorerServiceRolePolicy 該策略允許服務對下列資源類型建立索引： • 存取分析器:分析器 • 公告:证书管理局 • 放大:應用程式 • 放大:後端電容 • 放大:分支 • 放大:網域關聯 • 放大器:元件 • 放大器:主題 • 應用程式整合:事件整合 • 應用程式:服務 • 應用程式流:應用程式塊 • 應用程式串流:應用 • 應用程式流:艦隊 • 應用程式流:影像建置器 • 應用程式流:堆疊 • 應用程序:圖形 • ps: 規則群組命名空間 • 應用:工作區 • 原理:重建 • 主要方式:部署 • 雅典:資料目錄 • 雅典:工作群組	2023 年 10 月 17 日

變更	描述	日期
	• 自動調整比例:自動調整比例群組 • 備份:備份計劃 • 批次:計算環境 • 批次:工作佇列 • 批次:排程政策 • 雲形成:堆疊 • 雲端格式化:堆疊集 • 雲端前端:欄位層級加密設定 • 雲端前端:欄位層級加密設定檔 • 雲端前端:原始存取控制 • 雲路:軌跡 • 程式碼:網域 • 程式碼元件:儲存庫 • 程式碼交付:儲存庫 • 程式碼群組:效能分析群組 • 程式碼啟動連線:連線 • 資料庫:資料集 • 資料庫:配方 • 資料庫:規則集 • 偵測:圖形 • 目錄服務:目錄 • ec2: 運營商網關 • ec2: 驗證存取端點 • ec2: 驗證存取群組 • ec2: 驗證存取實例 • ec2: 驗證訪問提供者 • ecr: 儲存庫	

變更	描述	日期
	• 彈性:緩存組 • 彈性檔案系統:存取 • 事件:規則 • 證明:實驗 • 明顯:特徵 • 證明:啟動 • 明顯:專案 • 尋找空間:環境 • 防火管:交付串流 • 錯誤注入模擬器:實驗樣板 • 預測:資料集群組 • 預測:資料集 • 欺詐偵測器:偵測器 • 欺詐偵測器:圖元類型 • 詐騙偵測器:事件類型 • 欺詐偵測器:標籤 • 詐騙偵測器:結果 • 欺詐偵測器:變數 • 遊戲:別名 • 全域加速器:加速器 • 全域加速器:端點群組 • 全域加速器:監聽器 • 膠水:資料庫 • 膠水:工作 • 膠水:桌子 • 膠水:觸發器 • 格蘭:群組 • 健康湖:健康資料存放區 • 位置:虛擬裝置	

變更	描述	日期
	• 影像建置器:元件建置版本 • 影像建置器:元件 • 影像建置器:容器配方 • 影像建置器:分散組態 • 影像建置器:影像建置版本 • 影像建置器:影像管線 • 影像建置器:影像配方 • 影像建置器:影像 • 影像建置器:基礎架構組態 • 物聯網:授權者 • 物聯網:工作樣板 • 物聯網:緩和作用 • 物聯網:佈建樣板 • 物聯網:安全性設定檔 • 物聯網:物件 • 物聯網:主題規則目標 • 物聯分析:頻道 • 物聯分析:資料集 • 物聯分析:資料存放區 • 物聯分析:配管 • 碘:報警模型 • 碘元:偵測器模型 • 物件數:輸入 • 物聯網智慧:資產模型 • 物聯網智慧:資產 • 物聯網智慧:閘道 • 物聯軸器:工作區 • iv: 頻道 • iv: 串流鍵	

變更	描述	日期
	• 卡片:叢集 • 動態視訊:串流 • 羊巴達:別名 • 羊巴達:圖層版本 • 羊巴達:圖層 • 查看度量:警示 • 查看:專案 • 媒體封裝:通道 • 媒體封裝:原始端點 • 媒體順序:播放組態 • 記憶體:ACL • 記憶體:叢集 • 記憶體:參數群組 • 記憶體:使用者 • 行動裝置:應用程式 • 行動裝置:區段 • 行動裝置:範本 • 網路防火牆:防火牆政策 • 網路防火牆:防火牆 • 網路管理員:全球網路 • 網路管理員:設備 • 網路管理員:連結 • 網路管理員:貼附 • 網路管理員:核心網路 • 全景:套件 • qldb: 分類帳中的日誌資料流 • 分類帳:分類帳 • rds: 藍綠部署 • 重構空間:應用程式	

變更	描述	日期
	• 重構空間:環境 • 重構空間:佈線 • 重構:服務 • 重新認知:專案 • 恢復中心:應用程式 • 復原中心:彈性原則 • 資源群組:群組 • 路由 53: 恢复组 • 路線 53：資源 • 路線 53: 防火牆域 • 路線 53: 防火牆組 • 路線 53: 解析倫敦點 • 路線 53: 解析規則 • 下模器:模型 • 下垂器:筆記本例證 • 簽署者:簽署設定檔 • 回應計劃:回應計劃 • ssm: 庫存輸入 • SSM: 資源資料異步 • 狀態:活動 • 時間流:資料庫 • 智慧:助理 • 智慧:助理協會 • 智慧:知識庫	

變更	描述	日期
AWSResourceExplorerServiceRolePolicy-更新了策略以支持其他資源類型	Resource Explorer 將權限新增至服務連結角色原則，AWSResourceExplorerServiceRolePolicy 該策略允許服務對下列資源類型建立索引： • 程式碼建置:專案 • 程式碼管線:配管 • 認知:識別池 • 認知:使用者集區 • ecr: 儲存庫 • ef: 檔案系統 • 彈性狀態:應用程式 • 彈性鏈條:應用程式版本 • 彈性狀態:環境 • 物聯網:策略 • 物聯網:主題規 • 步驟函數:靜態 • S3: 桶	2023 年 8 月 1 日

變更	描述	日期
AWSResourceExplorerServiceRolePolicy-更新了策略以支持其他資源類型	Resource Explorer 將權限新增至服務連結角色原則，AWSResourceExplorerServiceRolePolicy 該策略允許服務對下列資源類型建立索引： • 彈性:叢集 • 彈性:全域複製群組 • 彈性:參數群組 • 彈性:複製群組 • 彈性:保留執行個體 • 彈性:快照 • 彈性:子網路群組 • 彈性:使用者 • 彈性:使用者群組 • 拉姆達：code-signing-config • 拉姆達：event-source-mapping • 方塊:佇列	2023 年 3 月 7 日
新的受管理策略	資源總管新增下列AWS受管理的策略： • AWSResourceExplorerFullAccess • AWSResourceExplorerReadOnlyAccess • AWSResourceExplorerServiceRolePolicy	2022 年 11 月 7 日
資源總管開始追蹤變更	資源總管開始追蹤其AWS受管理策略的變更。	2022 年 11 月 7 日

針對資源總管使用服務連結角色

AWS 資源總管 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資源總管的唯一 IAM 角色類型。服務連結角色由 Resource Explorer 預先定義，並包含服務代表您呼叫其他人所需AWS 服務的所有權限。

服務連結角色可讓您更輕鬆地設定資源總管，因為您不需要手動新增必要的權限。資源總管會定義其服務連結角色的權限，除非另有定義，否則只有資源總管可以擔任其角色。定義的許可包括信任政策和許可政策，而且該許可政策無法指派給任何其他 IAM 實體。

如需支援服務連結角色之其他服務的資訊，請參閱《IAM 使用者指南》中的與 IAM 搭配運作的 AWS 服務。在那裡，尋找在服務連結角色欄中具有 [是] 的服務。選擇具有連結的是，以檢視該服務的服務連結角色文件。

資源總管的服務連結角色權限

資源總管使用名為AWSServiceRoleForResourceExplorer的服務連結角色。此角色會授與 Resource Explorer 服務的權限，以便代表您AWS 帳戶檢視資源和AWS CloudTrail事件，並為這些資源建立索引以支援搜尋。

服AWSServiceRoleForResourceExplorer務連結角色只會信任具有下列服務主體的服務擔任該角色：

- resource-explorer-2.amazonaws.com

名為的角色權限原則AWSResourceExplorerServiceRolePolicy允許 Resource Explorer 唯讀存取，以擷取支援資源的資AWS源名稱和屬性。若要檢視資源總管支援的服務和資源，請參閱您可以使用資源總管搜尋的資源類型。如需此角色可執行之所有動作的完整清單，您可以在 IAM 主控台中檢視AWSResourceExplorerServiceRolePolicy政策。

主體是 IAM 實體，例如使用者、群組或角色。如果讓 Resource Explorer 在帳號的第一個區域中建立索引時為您建立服務連結角色，則執行工作的主參與者只需要建立資源總管索引所需的權限。若要使用 IAM 手動建立服務連結角色，執行工作的主體必須具有建立服務連結角色的權限。如需詳細資訊，請參閱 IAM 使用者指南中的服務連結角色許可。

建立資源總管的服務連結角色

您不需要手動建立一個服務連結角色。當您在中開啟資源總管AWS Management Console，或使用或 AWS API CreateIndex在帳戶AWS 區域中的第一個執行時，資源總管會為您建立服務連結角色。AWS CLI

如果您刪除此服務連結角色，然後需要重新建立角色，則可以使用相同的程序在帳戶中重新建立角色。當您RegisterResourceExplorer在帳號中的第一個區域中時，資源總管會再次為您建立服務連結角色。

編輯資源總管的服務連結角色

資源總管不允許您編輯AWSServiceRoleForResourceExplorer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。

刪除資源總管的服務連結角色

您可以使用 IAM 主控台AWS CLI、或 AWS API 手動刪除服務連結角色。若要這麼做，您必須先從帳戶AWS 區域中的每個項目移除 Resource Explorer 索引，然後才能手動刪除服務連結角色。

> **Note**
>
> 當您嘗試刪除資源時，如果資源總管服務正在使用該角色，則刪除會失敗。如果發生這種情況，請確保刪除所有區域中的所有索引，然後等待幾分鐘，然後再次嘗試該操作。

使用 IAM 手動刪除服務連結角色

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

資源總管服務連結角色的支援區域

資源總管支援在所有提供服務的區域中使用服務連結角色。如需詳細資訊，請參閱中的AWS 服務端點Amazon Web Services 一般參考。

疑難排解AWS 資源總管權

請使用資源管理器和修復使用資源總管和修復使用資源總管和修復使用資源總管和修復使用資源總管和AWS Identity and Access Management修復使用資源總管

主題

- 我未獲授權在資源管理器中執行動作
- 我想要允許外的人員存取我AWS 帳戶的資源管理器資源

我未獲授權在資源管理器中執行動作

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嘗試進行此操作的認證。

例如，以下錯誤會在有resource-explorer-2:GetView人假設 IAM 角色MyExampleRole嘗試使用主控台檢視檢視檢視檢視檢視檢視檢視檢視檢視檢視檢視檢視檢視檢視檢視檢視視檢視視檢視視檢視視視視

```
User: arn:aws:iam::123456789012:role/MyExampleRole is not authorized to perform:
 resource-explorer-2:GetView on resource: arn:aws:resource-explorer-2:us-
east-1:123456789012:view/EC2-Only-View/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111
```

在此情況下，使用該角色的人員必須要求管理員更新角色的權限原則，以允許使用resource-explorer-2:GetView動作存取檢視。

我想要允許外的人員存取我AWS 帳戶的資源管理器資源

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

若要進一步了解，請參閱以下內容：

- 若要了解資源總管是否支援這些功能，請參閱資源 Explorer 如何與 IAM 搭配運作。
- 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。

AWS 資源總管 中的資料保護

AWS 共同的責任模型適用於 AWS 資源總管 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。您負責維護在此基礎設施上託管內容的控制權。您也必須負責您所使用

AWS 服務 的安全組態和管理任務。如需有關資料隱私權的更多相關資訊，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，並設定個人使用者。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 和使用者活動日誌記錄。
- 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 端點的更多相關資訊，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 使用資源總管或其他資源總管時。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。

靜態加密

Resource Explorer 所儲存的資料包括客戶所使用之資源及其相關聯 ARN 的索引清單，以及存取這些資源的檢視。

這些數據在靜態時通過使用 AWS Key Management Service（AWS KMS）對稱加密密鑰進行加密，該密鑰在 Galois 計數器模式（GCM）中使用 256 位密鑰（AES-256-GCM）實現高級加密標準（AES）進行加密。

傳輸中加密

客戶要求和所有關聯的資料會使用稍後傳輸安全性 (TLS) 1.2 或更新版本加密傳輸過程。所有資源總管端點都支援 HTTPS 來加密傳輸中的資料。如需資源總管服務端點的清單，請參閱 AWS 資源總管 AWS 一般參考.

AWS 資源總管 的合規驗證

若要瞭解AWS 服務是否在特定規範遵循方案的範圍內，請參閱規範遵循方案AWS 服務中的。如需一般資訊，請參閱 AWS 合規計劃 。

您可使用 AWS Artifact 下載第三方稽核報告。如需詳細資訊，請參閱《AWS Artifact使用指南》中的〈AWS Artifact的〈下載報告〉。

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

- 安全與合規快速入門指南：這些部署指南討論架構考量，並提供在 AWS 上部署以安全及合規為重心之基準環境的步驟。
- 在 Amazon Web Services 上架構 HIPAA 安全性與合規性 — 本白皮書說明公司如何使用建立符合 HIPAA 資格的應AWS用程式。

> **Note**
>
> 並非所有人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 合規資源：這組手冊和指南可能適用於您的產業和位置。
- AWS Config 開發人員指南中的使用規則評估資源 – AWS Config 可評估資源組態對於內部實務、業界準則和法規的遵循狀況。
- AWS Security Hub：此 AWS 服務可供您檢視 AWS 中的安全狀態，可助您檢查是否符合安全產業標準和最佳實務。

AWS 資源總管 中的恢復能力

。AWSAWS 區域區域提供多個分開且隔離的實際可用區域，並以低延遲、高輸送量和高度備援網路連線相互連結。透過可用區域，您可以設計與操作的應用程式和資料庫，在可用區域之間自動容錯移轉而不會發生中斷。可用區域的可用性、容錯能力和擴充能力，均較單一或多個資料中心的傳統基礎設施還高。

如需 AWS 區域 與可用區域的詳細資訊，請參閱AWS全球基礎架構。

AWS 資源總管 中的基礎設施安全

作為一種受管服務，AWS 資源總管 受 AWS 全球網路安全保護。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。

您使用AWS已發佈的 API 呼叫，以透過網路存取資源總管。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。

如需更多相關資訊AWS全球網路安全程序，請參閱亞馬遜網絡服務：安全流程概述白皮書。

監控 AWS 資源總管

Sport Sport、AWS。AWS 資源總管 AWSResource Exploport Exploport Explorer，：

- AWS CloudTrail 擷取您 AWS 帳戶 發出或代表發出的 API 呼叫和相關事件，並傳送記錄檔案至您指定的 Amazon S3 儲存貯體。您可以找出哪些使用者和帳戶呼叫 AWS、發出呼叫的來源 IP 地址，以及呼叫的發生時間。如需詳細資訊，請參閱 使用 AWS CloudTrail 記錄 AWS 資源總管 API 呼叫 及《AWS CloudTrail 使用者指南》。

使用 AWS CloudTrail 記錄 AWS 資源總管 API 呼叫

AWS 資源總管已與整合AWS CloudTrail，該服務提供由使用者、角色或資源總管AWS 服務中的服務所採取之動作的記錄。 CloudTrail 擷取資源瀏覽器的所有 API 呼叫當作事件。擷取的呼叫包括從資源總管主控台進行的呼叫，以及對資源總管 API 操作的程式碼呼叫。

如果您建立追蹤記錄，就可以持續傳送 CloudTrail 事件至 Amazon S3 儲存貯體，包括資源 Explorer 的事件。追蹤是一種組態，能讓事件以日誌檔案的形式交付到您指定的 Amazon S3 儲存貯體。如果您不設定追蹤記錄，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。您可以使用收集的資訊來 CloudTrail判斷向資源 Explorer 發出的請求，以及發出請求的 IP 地址、提出請求的對象、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。

資源總管資訊 CloudTrail

CloudTrail 當您建立帳戶AWS 帳戶時，系統即會在中啟用。此外，資源總管中發生活動時，系統便會將該活動記錄至 CloudTrail 事件，並將其他AWS 服務事件記錄到事件歷史記錄中。您可以檢視、搜尋和下載 AWS 帳戶 的最新事件。如需詳細資訊，請參閱使用 CloudTrail 事件歷程記錄檢視事件。

> **Important**
>
> 您可以通過搜索事件源 = 資源瀏覽器 -2.amazonaws.com 找到所有資源瀏覽器事件

若要持續記錄您的事件AWS 帳戶，包括資源總管的事件，請建立追蹤。線索能讓 CloudTrail 將日誌檔案交付至 Amazon S3 儲存貯體。依預設，當您在主控台中建立追蹤時，該追蹤會套用至所有的 AWS 區域。該追蹤會記錄來自 AWS 分割區中所有區域的事件，並將日誌檔案交付到您指定的 Amazon S3

儲存貯體。此外，您還能設定其他服務，AWS 服務以進一步分析和處理 CloudTrail 日誌中收集的事件資料。如需詳細資訊，請參閱《AWS CloudTrail 使用者指南》中的以下主題：

- 建立 AWS 帳戶 的追蹤
- AWS與 CloudTrail 日誌的服務整合
- 設定的 Amazon SNS 通知 CloudTrail
- 從多個區域接收 CloudTrail 日誌檔案
- 從多個帳戶接收 CloudTrail 日誌檔案

系統會記錄所有資源總管動作， CloudTrail 並記錄在 AWS 資源總管API 參考中。例如，呼叫`CreateIndex`、`DeleteIndex`和`UpdateIndex`動作會在 CloudTrail 記錄檔中產生項目。

每個事件或日誌項目都會包含可幫助您確定請求發出者的資訊。

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

> **Important**
>
> 基於安全理由`TagsFilters`，系統會從 CloudTrail 軌跡項目編輯所有、和`QueryString`值。

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

了解資源總管日誌檔案項目

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

主題

- CreateIndex
- DeleteIndex

- UpdateIndexType
- 搜尋
- CreateView
- DeleteView
- DisassociateDefaultView

CreateIndex

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


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAEXAMPLEEXAMPLE:botocore-session-166EXAMPLE",
        "arn": "arn:aws:sts::123456789012:assumed-role/cli-role/botocore-
session-166EXAMPLE",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAEXAMPLEEXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/cli-role",
                "accountId": "123456789012",
                "userName": "cli-role"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-08-23T19:13:59Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-08-23T19:13:59Z",
    "eventSource": "resource-explorer-2.amazonaws.com",
    "eventName": "CreateIndex",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "10.24.34.15",
    "userAgent": "aws-cli/2.7.14 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/
resource-explorer-2.create-index",
```

```
    "requestParameters": {
        "ClientToken": "792ee665-58af-423c-bfdb-d7c9aEXAMPLE"
    },
    "responseElements": {
        "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
        "State": "CREATING",
        "CreatedAt": "2022-08-23T19:13:59.775Z"
    },
    "requestID": "a193afe9-17ff-4f30-ae0a-73bb0EXAMPLE",
    "eventID": "2ec50598-4de6-474d-bd0e-f5c00EXAMPLE",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

DeleteIndex

以下範例顯示的是展示DeleteIndex動作的 CloudTrail 長項目。

> **Note**
>
> 此動作也會以非同步方式刪除該區域中帳戶的所有檢視，因此每個已刪除的檢視都會產生DeleteView事件。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAEXAMPLEEXAMPLE:My-Role-Name",
        "arn": "arn:aws:sts::123456789012:assumed-role/My-Admin-Role/My-Delegated-
Role",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAEXAMPLEEXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/My-Admin-Role",
```

```
                "accountId": "123456789012",
                "userName": "My-Admin-Role"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-08-23T18:33:06Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-08-23T19:04:06Z",
    "eventSource": "resource-explorer-2.amazonaws.com",
    "eventName": "DeleteIndex",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "10.24.34.15",
    "userAgent": "aws-cli/2.7.14 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/
resource-explorer-2.delete-index",
    "requestParameters": {
        "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
    },
    "responseElements": {
        "Access-Control-Expose-Headers": "x-amzn-RequestId,x-amzn-ErrorType,x-amzn-
ErrorMessage,Date",
        "State": "DELETING",
        "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
    },
    "requestID": "d7d80bd2-cd2d-47fb-88d6-5133aEXAMPLE",
    "eventID": "675eab39-c514-4d32-989d-0ea98EXAMPLE",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

UpdateIndexType

下列範例顯示示範將索引從類型LOCAL升級為的UpdateIndexType動作的 CloudTrail 記錄項目AGGREGATOR。

```
{
```

```
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAEXAMPLEEXAMPLE:botocore-session-1661282039",
        "arn": "arn:aws:sts::123456789012:assumed-role/cli-role/botocore-
session-1661282039",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAEXAMPLEEXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/cli-role",
                "accountId": "123456789012",
                "userName": "cli-role"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-08-23T19:13:59Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-08-23T19:21:18Z",
    "eventSource": "resource-explorer-2.amazonaws.com",
    "eventName": "UpdateIndexType",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "10.24.34.15",
    "userAgent": "aws-cli/2.7.14 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/
resource-explorer-2.update-index-type",
    "requestParameters": {
        "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
        "Type": "AGGREGATOR"
    },
    "responseElements": {
        "Type": "AGGREGATOR",
        "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
        "LastUpdatedAt": "2022-08-23T19:21:17.924Z",
        "State": "UPDATING"
    },
    "requestID": "a145309d-df14-4c2e-a9f6-8ed45EXAMPLE",
    "eventID": "ed33ab96-f5c6-4a77-a69a-8585aEXAMPLE",
```

```
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

搜尋

以下範例顯示的是展示Search動作的 CloudTrail 日誌項目。

> **Note**
>
> 基於安全理由，系統會在 CloudTrail 追蹤項目中編輯Filters、和QueryString參數的所有參照。Tag

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAEXAMPLEEXAMPLE:botocore-session-1661282039",
        "arn": "arn:aws:sts::123456789012:assumed-role/cli-role/botocore-
session-1661282039",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAEXAMPLEEXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/cli-role",
                "accountId": "123456789012",
                "userName": "cli-role"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-08-23T19:13:59Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-08-03T16:50:11Z",
```

```
    "eventSource": "resource-explorer-2.amazonaws.com",
    "eventName": "Search",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "10.24.34.15",
    "userAgent": "aws-cli/2.7.14 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/
resource-explorer-2.search",
    "requestParameters": {
        "QueryString": "***"
    },
    "responseElements": null,
    "requestID": "22320db5-b194-446f-b9f4-e603bEXAMPLE",
    "eventID": "addb3bca-0c41-46bf-a5e6-42299EXAMPLE",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

CreateView

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

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAEXAMPLEEXAMPLE:botocore-session-1661282039",
        "arn": "arn:aws:sts::123456789012:assumed-role/cli-role/botocore-
session-1661282039",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAEXAMPLEEXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/cli-role",
                "accountId": "123456789012",
                "userName": "cli-role"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-08-23T19:13:59Z",
```

```
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-01-20T21:54:48Z",
    "eventSource": "resource-explorer-2.amazonaws.com",
    "eventName": "CreateView",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "10.24.34.15",
    "userAgent": "aws-cli/2.7.14 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/
resource-explorer-2.create-view",
    "requestParameters": {
        "ViewName": "CTTagsTest",
        "Tags": "***"
    },
    "responseElements": {
        "View": {
            "Filters": "***",
            "IncludedProperties": [],
            "LastUpdatedAt": "2023-01-20T21:54:48.079Z",
            "Owner": "123456789012",
            "Scope": "arn:aws:iam::123456789012:root",
            "ViewArn": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/
CTTest/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
        }
    },
    "requestID": "b22d8ced-4905-42c4-b1aa-ef713EXAMPLE",
    "eventID": "f62e339f-1070-41a8-a6ec-12491EXAMPLE",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

DeleteView

下列範例顯示 CloudTrail 記錄項目，其中示範由於相同作業而自DeleteView動啟動動DeleteIndex作時可能發生的事件AWS 區域。

> **Note**
>
> 如果已刪除的檢視是 [區域] 的預設檢視，此動作也會非同步取消檢視作為預設檢視的關聯性。這會產生一個DisassociateDefaultView事件。


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAEXAMPLEEXAMPLE:botocore-session-1661282039",
        "arn": "arn:aws:sts::123456789012:assumed-role/cli-role/botocore-
session-1661282039",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAEXAMPLEEXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/cli-role",
                "accountId": "123456789012",
                "userName": "cli-role"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-08-23T19:13:59Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-09-16T19:33:27Z",
    "eventSource": "resource-explorer-2.amazonaws.com",
    "eventName": "DeleteView",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "10.24.34.15",
    "userAgent": "aws-cli/2.7.14 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/
resource-explorer-2.delete-view",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "cd174d1e-0a24-4b47-8b67-d024aEXAMPLE",
    "readOnly": false,
    "resources": [{
```

```
        "accountId": "334026708824",
        "type": "AWS::ResourceExplorer2::View",
        "ARN": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/
CTTest/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
    }],
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

DisassociateDefaultView

下列範例顯示的 CloudTrail 記錄項目會示範由於目前預設檢視上的DisassociateDefaultView作業而自動啟動動DeleteView作時可能發生的事件。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "accountId": "123456789012",
        "invokedBy": "resource-explorer-2.amazonaws.com"
    },
    "eventTime": "2022-09-16T19:33:26Z",
    "eventSource": "resource-explorer-2.amazonaws.com",
    "eventName": "DisassociateDefaultView",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "10.24.34.15",
    "userAgent": "aws-cli/2.7.14 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/
resource-explorer-2.disassociate-default-view",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "d8016cb1-5c23-4ea4-bda2-70b03EXAMPLE",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

建立資源總管資源 CloudFormation

AWS 資源總管已整合AWS CloudFormation，這項服務可協助您建AWS資源的模型和設定。這項整合可協助您建資的資源和基礎設施的時間。您可以建立一個範本，描述所有您想要的 AWS 資源，CloudFormation 就會為您佈建和設定那些資源。資源的範例包括索引、檢視表或預設檢視表的指定AWS 區域。

當您使用時CloudFormation，您可以重複使用您的範本，以便重複且一致地設定您的資源資源。只需描述一次您的資源，即可在多個和區域內反復佈建相同AWS 帳戶的資源。

使用AWS CloudFormation將資源總管部署到 AWS Organizations

您可以使AWS CloudFormationStackSets用將資源總管部署到組織中的所有帳號。當您在組織中新增或建立成員帳戶時，StackSets可以自動為每個新成員帳戶設定每個AWS 區域成員帳戶中的索引，包括您在其中指定的彙總索引。如需相關指示，請參閱將資源總管部署到組織中的帳號。

資源總管和CloudFormation範本

若要佈建和設定資源總管與相關服務的資源，您必須了解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 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 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？。

資源總管支援在中建以下資源類型CloudFormation：

- 索引 — 在區域中建立索引，並開啟該區域中的資源總管。您可以指定索引是本機索引，也可以是的彙總索引AWS 帳戶。如需詳細資訊，請參閱 在中打開資源瀏覽器AWS 區域以索引您的資源 及 透過建立彙總索引開啟跨區域搜尋。
- 檢視 — 建立可決定使用者執行搜尋時可顯示哪些結果的檢視。每個搜索操作都必須指定一個視圖。您必須授予使用者使用您希望他們存取的資源。如需詳細資訊，請參閱管理資源總管檢視以提供搜尋存取權。

> **Note**
>
> 您必須先在 [區域] 中建立索引，然後才能在同一個 [區域] 中建立檢視表。如果您建立索引和檢視做為相同堆疊的一部分，請使用檢視表上的DependsOn屬性 (如下列範例範本所示)，以確保首先建立索引。

- DefaultViewAssociation— 將指定的檢視指定為其 [區域] 中的預設檢視。當使用者沒有明確指定要用於搜尋作業的檢視時，Resource Explorer 會嘗試使用與使用者執行搜尋的區域相關聯的預設檢視。如需詳細資訊，請參閱 在中設定預設檢視AWS 區域

下列範例說明如何在同一個 [區域] 中建立一個索引和檢視表，並將檢視設定為 [區域] 的預設值。

YAML

```
Description: >-
  Sample CFN Stack setting up Resource Explorer with an aggregator index and a default
 view
Resources:
  SampleIndex:
    Type: 'AWS::ResourceExplorer2::Index'
    Properties:
      Type: AGGREGATOR
      Tags:
        Purpose: ResourceExplorer Sample CFN Stack
  SampleView:
    Type: 'AWS::ResourceExplorer2::View'
    Properties:
      ViewName: mySampleView
      IncludedProperties:
        - Name: tags
      Tags:
        Purpose: ResourceExplorer Sample CFN Stack
    DependsOn: SampleIndex
  SampleDefaultViewAssociation:
    Type: 'AWS::ResourceExplorer2::DefaultViewAssociation'
    Properties:
      ViewArn: !Ref SampleView
```

JSON

```
{
    "Description": "Sample CFN Stack setting up Resource Explorer with an aggregator
 index and a default view ",
    "Resources": {
        "SampleIndex": {
            "Type": "AWS::ResourceExplorer2::Index",
            "Properties": {
                "Type": "AGGREGATOR",
```

```
                "Tags": {
                    "Purpose": "ResourceExplorer Sample Stack"
                }
            }
        },
        "SampleView": {
            "Type": "AWS::ResourceExplorer2::View",
            "Properties": {
                "ViewName": "mySampleView",
                "IncludedProperties": [
                    {
                        "Name": "tags"
                    }
                ],
                "Tags": {
                    "Purpose": "ResourceExplorer Sample CFN Stack"
                }
            },
            "DependsOn": "SampleIndex"
        },
        "SampleDefaultViewAssociation": {
            "Type": "AWS::ResourceExplorer2::DefaultViewAssociation",
            "Properties": {
                "ViewArn": {
                    "Ref": "SampleView"
                }
            }
        }
    }
}
```

如需詳細資訊，包括資源總管索引和檢視的 JSON 和 YAML 範本範例，請參閱《AWS CloudFormation使用者指南》中的 ResourceExplorer2 個資源類型參考。

進一步了解 AWS CloudFormation

若要進一步了解 CloudFormation，請參閱下列資源：

- AWS CloudFormation
- 《AWS CloudFormation 使用者指南》https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/Welcome.html

- 《AWS CloudFormation 命令列介面使用者指南》https://docs.aws.amazon.com/cloudformation-cli/latest/userguide/what-is-cloudformation-cli.html

資源 Ex器

如果您在使用 Cost 時遇到問題，請參閱本節中的主題。另請參閱疑難排解AWS 資源總管權本指南的「安全性」一節。

主題

一般問題

主題

我收到了資源資源管理器的鏈接，但是當我打開它時，控制台只顯示一個錯誤。

某些協力廠商工具會產生資源總管中頁面的連結 URL。在某些情況下，這些 URL 不包含將控制台定向到特定的參數AWS 區域。如果您開啟此類連結，資源總管主控台不會告知要使用哪個區域，而且預設會使用使用者登入的最後一個 [區域]。如果使用者沒有存取該區域中 Resource Explorer 的權限，則主控台會嘗試使用美國東部 (維吉尼亞北部) (us-east-1) 區域，或者如果主控台無法連線，則主控台會嘗試使用美國西部 (奧勒岡us-west-2) ()us-east-1。

如果使用者沒有存取這些區域中的任何一個區域中的許可，資源 Ex器會傳回錯誤。

您可以確保所有使用者都具有下列權限，以避免發生此問題：

- ListIndexes— 沒有特定的資源; 使用*.
- GetIndex用於帳戶中創建的每個索引的 ARN。若要避免在刪除並重新建立索引時必須重做權限原則，建議您使用*。

實現此目標的最低政策看起來像這個範例：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "resource-explorer-2:GetIndex",
                "resource-explorer-2:ListIndexes",
            ],
            "Resource": "*"
        }
    ]
}
```

或者，您可以考慮將AWS受管理的權限附加AWSResourceExplorerReadOnlyAccess到需要使用資源總管的所有使用者。這將授予這些必要權限，以及所需的權限，請參閱「地區」中的可用視圖並使用這些視圖進行搜索。

為什麼控制台中的統一搜索在我的 CloudTrail 日誌中導致「訪問被拒絕」錯誤？

中的統一搜尋AWS Management Console可讓主參與者從中的任何頁面進行搜尋AWS Management Console。如果「資源總管」已開啟並設定為支援統一搜尋，則結果可能會包含主參與者帳戶中的資源。每當您開始在統一搜索欄中輸入時，統一搜索都會嘗試調用resource-explorer-2:ListIndexes操作以檢查其是否可以在結果中包含用戶帳戶的資源。

整合搜尋會使用目前登入的使用者權限來執行此檢查。如果該使用者沒有在附加AWS Identity and Access Management (IAM) 權限政策中resource-explorer-2:ListIndexes授與呼叫的權限，則檢查會失敗。該失敗會新增為 CloudTrail 記錄檔中的Access denied項目。

此 CloudTrail 記錄項目具有下列特性：

- 事件來源：resource-explorer-2.amazonaws.com
- 活動名稱：ListIndexes
- 錯誤代碼：403（訪問被拒絕）

下列AWS受管理的原則包含呼叫權限resource-explorer-2:ListIndexes。如果您將下列任何一項指派給主參與者，或任何其他包含此權限的原則，則不會發生此錯誤：

- AWSResourceExplorerReadOnlyAccess
- AWSResourceExplorerFullAccess
- ReadOnlyAccess
- ViewOnlyAccess

疑難排解資源總管設定和組態問題

使用此處的資訊，來協助您針對在初始設定或設定時所可能發生的問題，進行故障診斷與排除AWS 資源總管。

主題

當我向資源資源管理器發出請求時，出現「存取遭拒」訊息

- 確定您擁有呼叫所請求之動作和資源的許可。管理員可以透過將AWS Identity and Access Management (IAM) 權限政策指派給您的 IAM 主體 (例如角色、群組或使用者) 來授與許可。

  若要提供存取權，請新增許可到您的使用者、群組或角色：

  - AWS IAM Identity Center 中的使用者和群組：

    建立許可集合。請遵循《AWS IAM Identity Center 使用者指南》的建立許可集合中的指示。

  - 透過身分提供者在 IAM 中管理的使用者：

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

  - IAM 使用者：
    - 建立您的使用者可擔任的角色。請遵循《IAM 使用者指南》的為 IAM 使用者建立角色中的指示。
    - (不建議) 將政策直接連接至使用者，或將使用者新增至使用者群組。請遵循《IAM 使用者指南》的新增許可到使用者 (主控台)中的指示。

  該策略必須允許您`Resource`要訪問的請`Action`求。

如果授予這些許可的政策內容中包含了任何條件，例如 time-of-day 或 IP 地址的限制，則當您傳送請求時，也必須滿足這些要求。關於檢視或修改 IAM 主體的政策方面的相關資訊，請參閱 IAM 使用者指南中的管理 IAM 政策。

- 如果您是手動簽署 API 請求 (而未使用AWS開發套件)，請確認您已正確地簽署請求。

當我使用臨時安全憑證來發出請求時，出現「存取遭拒」訊息

- 確認您用來提出請求的 IAM 主體擁有正確的許可。臨時安全憑證的許可衍生自 IAM 中定義的主體，因此許可僅限於授予主體的範圍。關於臨時安全憑證許可的決定方式，詳細資訊請參閱 IAM 使用者指南中的控管臨時安全憑證的許可。
- 確認您的請求正確簽署且請求的格式也正確。如需詳細資訊，請參閱所選 SDK 的工具組文件，或在 IAM 使用者指南中使用臨時登入資料搭配AWS資源。
- 確認您的臨時安全憑證並未過期。如需詳細資訊，請參閱 IAM 使用者指南中的要求臨時安全登入資料。

疑難排解資源瀏覽器搜尋

使用此處的資訊可協助您診斷和修正使用資源總管搜尋資源時可能發生的常見錯誤。

主題

為什麼我的資源瀏覽器搜索結果中缺少某些資源？

下列清單提供部分資源可能無法如預期般顯示在搜尋結果中的原因：

初始索引未完成

在中初次開啟資源總管之後AWS 區域，可能需要長達 36 小時的時間才能完成索引和複寫至彙總器索引。請稍後再嘗試搜尋。

資源是新的

資源總管探索新資源並新增至本機索引可能需要幾分鐘的時間。請在幾分鐘後再試一次。

一個區域中新資源的相關資訊尚未傳播至彙總索引

可能需要一些時間才能取得有關在某個區域中發現的新資源的詳細資訊，以便在自己的區域中建立索引，然後複寫到帳戶的彙總器索引。只有在複寫完成後，新資源才會出現在跨區域搜尋結果中。請稍後再嘗試搜尋。

包含資源的區域未開啟資源總管

您的管理員會決定「AWS 區域資源總管」可以在哪些中操作。[設定] 頁面會顯示哪些區域已開啟 [資源總管] 並包含索引。如果包含您資源的區域未開啟，請要求您的管理員開啟該區域中的資源總管。

資源存在於不同的區域，且搜尋的區域不包含彙總器索引

您只能使用「地區」中包含彙總索引的檢視，來搜尋帳戶中所有區域的資源。在任何其他區域中進行搜尋，只會傳回您執行搜尋之「區域」的資源。

檢視上的篩選器會排除該資源

每個檢視都可以在組態中包含篩選器，以限制哪些結果可以包含在使用該檢視所產生的搜尋結果中。確保您要尋找的資源與您用於搜尋的檢視中的篩選條件相符。如需篩選器的詳細資訊，請參閱篩選條件。如需視圖的詳細資訊，請參閱關於資源總管。

資源總管不支援資源類型

資源總管不支援某些資源類型。如需詳細資訊，請參閱您可以使用資源總管搜尋的資源類型。

控制台區域中未配置索引或視圖

如果使用 Widget 的主控台所預期的區域中未設定索引或檢視，您將不會看到預期的結果。如需詳細資訊，請參閱 透過建立彙總索引開啟跨區域搜尋 和 關於資源總管。

您的檢視不包含標籤

資源總管小器具需要標籤。如果您的檢視不包含標籤，資源就不會包含在結果中。如需詳細資訊，請參閱對檢視新增標籤。

您的搜尋使用錯誤的搜尋查詢語法

在資源總管中搜尋對此服務而言是唯一的。如果沒有正確的語法，您將找不到所期望的資源。如需詳細資訊，請參閱資源總管的搜尋查詢語法參考。

您最近標記了您的資源

標記資源之後，資源會有 30 秒的延遲時間才會顯示在搜尋結果中。

資源類型不支援標籤篩選

如果資源類型不支援標籤篩選器，它們將不會顯示在資源總管小器具中。不支援標籤篩選的資源類型有：

- cloudfront:cache-policy
- cloudfront:origin-access-identity
- cloudfront:function
- cloudfront:origin-request-policy
- cloudfront:realtime-log-config
- cloudfront:response-headers-policy
- cloudwatch:dashboard
- docdb:globalcluster
- elasticache:globalreplicationgroup
- iam:group
- lambda:code-signing-config
- lambda:event-source-mapping
- ssm:windowtarget
- ssm:windowtask
- rds:auto-backup
- rds:global-cluster
- s3:accesspoint

為什麼我的資源沒有出現在主控台的統一搜尋結果中？

統一的搜索結果可在每個AWS Management Console頁面頂部的搜索欄中找到。但是，只有在下列組態選項完成之後，搜尋才會傳回符合搜尋結果中查詢的資源：

- 帳戶中的其中一個區域中必須有彙總索引。
- 「地區」中必須有包含彙總器索引的預設檢視。
- 所有主體 (IAM 角色和使用者) 都必須具有使用該預設檢視進行搜尋的權限。

為什麼控制台和資源瀏覽器中的統一搜索有時會產生不同的結果？

統一的搜索結果可在每個AWS Management Console頁面頂部的搜索欄中找到。當您使用統一搜尋時，統一的搜尋程序會自動在您在查詢字串中輸入的第一個字詞結尾插入萬用字元 (*)。該萬用字元在統一的搜尋方塊中不可見，但確實會影響結果。

> **Important**
>
> 統一搜尋會在字串中第一個關鍵字的結尾自動插入萬用字元 (*) 運算子。這意味著統一的搜索結果包括匹配以指定關鍵字開頭的任何字符串的資源。
> [資源總管] 主控台中 [資源搜尋] 頁面上的 [查詢] 文字方塊執行的搜尋不會自動附加萬用字元。您可以在搜尋字串中的任何字詞之後*手動插入。

我需要哪些權限才能搜尋資源？

若要搜尋，您必須擁有在您呼叫作業之「區域」中的檢視表上執行下列兩項作業的權限：

- `resource-explorer-2:GetView`
- `resource-explorer-2:Search`

您可以在指派給 IAM 主體的政策中新增類似下列範例的陳述式。

```
        {
            "Effect": "Allow",
            "Action": [
                "resource-explorer-2:GetView",
                "resource-explorer-2:Search"
            ],
            "Resource": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/My-
View-Name/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
        }
```

您可以使用包含萬用字元 () 的 ARN 取代特定檢視的 Amazon 資源編號 (ARN*)，以授與所有相符檢視的權限。

如果您未在要求中指定檢視，Resource Explorer 會自動使用您提出要求之地區的預設檢視。如果您沒有使用預設檢視的權限，請洽詢您的系統管理員。

> **Note**
>
> 即使您在 Resource Explorer 搜尋查詢的結果中看到資源，您仍需要資源本身的權限才能與該資源互動。

您可以使用資源總管搜尋的資源類型

主題

下表列出在中搜尋所支援的資源類型 AWS 資源總管。

> **備註**
>
> - 某些資源類型由 Amazon 資源名稱 (ARN) 字串識別，這些字串與其他資源類型共用通用格式。發生這種情況時，資源總管可以報告該其他資源類型的資源。如需受此問題影響的資源類型清單，請參閱顯示為其他類型的資源類型。
> - 目前無法使用附加至 AWS Identity and Access Management (IAM) 資源的標籤 (例如角色或使用者) 進行搜尋。
> - 如果您擁有某些資源的加密存取權，則資源總管無法探索它們。您不會在搜尋結果中看到這些資源。

支援的服務和資源類型

支援 AWS 服務

- Amazon API Gateway
- AWS App Runner
- Amazon AppStream 2.0
- AWS AppSync
- Amazon Athena
- AWS Backup
- AWS Batch
- AWS CloudFormation

- Amazon CloudFront
- AWS CloudTrail
- Amazon CloudWatch
- Amazon CloudWatch 顯然
- Amazon CloudWatch 日誌
- AWS CodeArtifact
- AWS CodeBuild
- AWS CodeCommit
- Amazon CodeGuru 分析器
- AWS CodePipeline
- AWS CodeConnections
- Amazon Cognito
- Amazon Connect
- Amazon Connect Wisdom
- Amazon Detective
- Amazon DynamoDB
- EC2 Image Builder
- Amazon ECR Public
- AWS Elastic Beanstalk
- Amazon ElastiCache
- Amazon Elastic Compute Cloud (Amazon EC2)
- Amazon Elastic Container Registry
- Amazon Elastic Container Service
- Amazon Elastic File System
- Elastic Load Balancing
- AWS Elemental MediaPackage
- AWS Elemental MediaTailor
- Amazon EMR Serverless
- Amazon EventBridge

- AWS Fault Injection Service
- Amazon Forecast
- Amazon Fraud Detector
- Amazon GameLift
- AWS Global Accelerator
- AWS Glue
- AWS Glue DataBrew
- AWS Identity and Access Management
- Amazon Interactive Video Service
- AWS IoT
- AWS IoT Analytics
- AWS IoT Events
- AWS IoT Greengrass Version 1
- AWS IoT SiteWise
- AWS IoT TwinMaker
- AWS Key Management Service
- Amazon Kinesis
- Amazon 數據 Firehose
- Amazon Kinesis Video Streams
- AWS Lambda
- Amazon Lex
- Amazon Location Service
- Amazon Lookout for Metrics
- Amazon Lookout for Vision
- Amazon Managed Service for Apache Flink
- Amazon Managed Service for Prometheus
- Amazon Managed Service for Prometheus
- Amazon Managed Streaming for Apache Kafka
- AWS Migration Hub Refactor Spaces

- AWS Network Firewall
- AWS Network Manager
- Amazon OpenSearch 服務
- AWS Panorama
- Amazon Personalize
- AWS Private Certificate Authority
- Amazon QLDB
- Amazon Redshift
- Amazon Rekognition
- Amazon Relational Database Service (Amazon RDS)
- AWS Resilience Hub
- AWS Resource Groups
- AWS 資源總管
- Amazon Route 53
- Amazon Route 53 Recovery Readiness
- Amazon Route 53 Resolver
- Amazon SageMaker
- AWS Secrets Manager
- AWS Service Catalog
- Amazon Simple Notification Service
- Amazon Simple Queue Service
- Amazon Simple Storage Service (Amazon S3)
- AWS Step Functions
- AWS Systems Manager
- AWS Verified Access
- AWS Wavelength

Amazon API Gateway

- `apigateway:restapi`

AWS App Runner

- apprunner:vpcconnector

Amazon AppStream 2.0

- appstream:appblock
- appstream:application
- appstream:fleet
- appstream:stack

AWS AppSync

- appsync:apis

Amazon Athena

- athena:datacatalog
- athena:workgroup

AWS Backup

- backup:backupplan

AWS Batch

- batch:computeenvironment
- batch:jobqueue
- batch:schedulingpolicy

AWS CloudFormation

- cloudformation:stack

- cloudformation:stackset

Amazon CloudFront

- cloudfront:cache-policy
- cloudfront:distribution
- cloudfront:function
- cloudfront:fieldlevelencryptionconfig
- cloudfront:fieldlevelencryptionprofile
- cloudfront:origin-access-identity
- cloudfront:originaccesscontrol
- cloudfront:origin-request-policy
- cloudfront:realtime-log-config
- cloudfront:response-headers-policy

AWS CloudTrail

- cloudtrail:trail

Amazon CloudWatch

- cloudwatch:alarm
- cloudwatch:dashboard
- cloudwatch:insight-rule
- cloudwatch:metric-stream
- evidently:project

Amazon CloudWatch 顯然

- evidently:project-experiment
- evidently:project-feature
- evidently:project-launch

Amazon CloudWatch 日誌

- logs:destination
- logs:log-group

AWS CodeArtifact

- codeartifact:domain
- codeartifact:repository

AWS CodeBuild

- codebuild:project

AWS CodeCommit

- codecommit:repository

Amazon CodeGuru 分析器

- codeguru-profiler:profilingGroup

AWS CodePipeline

- codepipeline:pipeline

AWS CodeConnections

- codestarconnections:connect

Amazon Cognito

- cognito:identitypool

- cognito:userpool

Amazon Connect

- appintegrations:eventintegration

Amazon Connect Wisdom

- wisdom:assistant
- wisdom:association
- wisdom:knowledge-base

Amazon Detective

- detective:graph

Amazon DynamoDB

- dynamodb:table

EC2 Image Builder

- imagebuilder:component
- imagebuilder:containerrecipe
- imagebuilder:distributionconfiguration
- imagebuilder:image
- imagebuilder:imagepipeline
- imagebuilder:imagerecipe
- imagebuilder:infrastructureconfiguration

Amazon ECR Public

- ecrpublic:repository

AWS Elastic Beanstalk

- elasticbeanstalk:application
- elasticbeanstalk:applicationversion
- elasticbeanstalk:configurationtemplate
- elasticbeanstalk:environment

Amazon ElastiCache

- elasticache:cluster
- elasticache:globalreplicationgroup
- elasticache:parametergroup
- elasticache:replicationgroup
- elasticache:reserved-instance
- elasticache:snapshot
- elasticache:subnetgroup
- elasticache:user
- elasticache:usergroup

Amazon Elastic Compute Cloud (Amazon EC2)

- ec2:capacity-reservation
- ec2:capacity-reservation-fleet
- ec2:client-vpn-endpoint
- ec2:customer-gateway
- ec2:dedicated-host
- ec2:dhcp-options
- ec2:egress-only-internet-gateway
- ec2:elastic-gpu
- ec2:elastic-ip

- ec2:fleet
- ec2:fpga-image
- ec2:host-reservation
- ec2:image
- ec2:instance
- ec2:instance-event-window
- ec2:internet-gateway
- ec2:ipam
- ec2:ipam-pool
- ec2:ipam-scope
- ec2:ipv4pool-ec2
- ec2:key-pair
- ec2:launch-template
- ec2:natgateway
- ec2:network-acl
- ec2:network-insights-access-scope
- ec2:network-insights-access-scope-analysis
- ec2:network-insights-analysis
- ec2:network-insights-path
- ec2:network-interface
- ec2:placement-group
- ec2:prefix-list
- ec2:reserved-instances
- ec2:route-table
- ec2:security-group
- ec2:security-group-rule
- ec2:snapshot
- ec2:spot-fleet-request
- ec2:spot-instances-request

- ec2:subnet
- ec2:subnet-cidr-reservation
- ec2:traffic-mirror-filter
- ec2:traffic-mirror-filter-rule
- ec2:traffic-mirror-session
- ec2:traffic-mirror-target
- ec2:transit-gateway
- ec2:transit-gateway-attachment
- ec2:transit-gateway-connect-peer
- ec2:transit-gateway-multicast-domain
- ec2:transit-gateway-policy-table
- ec2:transit-gateway-route-table
- ec2:transitgatewayroutetableannouncement
- ec2:volume
- ec2:vpc
- ec2:vpc-endpoint
- ec2:vpc-flow-log
- ec2:vpc-peering-connection
- ec2:vpn-connection
- ec2:vpn-gateway

Amazon Elastic Container Registry

- ecr:repository

Amazon Elastic Container Service

- ecs:cluster
- ecs:container-instance
- ecs:service

- ecs:task
- ecs:task-definition
- ecs:task-set

Amazon Elastic File System

- efs:filesystem
- efs:accesspoint

Elastic Load Balancing

- elasticloadbalancing:listener
- elasticloadbalancing:listener-rule
- elasticloadbalancing:listener-rule/app
- elasticloadbalancing:listener/app
- elasticloadbalancing:listener/net
- elasticloadbalancing:loadbalancer
- elasticloadbalancing:loadbalancer/app
- elasticloadbalancing:loadbalancer/net
- elasticloadbalancing:targetgroup

AWS Elemental MediaPackage

- mediapackage:channel
- mediapackage:originendpoint
- mediapackage-vod:packaging-configurations
- mediapackage-vod:packaging-groups

AWS Elemental MediaTailor

- mediatailor:playbackConfiguration

Amazon EMR Serverless

- emr-serverless:applications

Amazon EventBridge

- events:event-bus
- events:rule

AWS Fault Injection Service

- fis:experimenttemplate

Amazon Forecast

- forcast:dataset
- forcast:dataset-group

Amazon Fraud Detector

- frauddetector:detector
- frauddetector:entity-type
- frauddetector:event-type
- frauddetector:label
- frauddetector:outcome
- frauddetector:variable

Amazon GameLift

- gamelift:alias

AWS Global Accelerator

- globalaccelerator:accelerator
- globalaccelerator:accelerator-listener
- globalaccelerator:accelerator-listener-endpoint-group

AWS Glue

- glue:database
- glue:job
- glue:table
- glue:trigger

AWS Glue DataBrew

- databrew:dataset
- databrew:recipe
- databrew:ruleset

AWS Identity and Access Management

- iam:group
- iam:instance-profile
- iam:oidc-provider
- iam:policy
- iam:role
- iam:saml-provider
- iam:server-certificate
- iam:user
- iam:virtualmfadevice

Amazon Interactive Video Service

- ivs:channel
- ivs:streamkey

AWS IoT

- iot:authorizer
- iot:jobtemplate
- iot:mitigationaction
- iot:policy
- iot:provisioningtemplate
- iot:rolealias
- iot:securityprofile
- iot:thing
- iot:topicrule

AWS IoT Analytics

- iotanalytics:channel
- iotanalytics:dataset
- iotanalytics:datastore
- iotanalytics:pipeline

AWS IoT Events

- iotevents:alarmModel
- iotevents:detectorModel
- iotevents:input

AWS IoT Greengrass Version 1

- greengrass:components
- greengrass:groups

AWS IoT SiteWise

- iotsitewise:asset
- iotsitewise:assetmodel
- iotsitewise:gateway

AWS IoT TwinMaker

- iottwinmaker:workspace
- iottwinmaker:workspace-component-type
- iottwinmaker:workspace-entity

AWS Key Management Service

- kms:key

Amazon Kinesis

- kinesis:stream

Amazon 數據 Firehose

- kinesisfirehose:deliverystream

Amazon Kinesis Video Streams

- kinesisvideo:stream

AWS Lambda

- lambda:code-signing-config
- lambda:event-source-mapping
- lambda:function

Amazon Lex

- lex:bot

Amazon Location Service

- geo:place-index
- geo:tracker

Amazon Lookout for Metrics

- lookoutmetrics:Alert

Amazon Lookout for Vision

- lookoutvision:project

Amazon Managed Service for Apache Flink

- kinesisanalytics:application

Amazon Managed Service for Prometheus

- aps:rulegroupsnamespace
- aps:workspace

Amazon Managed Service for Prometheus

- memorydb:cluster
- memorydb:parametergroup
- memorydb:user

Amazon Managed Streaming for Apache Kafka

- kafka:cluster
- kafka:configuration

AWS Migration Hub Refactor Spaces

- refactorspaces:enviornment
- refactorspaces:enviornment-application
- refactorspaces:enviornment-application-route
- refactorspaces:enviornment-application-service

AWS Network Firewall

- network-firewall:firewall-policy

AWS Network Manager

- networkmanager:core-network
- networkmanager:device
- networkmanager:global-network
- networkmanager:link

Amazon OpenSearch 服務

- es:domain

AWS Panorama

- panorama:package

Amazon Personalize

- personalize:dataset
- personalize:dataset-group
- personalize:schema

AWS Private Certificate Authority

- acmpca:certificateauthority

Amazon QLDB

- qldb:ledger
- qldb:stream

Amazon Redshift

- redshift:cluster
- redshift:eventsubscription
- redshift:parametergroup
- redshift:snapshot
- redshift:snapshotcopygrant
- redshift:snapshotschedule
- redshift:subnetgroup
- redshift:usagelimit

Amazon Rekognition

- rekognition:project

Amazon Relational Database Service (Amazon RDS)

- rds:auto-backup
- rds:cev
- rds:cluster
- rds:cluster-endpoint
- rds:cluster-pg
- rds:cluster-snapshot
- rds:db
- rds:db-proxy
- rds:db-proxy-endpoint
- rds:deployment
- rds:es
- rds:global-cluster
- rds:og
- rds:pg
- rds:ri
- rds:secgrp
- rds:snapshot
- rds:subgrp

AWS Resilience Hub

- resiliencehub:resiliencypolicy

AWS Resource Groups

- resourcegroups:group

AWS 資源總管

- resource-explorer-2:index

- resource-explorer-2:view

Amazon Route 53

- route53:healthcheck
- route53:hostedzone

Amazon Route 53 Recovery Readiness

- route53-recover-readiness:recovery-group
- route53-recover-readiness:resource-set

Amazon Route 53 Resolver

- route53resolver:firewalldomainlist
- route53resolver:firewallrulegroup
- route53resolver:resolverendpoint
- route53resolver:resolverrule

Amazon SageMaker

- sagemaker:model
- sagemaker:notebookinstance

AWS Secrets Manager

- secretsmanager:secret

AWS Service Catalog

- servicecatalog:applications
- servicecatalog:attribute-groups

Amazon Simple Notification Service

- sns:topic

Amazon Simple Queue Service

- sqs:queue

Amazon Simple Storage Service (Amazon S3)

- s3:accesspoint
- s3:bucket
- s3:storage-lens

AWS Step Functions

- states:statemachine
- stepfunctions:activity

AWS Systems Manager

- ssm:association
- ssm:automation-execution
- ssm:document
- ssm:maintenancewindow
- ssm:managed-instance
- ssm:parameter
- ssm:patchbaseline
- ssm:resourcedatasync
- ssm:windowtarget
- ssm:windowtask

AWS Verified Access

- ec2:verifiedaccessendpoint
- ec2:verifiedaccessgroup
- ec2:verifiedaccessinstance
- ec2:verifiedaccesstrustprovider

AWS Wavelength

- ec2:carriergateway

以編程方式訪問支持的資源類型列表

若要從程式碼存取受支援的資源類型清單，您可以從任何 AWS SDK 叫用ListSupportedResourceTypes作業。

例如，您可以執行 list-supported-resource-types AWS Command Line Interface (AWS CLI) 命令，如下列範例所示。

```
$ aws resource-explorer-2 list-supported-resource-types
{
    "ResourceTypes": [
        {
            "ResourceType": "acm-pca:certificate-authority",
            "Service": "acm-pca"
        },
        {
            "ResourceType": "airflow:environment",
            "Service": "airflow"
        },
        {
            "ResourceType": "amplify:branches",
            "Service": "amplify"
        },
... truncated for brevity ...
```

顯示為其他類型的資源類型

某些資源類型由 Amazon 資源名稱 (ARN) 字串識別，這些字串與其他資源類型共用通用格式。發生這種情況時，資源總管可以報告該其他資源類型的資源。這會影響下表中的資源類型。

實際資源類型	報告為資源類型
ec2:securitygroupegress ec2:securitygroupingress	ec2:security-group-rule
elasticloadbalancingv2:loadbalancer	elasticloadbalancing:loadbalancer
docdb:dbcluster neptune:dbcluster rds:dbcluster	rds:cluster
docdb:dbclusterparametergroup neptune:dbclusterparametergroup rds:dbclusterparametergroup	rds:cluster-pg
docdb:clustersnapshot neptune:dbclustersnapshot rds:clustersnapshot	rds:cluster-snapshot
docdb:dbinstance neptune:dbinstance rds:dbinstance	rds:db
docdb:eventsubscription neptune:eventsubscription	rds:es

實際資源類型	報告為資源類型
rds:eventsubscription	
docdb:globalcluster rds:globalcluster	rds:global-cluster
neptune:dbparametergroup rds:dbparametergroup	rds:pg
docdb:dbsubnetgroup neptune:dbsubnetgroup rds:dbsubnetgroup	rds:subgrp

資源總管的配額

您的每個配額都AWS 帳戶有預設配額AWS 服務。，Quotas ()。您可以要求提高某些配額，而其他配額無法提高。

AWS 資源總管，Service Quotas ()。，Resource Explorer ()。AWS 服務

若要請求提升配額，請參閱《Service Quotas 使用者指南》中的請求提升配額。如果 Service Quotas 中尚未提供配額，請使用增加服務配額表單。

以下是「資源總管」的預設配額。

最大值配額	預設值
在一個中的視圖數AWS 區域	10

作業的速率限制	預設值
每秒搜尋作業上限	5
每秒非搜尋作業上限	3
每月彙總區域中的搜尋作業上限	10,000
每月本地區域的搜尋作業上限	500

搭 AWS 資源總管 配 AWS SDK 使用

AWS 軟件開發套件（SDK）可用於許多流行的編程語言。每個 SDK 都提供 API、程式碼範例和說明文件，讓開發人員能夠更輕鬆地以偏好的語言建置應用程式。

SDK 文件	代碼範例
AWS SDK for C++	AWS SDK for C++ 程式碼範例
AWS SDK for Go	AWS SDK for Go 程式碼範例
AWS SDK for Java	AWS SDK for Java 程式碼範例
AWS SDK for JavaScript	AWS SDK for JavaScript 程式碼範例
適用於 Kotlin 的 AWS SDK	適用於 Kotlin 的 AWS SDK 程式碼範例
AWS SDK for .NET	AWS SDK for .NET 程式碼範例
AWS SDK for PHP	AWS SDK for PHP 程式碼範例
AWS SDK for Python (Boto3)	AWS SDK for Python (Boto3) 程式碼範例
AWS SDK for Ruby	AWS SDK for Ruby 程式碼範例
適用於 Rust 的 AWS SDK	適用於 Rust 的 AWS SDK 程式碼範例
適用於 SAP ABAP 的 AWS SDK	適用於 SAP ABAP 的 AWS SDK 程式碼範例
適用於 Swift 的 AWS SDK	適用於 Swift 的 AWS SDK 程式碼範例

可用性範例

找不到所需的內容嗎？ 請使用本頁面底部的提供意見回饋連結申請程式碼範例。

資源總管使用者指南的文件歷程記錄

下表說明的文件版本 AWS 資源總管。如需有關此文件更新的通知，您可以訂閱 RSS 訂閱源。

變更	描述	日期
增加了對新資源類型的支持	資源瀏覽器增加了對 65 新資源的支持 AWS Key Management Service， AWS 服務 包括 Amazon 路線 53 和 Amazon Fraud Detector。	2024年2月20日
新的搜索過濾器添加	資源瀏覽器現在支持按應用程序搜索您的資源。	2023 年 11 月 16 日
增加了對新資源類型的支持	資源瀏覽器增加了對 86 新資源的支持 AWS CloudFormation AWS Glue， AWS 服務 包括，和 Amazon SageMaker。	2023 年 11 月 15 日
資源瀏覽器支援多帳號搜尋	您現在可以使用資源總管來搜尋和探索組織或組織單位 AWS 帳戶 內的資源。如需詳細資訊，請參閱開啟多帳戶搜尋。	2023 年 11 月 14 日
新的及更新的受管政策	資源瀏覽器添加了對 AWS Organizations. 已新增並更新AWS 受管理的策略，以授與 Resource Explorer 存取權給您的組織、組織結構、帳戶和委派的管理員。	2023 年 11 月 14 日
增加了對新資源類型的支持	資源瀏覽器添加了對 AWS Organizations. AWS 受管理的策略已更新，將 Resource Explorer 存取權授與您的組織	2023 年 11 月 14 日

	、組織結構、帳戶和委派的管理員。	
增加了對新資源類型的支持	資源瀏覽器現在支援服務的 12 種新資源類型 AWS Elastic Beanstalk，包括 Amazon Cognito 和 Amazon Elastic File System。	2023 年 10 月 18 日
增加了對新資源類型的支持	資源瀏覽器添加了對 164 個資源的支持。授與 Resource Explorer 索引資源存取權的AWS 受管理策略已更新，以包含這些新的資源類型。	2023 年 10 月 17 日
資源總管現在可在特定選擇加入區域使用	BAH 和 CGK 中的客戶現在可以選擇加入資源總管。	2023 年 10 月 5 日
增加了對新資源類型的支持	資源瀏覽器增加了對以下資源的支持 AWS 服務： AWS CodeBuild AWS CodePipeline，Amazon Cognito，Amazon 彈性容器註冊表 AWS Elastic Beanstalk，Amazon Elastic File System AWS IoT，和 AWS Step Functions. 授與 Resource Explorer 索引資源存取權的AWS 受管理策略已更新，以包含這些新的資源類型。	2023 年 8 月 1 日
資源瀏覽器現在支持將搜索結果導出到 CSV	您現在可以將 [資源搜尋] 頁面上的搜尋結果匯出為 CSV 格式的檔案。	2023 年 4 月 4 日

用 AWS Chatbot 於搜索和發現您的 AWS 資源	您現在可以使用自然語言問題 AWS Chatbot 來搜尋資源。如需詳細資訊，請參閱使用 AWS Chatbot 來搜尋資源。	2023 年 3 月 30 日
增加了對新資源類型的支持	資源瀏覽器增加了對以下資源的支持 AWS 服務：Amazon ElastiCache 和 Amazon Simple Queue Service (Amazon SQS)。AWS Lambda授與 Resource Explorer 索引資源存取權的AWS 受管理策略已更新，以包含這些新的資源類型。	2023 年 3 月 7 日
IAM 最佳做法更新	更新了指南以符合 IAM 最佳實務。如需更多詳細資訊，請參閱 IAM 中的安全最佳實務。	2022 年 12 月 6 日
新的 AWS 受管理策略	資源總管新增 AWSResourceExplorerFullAccess AWSResourceExplorerReadOnlyAccess、和 AWSResourceExplorerServiceRolePolicy 受管理的策略。	2022 年 11 月 7 日
初始版本	資源總管使用者指南的初始版本	2022 年 11 月 7 日

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。