使用者指南

# 標記 AWS 資源和標籤編輯器

版本 1.0

# 標記 AWS 資源和標籤編輯器: 使用者指南

# Table of Contents

AWS 已將標籤編輯器標籤管理功能從 AWS Resource Groups 主控台移至 AWS 資源總管 主控台。使用 Resource Explorer，您可以搜尋和篩選資源，然後從單一主控台管理資源標籤。若要進一步了解如何在 Resource Explorer 中管理資源標籤，請參閱 Resource Explorer 使用者指南中的管理資源。

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。

# 什麼是標籤編輯器？

標籤編輯器可讓您有效地管理標籤。標籤是金鑰和值對，可做為中繼資料來組織您的 AWS 資源。使用大多數 AWS 資源時，您可以選擇在建立資源時新增標籤。資源的範例包括 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體、Amazon Simple Storage Service (Amazon S3) 儲存貯體或秘密 AWS Secrets Manager。

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

標籤可協助您管理、識別、組織、搜尋及篩選資源。您可建立標籤，依照用途、擁有者、環境或其他條件分類資源。

每個標籤有兩個部分：

- 標籤鍵 (例如，`CostCenter`、`Environment` 或 `Project`)。標籤鍵會區分大小寫。
- 標籤值 (例如 `111122223333` 或 `Production`)。與標籤鍵相同，標籤值會區分大小寫。

> **Note**
>
> 雖然標籤金鑰區分大小寫，但 IAM 對 IAM 資源有其他驗證，以防止套用只有不同大小寫的標籤金鑰。我們建議不要使用只有不同大小寫的金鑰。反之，您可以使用服務控制政策 SCPs)，以集中控制組織中 IAM 使用者和 IAM 角色的最大可用許可。

## 資源標記方法

有三種方式可將標籤新增至 AWS 資源：

- AWS 服務 API 操作 – 直接支援的標記 API 操作 AWS 服務。若要探索每個 AWS 服務 提供的標記功能，請參閱 文件AWS 索引中的服務文件。
- 標籤編輯器主控台 – 有些服務支援使用標籤編輯器主控台進行標記。
- 資源群組標記 API – 大多數服務也支援使用 標記AWS Resource Groups Tagging API。

> **Note**
>
> 您也可以使用 AWS Service Catalog TagOptions Library 輕鬆管理佈建產品上的標籤。TagOption 是 Service Catalog 中管理的鍵值對。它不是 AWS 標籤，而是做為根據 TagOption 建立 AWS 標籤的範本。

您可以在 AWS中標記所有成本累計服務的資源。針對下列服務， AWS 建議支援標記的較新替代方案 AWS 服務 ，以更符合客戶使用案例。

| | | |
|---|---|---|
| Amazon 雲端目錄 | Amazon CloudSearch | Amazon Cognito Sync |
| AWS Data Pipeline | Amazon Elastic Transcoder | Amazon Machine Learning |
| AWS OpsWorks Stacks | Amazon S3 Glacier Direct | Amazon SimpleDB |
| Amazon WorkSpaces Application Manager | AWS DeepLens | |

## 進一步了解

此頁面提供標記 AWS 資源的一般資訊。如需在特定 AWS 服務中標記資源的詳細資訊，請參閱其文件。以下也是很好了解標記的資訊來源：

- 如需 的相關資訊 AWS Resource Groups Tagging API，請參閱資源群組標記 API 參考指南。
- 如需有關每個 AWS 服務 提供的標記功能的資訊，請參閱 文件AWS 索引中的服務文件。
- 如需在 IAM 政策中使用標籤來協助控制誰可以檢視和與您的 AWS 資源互動的資訊，請參閱《IAM 使用者指南》中的使用標籤控制對 和 IAM 使用者和角色的存取。

# 最佳實務和策略

這些區段提供標記 AWS 資源和使用標籤編輯器時最佳實務和策略的相關資訊。

## 標記最佳實務

當您為 AWS 資源建立標記策略時，請遵循最佳實務：

- 請勿在標籤中加入個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多 AWS 服務都可以存取標籤，包括帳單。標籤不適用於私人或敏感資料。
- 使用標準化、區分大小寫的標籤格式，並統一套用在所有資源類型上。
- 考慮支援多種用途的標籤準則，例如資源存取控制管理、成本追蹤、自動化和組織。
- 使用自動化工具來協助管理資源標籤。標籤編輯器和資源群組標記 API 可讓您以程式設計方式控制標籤，讓您更輕鬆地自動管理、搜尋和篩選標籤和資源。
- 使用太多標籤，還不如使用較少的標籤。
- 請記住，變更標籤以因應不斷變更的業務需求很容易，但請考量變更後的後果。例如，變更存取控制標籤表示您也必須更新參考這些標籤的政策，以及控制對資源的存取。
- 您可以使用 AWS Organizations建立和部署標籤政策，自動強制執行組織選擇採用的標記標準。標籤政策可讓您指定標記規則，這些規則可定義有效索引鍵名稱以及每個索引鍵的有效值。您可以選擇只進行監控，讓您有機會評估和清理現有標籤。一旦標籤符合所選標準，您就可以在標籤政策中啟用強制執行功能，以防止建立不合規的標籤。如需詳細資訊，請參閱《AWS Organizations 使用者指南》中的標籤政策。

## 標籤命名最佳實務

這些是一些最佳實務和命名慣例，建議您搭配標籤使用。

AWS 標籤的金鑰名稱區分大小寫，因此請確保標籤的使用一致。例如，標籤索引鍵 `CostCenter`和 `costcenter` 不同。一個標籤金鑰可能設定為財務分析和報告的成本分配標籤，而另一個標籤金鑰可能不會設定為相同用途。

許多標籤是由 預先定義， AWS 或由各種 自動建立 AWS 服務。許多AWS 產生的標籤使用小寫的金鑰名稱，連字號分隔名稱中的單字，字首後面加上冒號，以識別標籤的來源服務。例如，請參閱下列內容：

- `aws:ec2spot:fleet-request-id` 是識別啟動執行個體之 Amazon EC2 Spot 執行個體請求的標籤。
- `aws:cloudformation:stack-name` 是識別建立資源之 AWS CloudFormation 堆疊的標籤。
- `elasticbeanstalk:environment-name` 是識別建立資源之應用程式的標籤。

請考慮使用下列規則來命名標籤：

- 使用所有小寫的單字。
- 使用連字號分隔單字。

- 使用字首後面加上冒號，以識別組織名稱或縮寫名稱。

例如，對於一家名為 AnyCompany 的虛構公司，您可以定義如下的標籤：

- anycompany:cost-center 識別內部成本中心程式碼。
- anycompany:environment-type 以識別環境是開發、測試還是生產。
- anycompany:application-id 以識別資源所建立的應用程式。

字首可確保標籤可清楚辨識，如您的組織所定義，而不是由您或您可能正在使用 AWS 的第三方工具所識別。將所有小寫字母和連字號 (作為分隔符號) 搭配使用可避免對如何大寫標籤名稱造成混淆。例如：anycompany:project-id 比 ANYCOMPANY:ProjectID、anycompany:projectID 或 Anycompany:ProjectId 更容易記住。

### 標籤命名限制和需求

下列基本命名和使用需求適用於標籤：

- 每個資源最多可以有 50 個使用者建立的標籤。
- 系統建立以 aws: 開頭的標籤會保留供 AWS 使用，且不會計入此限制。您無法編輯或刪除以 aws: 字首開頭的標籤。
- 對於每一個資源，每個標籤金鑰必須是唯一的，且每個標籤金鑰只能有一個值。
- 在 UTF-8 中，標籤金鑰必須至少為 1 且最多為 128 個 Unicode 字元。
- 在 UTF-8 中，標籤值必須是最小為 0 且最多為 256 個 Unicode 字元。
- 允許的字元可能因 AWS 服務而異。如需有關您可以使用哪些字元來標記特定 AWS 服務中的資源的資訊，請參閱其文件。一般而言，允許的字元包含可用 UTF-8 表示的英文字母、數字、空格，以及 _ . : / = + - @ 等特殊字元。
- 標籤鍵與值皆區分大小寫。做為最佳實務，請決定大寫標籤的策略，並一致地在所有資源類型中實作該策略。例如，決定要使用 Costcenter、costcenter 還是 CostCenter，並針對所有標籤使用相同的慣例。避免針對相似的標籤使用不一致的大小寫處理。

## 通用標記策略

使用下列標記策略來協助識別和管理 AWS 資源。

目錄

- 資源組織的標籤
- 成本配置的標籤
- 用於自動化的標籤
- 存取控制的標籤
- 標記管理

## 資源組織的標籤

標籤是組織 中 AWS 資源的好方法 AWS Management Console。您可以設定標籤與資源一起顯示，也可以設定依標籤搜尋及篩選。使用 AWS Resource Groups 服務，您可以根據一或多個標籤或標籤部分來建立 AWS 資源群組。您也可以根據群組在 AWS CloudFormation 堆疊中的出現情況來建立群組。使用資源群組和標籤編輯器，您可以合併將多項服務、資源和區域集結在一處的應用程式資料，然後進行檢視。

## 成本配置的標籤

AWS Cost Explorer 和詳細帳單報告可讓您依標籤細分 AWS 成本。一般而言，您可以使用成本中心/業務單位、客戶或專案等商業標籤，將 AWS 成本與傳統成本分配維度建立關聯。不過，成本分配報告可包含各種標籤。這可讓您建立成本與技術或安全性方面的關聯性，像是特定的應用程式、環境或合規計劃。

對於某些 服務，您可以使用 AWS產生的`createdBy`標籤進行成本分配，以協助考慮可能未分類的資源。`createdBy` 標籤僅適用於支援的 AWS 服務和資源。其值包含與特定 API 或主控台事件相關聯的資料。如需詳細資訊，請參閱 AWS 帳單與成本管理 使用者指南中的 AWS產生的成本分配標籤。

## 用於自動化的標籤

特定資源或服務的標籤通常用於在自動化活動期間篩選資源。自動化標籤是用來選擇加入或選擇退出自動化任務，或用以識別要存檔、更新或刪除的特定資源版本。例如，您可以執行自動化的 `start` 或 `stop` 指令碼，在非上班時間關閉開發環境以降低成本。在此案例中，Amazon Elastic Compute Cloud (Amazon EC2) 執行個體標籤是找出要選擇退出此動作之執行個體的簡單方法。至於尋找和刪除過時、非最新或輪換 Amazon EBS 快照的指令碼，快照標籤可以新增額外的搜尋條件特點。

## 存取控制的標籤

IAM 政策支援標籤型條件，可讓您根據特定的標籤或標籤值來限制 IAM 許可。例如，IAM 使用者或角色許可可以包含這樣的條件：根據標籤將 EC2 API 呼叫限制於特定環境 (例如開發、測試或生產)。相

同的策略可用於將 API 呼叫限制在特定的 Amazon Virtual Private Cloud (Amazon VPC) 網路。只有特定服務才支援標籤型的資源層級 IAM 許可。當您使用標籤型條件控制存取時，請務必定義並限制能修改標籤的人員。如需使用標籤控制 API 存取 AWS 資源的詳細資訊，請參閱《IAM 使用者指南》中的AWS 使用 IAM 的 服務。

### 標記管理

有效的標記策略使用標準化標籤，並以程式設計方式一致地跨 AWS 資源套用它們。您可以使用被動和主動方法來管理 AWS 環境中的標籤。

- 被動控管是使用資源群組標記 API 和自訂指令碼等工具 AWS Config 規則，尋找未正確標記的資源。若要手動尋找資源，您可以使用標籤編輯器和詳細的帳單報告。
- 主動控管會使用 AWS CloudFormation、Service Catalog AWS Organizations、 中的標籤政策或 IAM 資源層級許可等工具，以確保標準化標籤在資源建立時一致套用。

  例如，您可以使用 AWS CloudFormation `Resource Tags` 屬性將標籤套用至資源類型。在 Service Catalog 中，您可以新增在產品啟動時，自動合併並套用至產品的組合和產品標籤。更嚴格的主動式管理形式包含自動化的任務。例如，您可以使用資源群組標記 API 搜尋 AWS 環境標籤，或執行指令碼隔離或刪除標記不正確的資源。

## 標記類別

使用標籤最有效的公司通常會建立與業務相關的標籤群組，依技術、業務和安全性層面組織資源。使用自動化程序管理基礎結構的公司也會包含額外的自動化特定標籤。

| 技術標籤 | 用於自動化的標籤 | 商業標籤 | 安全性標籤 |
| --- | --- | --- | --- |
| • 名稱 – 識別個別資源<br>• 應用程式 ID – 識別與特定應用程式相關的資源<br>• 應用程式角色 – 描述特定資源的功能 (例如 Web 伺服器、訊息經紀人、資料庫) | • 日期/時間 – 識別資源應啟動、停止、刪除或輪換的日期或時間<br>• 選擇加入/選擇退出 – 指示資源是否應包含在自動化活動中，例如啟動、停止或調整執行個體大小 | • 專案 – 識別資源支援的專案<br>• 擁有者 – 識別資源的負責人<br>• 成本中心/業務單位 – 識別與資源相關聯的成本中心或業務單位，通常適用於成本配置與追蹤 | • 機密性 – 資源支援的特定資料機密等級識別符<br>• 合規性 – 必須遵守特定合規要求的工作負載識別碼 |

| 技術標籤 | 用於自動化的標籤 | 商業標籤 | 安全性標籤 |
| --- | --- | --- | --- |
| • 叢集 – 識別共用通用組態並執行應用程式特定功能的資源伺服器陣列<br>• 環境 – 區分開發、測試和生產資源<br>• 版本 – 協助區分資源或應用程式的版本 | • 安全性 – 決定需求，例如加密或啟用 Amazon VPC 流程日誌；識別需要特別仔細檢查的路由表或安全群組 | • 客戶 – 識別受特定資源群組服務的特定用戶端 | |

# 標籤編輯器入門

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

若要一次為多個資源新增標籤，或編輯或刪除標籤，請使用標籤編輯器。利用標籤編輯器，您會搜尋要加標籤的資源，然後為搜尋結果中的資源管理標籤。

啟動標籤編輯器

1. 登入 AWS Management Console。
2. 執行下列其中一個步驟：
   - 選擇 服務。然後在管理與控管下，選擇資源群組和標籤編輯器。在左側導覽窗格中，選擇標籤編輯器。
   - 使用直接連結：AWS 標籤編輯器主控台。

並不是所有資源都可以套用標籤。如需有關標籤編輯器支援哪些資源的資訊，請參閱AWS Resource Groups 《 使用者指南》中支援的資源類型的標籤編輯器標記欄。如果不支援您要標記的資源類型，請選擇主控台視窗左下角的意見回饋來 AWS 告知 。

如需對資源加標籤所需之許可和角色的相關資訊，請參閱設定許可。

主題



## 使用標籤編輯器的先決條件

開始為資源加上標籤之前，請確定您具有作用中 AWS 帳戶 的現有資源，以及標記資源和建立群組的適當權限。

主題

- 註冊 AWS 帳戶
- 建立具有管理存取權的使用者
- 建立 資源

## 註冊 AWS 帳戶

如果您沒有 AWS 帳戶，請完成下列步驟來建立一個。

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。

   註冊程序的一部分包括接聽電話或文字訊息，以及在電話鍵盤上輸入驗證碼。

   當您註冊 時 AWS 帳戶，AWS 帳戶根使用者會建立 。根使用者有權存取該帳戶中的所有 AWS 服務 和資源。作為安全最佳實務，請將管理存取權指派給使用者，並且僅使用根使用者來執行需要根使用者存取權的任務。

AWS 會在註冊程序完成後傳送確認電子郵件給您。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。

## 建立具有管理存取權的使用者

註冊 後 AWS 帳戶，請保護 AWS 帳戶根使用者、啟用 AWS IAM Identity Center和建立管理使用者，以免將根使用者用於日常任務。

保護您的 AWS 帳戶根使用者

1. 選擇根使用者並輸入 AWS 帳戶 您的電子郵件地址，以帳戶擁有者AWS Management Console身分登入 。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)。

   如需說明，請參閱《IAM 使用者指南》中的為您的 AWS 帳戶 根使用者 （主控台） 啟用虛擬 MFA 裝置。

建立具有管理存取權的使用者

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，將管理存取權授予使用者。

   如需使用 IAM Identity Center 目錄 做為身分來源的教學課程，請參閱AWS IAM Identity Center 《 使用者指南》中的使用預設值設定使用者存取權 IAM Identity Center 目錄。

以具有管理存取權的使用者身分登入

- 若要使用您的 IAM Identity Center 使用者簽署，請使用建立 IAM Identity Center 使用者時傳送至您電子郵件地址的簽署 URL。

  如需使用 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。

指派存取權給其他使用者

1. 在 IAM Identity Center 中，建立一個許可集來遵循套用最低權限的最佳實務。

   如需指示，請參閱《AWS IAM Identity Center 使用者指南》中的建立許可集。
2. 將使用者指派至群組，然後對該群組指派單一登入存取權。

   如需指示，請參閱《AWS IAM Identity Center 使用者指南》中的新增群組。

## 建立 資源

您的 中必須有 AWS 帳戶 要標記的資源。如需支援資源類型的詳細資訊，請參閱AWS Resource Groups 《 使用者指南》中支援的資源類型下的標籤編輯器標記欄。

# 設定許可

若要充分利用標籤編輯器，您可能需要額外的許可來標記資源或查看資源的標籤索引鍵和值。這些許可屬於下列類別：

- 個別服務的許可，使得您可以為來自那些服務的資源加上標籤，並將它們包含在資源群組中。

- 使用標籤編輯器主控台所需的許可。

如果您是管理員，您可以透過 AWS Identity and Access Management (IAM) 服務建立政策，為使用者提供許可。您首先建立 IAM 角色、使用者或群組，然後套用具有其所需許可的政策。如需建立和連接 IAM 政策的資訊，請參閱使用政策。

## 個別服務的許可

> **Important**
>
> 本節說明如果您想要標記來自其他 AWS 服務主控台和 APIs 的資源時所需的許可。

若要將標籤新增到資源，您需要資源所屬服務所需的許可。例如，若要標記 Amazon EC2 執行個體，您必須擁有該服務 API 中標記操作的許可，例如 Amazon EC2 CreateTags操作。

## 使用標籤編輯器主控台所需的許可

若要使用標籤編輯器主控台列出和標記資源，必須將下列許可新增至 IAM 中的使用者政策陳述式。您可以新增由 維護並保持最新狀態的 AWS 受管政策 AWS，也可以建立和維護自己的自訂政策。

### 針對標籤編輯器許可使用 AWS 受管政策

標籤編輯器支援下列 AWS 受管政策，您可以使用這些政策為您的使用者提供一組預先定義的許可。您可以將這些受管政策連接到任何角色、使用者或群組，就像您建立的任何其他政策一樣。

ResourceGroupsandTagEditorReadOnlyAccess

此政策會授予連接的 IAM 角色或使用者許可，以呼叫 AWS Resource Groups 和標籤編輯器的唯讀操作。若要讀取資源的標籤，您還必須透過單獨的政策擁有該資源的許可。如需進一步了解，請參閱下列重要注意事項。

ResourceGroupsandTagEditorFullAccess

此政策授予連接的 IAM 角色或使用者許可，以呼叫任何資源群組操作和標籤編輯器中的讀取和寫入標籤操作。若要讀取或寫入資源的標籤，您還必須透過單獨的政策擁有該資源的許可。如需進一步了解，請參閱下列重要注意事項。

**Important**

先前的兩個政策會授予呼叫標籤編輯器操作並使用標籤編輯器主控台的許可。不過，您不僅必須擁有叫用 操作的許可，還必須擁有您嘗試存取其標籤之特定資源的適當許可。若要授予標籤的存取權，您還必須連接下列其中一個政策：

- AWS 受管政策ReadOnlyAccess會針對每個服務的資源授予唯讀操作的許可。當新政策可供使用 AWS 服務 時， AWS 會自動將此政策保持在最新狀態。
- 許多 服務提供服務特定的唯讀 AWS 受管政策，可用來限制只能存取該服務提供的資源。例如，Amazon EC2 提供 AmazonEC2ReadOnlyAccess。
- 您可以建立自己的政策，僅針對您希望使用者存取的少數服務和資源，授予特定唯讀操作的存取權。此政策使用允許清單策略或拒絕清單策略。

  允許清單策略會利用預設拒絕存取的事實，直到您在政策中明確允許為止。因此，您可以使用類似下列範例的政策。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [ "tag:*" ],
            "Resource": "<ARNs of resources to allow tagging>"
        }
    ]
}
```

或者，您可以使用允許存取所有資源的拒絕清單策略，但您明確封鎖的資源除外。這需要個別的政策，適用於允許存取的相關使用者。以下範例政策接著會拒絕存取 Amazon Resource Name (ARN) 列出的特定資源。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
             "Action": [ "tag:*" ],
            "Resource": "<ARNs of resources to disallow tagging>"
        }
    ]
```

```
}
```

### 手動新增標籤編輯器許可

- `tag:*`（此許可允許所有標籤編輯器動作。 如果您改為限制使用者可用的動作，您可以將星號取代為特定動作，或以逗號分隔的動作清單。）
- `tag:GetResources`
- `tag:TagResources`
- `tag:UntagResources`
- `tag:getTagKeys`
- `tag:getTagValues`
- `resource-explorer:*`
- `resource-groups:SearchResources`
- `resource-groups:ListResourceTypes`

> **Note**
>
> 當您使用標籤索引鍵或值篩選搜尋時，`resource-groups:SearchResources`許可允許標籤編輯器列出資源。
> `resource-explorer:ListResources` 許可允許標籤編輯器在您搜尋資源時列出資源，而無需定義搜尋標籤。

## 授予使用標籤編輯器的許可

若要將使用 AWS Resource Groups 和標籤編輯器的政策新增至角色，請執行下列動作。

1. 開啟 IAM 主控台至角色頁面。
2. 尋找您要授予標籤編輯器許可的角色。選擇角色的名稱以開啟角色的摘要頁面。
3. 在 Permissions (許可) 標籤上，選擇 Add permissions (新增許可)。
4. 選擇直接連接現有政策。
5. 選擇建立政策。

6. 在 JSON 標籤上，貼上下列政策陳述式。

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

> **Note**
>
> 此範例政策陳述式授予僅執行標籤編輯器動作的許可。

7. 選擇 Next: Tags (下一步：標籤)，然後選擇 Next: Review (下一步：檢閱)。
8. 輸入新政策的名稱和描述。例如 **`AWSTaggingAccess`**。
9. 選擇建立政策。

現在政策已儲存在 IAM 中，您可以將政策連接到其他主體，例如角色、群組或使用者。如需如何將政策新增至委託人的詳細資訊，請參閱《IAM 使用者指南》中的新增和移除 IAM 身分許可。

## 根據標籤的授權和存取控制

AWS 服務 支援下列項目：

- 動作型政策 – 例如，您可以建立允許使用者執行 `GetTagKeys`或 `GetTagValues`操作的政策，但不能建立其他政策。
- 政策中的資源層級許可 – 許多 服務支援使用 ARNs 在政策中指定個別資源。

- 以標籤為基礎的授權 – 許多服務支援在政策條件中使用資源標籤。例如，您可以建立政策，允許使用者完整存取與使用者具有相同標籤的群組。如需詳細資訊，請參閱AWS Identity and Access Management 《 使用者指南》中的什麼是 ABAC AWS？。
- 暫時登入資料 – 使用者可以使用允許標籤編輯器操作的政策來擔任角色。

標籤編輯器不會使用任何服務連結角色。

如需標籤編輯器如何與 AWS Identity and Access Management (IAM) 整合的詳細資訊，請參閱AWS Identity and Access Management 《 使用者指南》中的下列主題：

- AWS 使用 IAM 的 服務
- 標籤編輯器的動作、資源和條件索引鍵
- 使用 政策控制對 AWS 資源的存取

# 尋找要標記的資源

使用標籤編輯器，您可以建置查詢，在一或多個 AWS 區域 可供標記的資源中尋找資源。您最多可以選擇 20 個個別的資源類型，或是根據All resource types (所有資源類型) 來建立查詢。您的查詢可以包含已有標籤的資源或沒有標籤的資源。如需詳細資訊，請參閱AWS Resource Groups 《 使用者指南》中支援的資源類型中的標籤編輯器標記欄。

找到要加標籤的資源之後，您可以使用標籤編輯器來新增標籤，或檢視、編輯或刪除標籤。

尋找要加標籤的資源

1. 開啟標籤編輯器主控台。
2. （選用）選擇要在 AWS 區域 其中搜尋要標記之資源的 。根據預設，會使用您目前的區域。針對此程序，選擇 us-east-1 和 us-west-2。
3. 從資源類型下拉式清單中選擇至少一個資源類型。您可以一次新增或編輯標籤最多 20 個個別的資源類型，或選擇 All resource types (所有資源類型)。針對此程序，選擇 AWS::EC2::Instance 和 AWS::S3::Bucket。
4. （選用）在標籤欄位中，輸入標籤索引鍵或標籤索引鍵和值對，將目前 中的資源限制 AWS 區域 為僅以您指定值標記的資源。當您輸入標籤索引鍵時，目前區域中相符的標籤索引鍵會出現在清單中。您可以從清單中選擇標籤金鑰。標籤編輯器會在您輸入了足夠的字元可比對現有的索引鍵時，為您自動完成標籤索引鍵。完成標籤時，選擇 Add (新增) 或按下 Enter 鍵。在這個範例中，對擁有 Stage (階段) 標籤索引鍵的資源進行篩選。標籤值是選用的，但會進一步縮小查詢的結果。若要新增更多標籤，請選擇 Add (新增)。查詢會將AND運算子指派給標籤，因此查詢只會傳回符合指定資源類型和所有指定標籤的資源。

   > **Note**
   >
   > 標籤編輯器主控台目前不支援萬用字元。

   若要尋找某個標籤索引鍵具有多個值的資源，請對查詢新增具有相同索引鍵的另一個標籤，但指定不同的值。結果會包含使用相同標籤索引鍵加標籤以及具有任何所選值的所有資源。搜尋區分大小寫。

   將標籤方塊保留空白，以在選取的 中尋找指定類型的所有資源 AWS 區域。此查詢會傳回具有任何標籤的資源，並且包含沒有標籤的資源。若要從您的查詢移除標籤，請選擇標籤的標記上的 X。

若要尋找具有標籤但具有空值的資源，請選擇 （空值）。

> **Note**
>
> 在尋找具有指定標籤的資源之前，它們必須已套用到目前 中指定類型的至少一個資源 AWS 區域。

5. 當您的查詢就緒，請選擇 Search resources (搜尋資源)。結果會以資料表的形式顯示在資源搜尋結果區域中。

   若要篩選大量資源，請在 Filter resources (篩選資源) 中輸入任何篩選文字，例如資源名稱的一部分。

   > **Note**
   >
   > 您可以使用子字串來篩選結果。

6. （選用）若要設定標籤編輯器在資源搜尋結果中顯示的欄，請選擇資源搜尋結果中的偏好設定齒輪圖示。

   在 Preferences (偏好設定) 頁面上，選擇您想要顯示在您的搜尋結果中的列數。如果您想要查看資料表中的所有文字，請選取包裝行核取方塊。

   開啟您要標籤編輯器在您的結果中顯示的欄。您可以為搜尋結果中出現的每個標籤或搜尋結果的選定子集顯示資料欄。您可以在找到要標記的資源之後隨時執行此操作。若要啟用資料欄，請選擇標籤旁的切換圖示，並將其從關閉變更為開啟。

   設定好可見欄和顯示的列數時，選擇 Confirm (確認)。

## 檢視和編輯所選資源的現有標籤

標籤編輯器會顯示所選資源上現有標籤，這些資源位於尋找資源以標記查詢的結果中。

如果您如上一節所述啟用任何標籤欄，您可以在搜尋結果中查看每個資源的該標籤的目前值。

> **Note**
>
> 本主題說明如何編輯個別資源的標籤。您也可以同時大量編輯多個所選資源的編輯標籤。如需詳細資訊，請參閱使用標籤編輯器管理標籤。

在搜尋結果資料表中內嵌編輯標籤

1. 在您要編輯的資源上，選擇標籤的值。

   > **Note**
   >
   > - 如果所選資源目前沒有具有所選索引鍵的標籤，則值會顯示為 （未標記）。
   > - 如果所選資源確實有具有所選索引鍵但沒有值的標籤，則值會顯示為 '–'。

2. 您可以輸入新的值，或從具有此標籤的其他資源上已存在的任何值中進行選擇。您也可以選擇移除標籤，從此資源中刪除標籤。

檢視個別資源的所有標籤

1. 在尋找要標記查詢的資源結果中，針對您要檢視現有標籤的任何資源，選擇標籤欄中的數字。Tags (標籤數) 欄中為破折號的資源沒有現有的標籤。
2. 在 Resource tags (資源標籤) 中檢視現有標籤。您也可以在從管理標籤頁面變更或移除標籤時，選擇管理所選資源的標籤，以開啟此視窗。

   > **Note**
   >
   > 如果沒有看到您最近對資源套用的標籤，請嘗試重新整理您的瀏覽器視窗。

## 匯出結果至 .csv 檔案

您可以將尋找資源的結果匯出為逗號分隔值 (.csv) 檔案，以標記查詢。.csv 檔案包含資源名稱、服務、區域、資源 IDs、標籤總數，以及集合中每個唯一標籤索引鍵的資料欄。.csv 檔案可協助您為組織中的資源制定標記策略，或判斷跨資源標記時存在重疊或不一致之處。

1. 在 Find resources to tag (尋找要加標籤的資源) 查詢的結果中，選擇 Export resources to CSV (匯出資源至 CSV)。
2. 當瀏覽器提示您時，選擇開啟 .csv 檔案，或將其儲存到方便的位置。

# 使用標籤編輯器管理標籤

找到要標記的資源後，您可以新增、移除和編輯部分或全部搜尋結果的標籤。標籤編輯器會顯示連接至資源的任何標籤。它也會顯示這些標籤是否由資源的服務主控台或使用 API 新增至標籤編輯器。

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

> **管理標籤的其他方式**
>
> 本主題討論在 中使用標籤編輯器來標記資源 AWS Management Console。不過，您也可以使用下列工具來管理 AWS 資源上的標籤：
>
> - 您可以使用 () 中的命令，在 shell AWS Command Line Interface 提示字元中輸入 或 指令碼`resourcegroupstaggingapi`命令AWS CLI。
> - 您可以使用 中的AWS Resource Groups 標記 API 來建立和執行PowerShell指令碼 AWS Tools for PowerShell Core。
> - 您可以使用標記 APIs 的資源群組，例如標記 Python APIs 或標記 Java APIs，以任何可用的 AWS SDKs 建立和執行程式。

當您新增、移除或編輯現有標籤時，您只會變更您在尋找資源結果中選取的那些資源上的標籤，以標記查詢。您可以選擇要在其上管理標籤的最多 500 個資源。

## 將標籤新增至選取的資源

您可以使用標籤編輯器對 Find resources to tag (尋找要加標籤的資源) 查詢結果中的所選資源新增標籤。

> **Note**
>
> 本主題說明如何大量編輯多個資源的標籤。您也可以編輯個別資源的標籤值。如需詳細資訊，請參閱檢視和編輯所選資源的現有標籤。

1. 開啟標籤編輯器主控台，然後提交查詢，以傳回您要標記的多個資源。
2. 在尋找要標記查詢之資源的結果資料表中，選取您要新增標籤之資源旁的核取方塊。在資料表頂端的篩選資源中輸入文字字串，以篩選部分資源的名稱、ID、標籤索引鍵或標籤值。在 Tags (標籤) 欄中，請注意，結果中的資源已套用標籤。
3. 選取一或多個資源的核取方塊，然後選擇管理所選資源的標籤。
4. 在 Manage tags (管理標籤) 頁面上，檢視您所選資源上的標籤。雖然原始查詢傳回更多資源，但您只會將標籤新增至您在步驟 1 中選取的資源。選擇 Add tag (新增標籤)。
5. 輸入標籤索引鍵和選用的標籤值。在此程序中，您將新增標籤索引鍵 **`Team`** 和標籤值 **`Development`**。

   > **Note**
   >
   > 一個資源最多可有 50 個使用者套用的標籤。如果您接近 50 個使用者套用的標籤，則可能無法將新標籤新增至資源。 AWS 產生的標籤不適用於 50 個標籤限制。在您所選的資源內，標籤索引鍵也必須是唯一的。您無法使用與所選資源中已存在的標籤索引鍵相符的索引鍵來新增標籤。

6. 新增標籤完成後，請選擇檢閱並套用變更。
7. 如果您接受變更，請選擇 Apply changes to all selected (套用變更到所有選取的項目)。
8. 根據您選取的資源數量，套用新標籤可能需要幾分鐘的時間。請勿離開頁面或在相同的瀏覽器索引標籤中開啟不同的頁面。如果變更成功，在頁面頂端會顯示綠色成功橫幅。等待成功或失敗橫幅顯示在頁面上，然後再繼續。

   如果標籤變更部分或全部資源失敗，請參閱對標籤變更進行故障診斷。解決失敗的標籤變更（例如許可不足）之後，您可以在標籤變更失敗的資源上重試標籤變更。如需詳細資訊，請參閱the section called “重試失敗的標籤變更”。

## 編輯所選資源的標籤

您可以使用標籤編輯器對 Find resources to tag (尋找要加標籤的資源) 查詢結果中的所選資源變更現有的標籤值。編輯標籤會變更具有相同標籤索引鍵的所有所選資源上的標籤值。您無法重新命名標籤金鑰，但您可以刪除標籤，並使用新名稱建立標籤，以取代原始標籤金鑰。這會刪除所選資源上具有該索引鍵的所有標籤。

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

1. 在 Find resources to tag (尋找要加標籤的資源) 查詢的結果中，選取您要變更現有標籤的資源旁核取方塊。在 Filter resources (篩選資源) 中輸入文字字串，以篩選資源的名稱或 ID 的一部分。在 Tags (標籤) 欄中，請注意，結果中的資源已套用標籤。
2. 選擇 Manage tags of the selected resources (管理所選資源的標籤)。
3. 在 Manage tags (管理標籤) 頁面上，於 Edit tags of selected resources (編輯所選資源的標籤) 中，檢視您選取的資源上的標籤。雖然您的原始查詢可能已傳回更多資源，但您只會變更您在步驟 1 中選取之資源的標籤。
4. 變更、新增或刪除標籤值。現有標籤都必須有標籤索引鍵，但標籤值則是選用的。

   在此程序中，我們將**Team**標籤的值變更為 **QA**。

   如果您選取的資源具有相同索引鍵的不同值，選取的資源具有不同的標籤值會顯示在標籤值欄位中。在此情況下，將游標放在方塊中會開啟下拉式清單，列出所選資源中此標籤索引鍵的所有可用值。

   如果您的選項中的資源具有您需要的標籤值，當您輸入標籤值時，會將它反白顯示。例如，如果您的選項中的資源具有 **QA**，當您輸入 **Q** 時，會將該值反白顯示。下拉式清單中的值有助於保持跨資源的標籤值一致。所有所選資源上的標籤值也會變更。在此範例中，會將具有 **Team** 標籤索引鍵的所有所選資源的標籤值變更為 **QA**。對於沒有**Team**標籤的所選資源，**QA**會新增具有 值的**Team**標籤。
5. 完成標籤變更後，請選擇檢閱並套用變更。
6. 如果您接受變更，請選擇 Apply changes to all selected (套用變更到所有選取的項目)。
7. 根據您所選的資源數量而定，編輯標籤可能需要幾分鐘的時間。請勿離開頁面或在相同的瀏覽器索引標籤中開啟不同的頁面。如果變更成功，在頁面頂端會顯示綠色成功橫幅。等待成功或失敗橫幅顯示在頁面上，然後再繼續。

   如果標籤變更部分或全部資源失敗，請參閱對標籤變更進行故障診斷。在您解決標籤變更失敗的根本原因 （ 例如許可不足 ） 之後，您可以重試標籤變更失敗的資源上的標籤變更。如需詳細資訊，請參閱the section called “重試失敗的標籤變更”。

# 從選取的資源移除標籤

您可以使用標籤編輯器，從位於 Find resources to tag (尋找要加標籤的資源) 查詢結果中的所選資源移除標籤。移除標籤會從具有該標籤的所有所選資源刪除標籤。由於您無法編輯標籤金鑰，因此如果您需要編輯標籤金鑰，可以移除標籤，並將它們取代為新標籤。這會刪除所選資源上具有該索引鍵的所有標籤。

1. 在 Find resources to tag (尋找要加標籤的資源) 查詢的結果中，選取您想要從中移除標籤的資源旁的核取方塊。在 Filter resources (篩選資源) 中輸入文字字串，以篩選資源的名稱或 ID 的一部分。
2. 選擇 Manage tags of the selected resources (管理所選資源的標籤)。
3. 在 Manage tags (管理標籤) 頁面上，於 Edit tags of selected resources (編輯所選資源的標籤) 中，檢視您所選資源上的標籤。雖然您的原始查詢可能已傳回更多資源，但您只會變更您在步驟 1 中選取之資源的標籤。
4. 選擇您要刪除的任何標籤旁的 Remove tag (移除標籤)。在此程序中，我們會移除 **Team**標籤。

   > **Note**
   >
   > 選擇 Remove tag (移除標籤) 會從具有該標籤的所有選取資源移除標籤。

5. 選擇 Review and apply changes (檢閱和套用變更)。
6. 在確認頁面上，選擇 Apply changes to all selected (套用變更到所有選取的項目)。
7. 根據您所選的資源數量而定，移除標籤可能需要幾分鐘的時間。請勿離開頁面或在相同的瀏覽器索引標籤中開啟不同的頁面。如果變更成功，在頁面頂端會顯示綠色成功橫幅。等待成功或失敗橫幅顯示在頁面上，然後再繼續。

   如果對部分或所有資源的標籤變更失敗，請參閱疑難排解標籤變更。在您解決標籤變更失敗的根本原因 （ 例如許可不足 ） 之後，您可以重試標籤變更失敗的資源上的標籤變更。如需詳細資訊，請參閱the section called “重試失敗的標籤變更”。

# 在 IAM 許可政策中使用標籤

AWS Identity and Access Management (IAM) 是您用來建立和管理許可政策 AWS 服務 的 ，以決定誰可以存取您的 AWS 資源。每次嘗試存取 AWS 服務或讀取或寫入 AWS 資源時，都會由 IAM 政策控制存取。

這些政策可讓您提供對 資源的精細存取。您可以使用其中一項功能來微調此存取，這是政策的 `Condition` 元素。此元素可讓您指定必須符合請求的條件，以判斷請求是否可以繼續。您可以使用 `Condition`元素檢查的項目如下：

- 連接至提出請求之使用者或角色的標籤。
- 連接至資源的標籤是請求的物件。

## 標籤和屬性型存取控制

標籤可能是 AWS 存取控制策略的重要部分。如需在屬性型存取控制 (ABAC) 策略中使用標籤做為屬性的資訊，請參閱《IAM 使用者指南》中的使用標籤控制對 AWS 資源的存取，以及使用標籤控制對 和 IAM 使用者和角色的存取。

有一個完整的教學課程，說明如何在 IAM 教學課程中使用標籤授予對不同專案和群組的存取權：在 使用者指南中根據標籤定義存取 AWS 資源的許可。 AWS Identity and Access Management

如果您使用以 SAML 為基礎的身分提供者 (IdP) 進行單一登入，您可以將標籤連接至提供使用者存取權的擔任角色。如需詳細資訊，請參閱《 AWS Identity and Access Management 使用者指南》中的 IAM 教學課程：使用 ABAC 的 SAML 工作階段標籤。

## 標籤相關條件索引鍵

下表說明您可以在 IAM 許可政策中使用的條件金鑰，以根據標籤控制存取。這些條件索引鍵可讓您執行下列動作：

- 比較呼叫 操作之委託人的標籤。
- 將提供的標籤與 操作進行比較，做為 參數。
- 比較連接到 操作將存取之資源的標籤。

如需條件金鑰及其使用方式的完整詳細資訊，請參閱條件金鑰名稱欄中連結的頁面。

| 條件索引鍵名稱 | 描述 |
| --- | --- |
| aws:PrincipalTag | 將連接至發出請求的委託人 (IAM 角色或使用者 ) 的標籤與您在政策中指定的標籤進行比較。 |
| aws:RequestTag | 將傳遞給請求的標籤鍵/值對做為參數與您在政策中指定的標籤鍵/值對進行比較。 |
| aws:ResourceTag | 將連接至資源的鍵值對與您在政策中指定的標籤鍵值對進行比較。 |
| aws:TagKeys | 僅比較請求中的標籤金鑰與您在政策中指定的金鑰。 |

# 使用標籤的範例 IAM 政策

Example 範例 1：強制使用者在建立資源時連接特定標籤

下列範例 IAM 許可政策示範如何強制建立或修改 IAM 政策標籤的使用者將標籤包含金鑰 Owner。此外，政策要求標籤的值設定為與目前連接至呼叫主體的Owner標籤相同的值。若要讓此策略運作，所有主體都必須連接Owner標籤，而且必須防止使用者修改該標籤。如果嘗試建立或修改政策而未包含Owner標籤，則政策不相符，且不允許操作。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "TagCustomerManagedPolicies",
            "Effect": "Allow",
            "Action": [
                "iam:CreatePolicy",
                "iam:TagPolicy"
            ],
            "Resource": "arn:aws:iam::123456789012:policy/*",
            "Condition": {
                "StringEquals": {"aws:RequestTag/Owner": "${aws:PrincipalTag/Owner}"}
            }
        }
    ]
}
```

Example 範例 2：使用標籤將資源的存取限制為其「擁有者」

下列範例 IAM 許可政策僅在呼叫主體標記的標籤`project`值與執行個體相同時，才允許使用者停止執行中的 Amazon EC2 執行個體。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor1",
      "Effect": "Allow",
      "Action": [
        "ec2:StopInstances"
      ],
      "Resource": [
        "arn:aws:iam::123456789012:instance/*"
      ],
      "Condition": {
        "StringEquals": {"aws:ResourceTag/project": "${aws:PrincipalTag/project}"}
      }
    }
  ]
}
```

此範例是屬性型存取控制 (ABAC) 的範例。如需使用 IAM 政策實作標籤型存取控制策略的詳細資訊和其他範例，請參閱 AWS Identity and Access Management 使用者指南中的下列主題：

- 使用標籤控制對 AWS 資源的存取
- 使用標籤控制對 IAM 使用者和角色的存取
- IAM 教學課程：定義根據標籤存取 AWS 資源的許可 – 示範如何使用多個標籤授予不同專案和群組的存取權。

# AWS Organizations 標籤政策

標籤政策是您在 中建立的一種政策 AWS Organizations。您可以使用標籤政策來協助標準化組織帳戶中資源的標籤。若要使用標籤政策，建議您遵循 AWS Organizations 使用者指南中的標籤政策入門中所述的工作流程。如該頁面所述，建議的工作流程包括尋找和更正不合規的標籤。若要完成這些任務，請使用標籤編輯器主控台。

## 先決條件和許可

在評估標籤編輯器中標籤政策的合規性之前，您必須滿足要求並設定必要的許可。

主題

- 評估標籤政策合規性的先決條件
- 評估帳戶合規的許可
- 評估整個組織合規的許可
- 報告儲存的 Amazon S3 儲存貯體政策

### 評估標籤政策合規性的先決條件

評估標籤政策的合規性需要下列項目：

- 您必須先在 中啟用 功能 AWS Organizations，並建立和連接標籤政策。如需詳細資訊，請參閱AWS Organizations 《 使用者指南》中的下列頁面：
  - 管理標籤政策的先決條件和許可
  - 啟用標籤政策
  - 標籤政策入門
- 若要尋找帳戶資源上的不合規標籤，您需要該帳戶的登入憑證和 中列出的許可評估帳戶合規的許可。
- 若要評估整個組織的合規，您需要組織的管理帳戶的登入憑證和 中列出的許可評估整個組織合規的許可 。您只能向 AWS 區域 美國東部 （維吉尼亞北部） 請求合規報告。

### 評估帳戶合規的許可

在帳戶資源上尋找不合規的標籤需要下列許可：

- organizations:DescribeEffectivePolicy – 取得帳戶有效標籤政策的內容。
- tag:GetResources – 取得不符合附加標籤政策的資源清單。
- tag:TagResources – 新增或更新標籤。您也需要服務特定的許可才能建立標籤。例如，若要標記 Amazon Elastic Compute Cloud (Amazon EC2) 中的資源，您需要 的許可ec2:CreateTags。
- tag:UnTagResources – 移除標籤。您也需要服務特定的許可才能移除標籤。例如，若要取消標記 Amazon EC2 中的資源，您需要 的許可ec2:DeleteTags。

下列範例 AWS Identity and Access Management (IAM) 政策提供評估帳戶標籤合規的許可。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EvaluateAccountCompliance",
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeEffectivePolicy",
                "tag:GetResources",
                "tag:TagResources",
                "tag:UnTagResources"
            ],
            "Resource": "*"
        }
    ]
}
```

如需有關 IAM 政策和許可的詳細資訊，請參閱 IAM 使用者指南。

## 評估整個組織合規的許可

評估整個組織的標籤政策合規性需要下列許可：

- organizations:DescribeEffectivePolicy – 取得連接到組織、組織單位 (OU) 或帳戶的標籤政策內容。
- tag:GetComplianceSummary – 取得組織中所有帳戶中不合規資源的摘要。
- tag:StartReportCreation – 將最新的合規評估結果匯出至 檔案。每 48 小時會評估整個組織的合規。
- tag:DescribeReportCreation – 檢查報告建立的狀態。

- `s3:ListAllMyBuckets` — 協助存取整個組織的合規報告。
- `s3:GetBucketAcl` – 檢查接收合規報告的 Amazon S3 儲存貯體的存取控制清單 (ACL)。
- `s3:GetObject` – 從服務擁有的 Amazon S3 儲存貯體擷取合規報告。
- `s3:PutObject` – 將合規報告放入指定的 Amazon S3 儲存貯體。

如果交付報告的 Amazon S3 儲存貯體是透過 SSE-KMS 加密，您還必須擁有該儲存貯體的`kms:GenerateDataKey`許可。

下列範例 IAM 政策提供評估整個組織合規的許可。將每個`####`取代為您自己的資訊：

- *`bucket_name`* – 您的 Amazon S3 儲存貯體名稱
- *`organization_id`* – 組織的 ID

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EvaluateAccountCompliance",
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeEffectivePolicy",
                "tag:StartReportCreation",
                "tag:DescribeReportCreation",
                "tag:GetComplianceSummary",
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*"
        },
        {
            "Sid": "GetBucketAclForReportDelivery",
            "Effect": "Allow",
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::bucket_name",
            "Condition": {
                "StringEquals": {
                    "aws:CalledViaLast": "tagpolicies.tag.amazonaws.com"
                }
            }
        },
        {
```

```
            "Sid": "GetObjectForReportDelivery",
            "Effect": "Allow",
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::*/tag-policy-compliance-reports/*",
            "Condition": {
                "StringEquals": {
                    "aws:CalledViaLast": "tagpolicies.tag.amazonaws.com"
                }
            }
        },
        {
            "Sid": "PutObjectForReportDelivery",
            "Effect": "Allow",
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::bucket_name/AwsTagPolicies/organization_id/*",
            "Condition": {
                "StringEquals": {
                    "aws:CalledViaLast": "tagpolicies.tag.amazonaws.com"
                },
                "StringLike": {
                    "s3:x-amz-copy-source": "*/tag-policy-compliance-reports/*"
                }
            }
        }
    ]
}
```

如需有關 IAM 政策和許可的詳細資訊，請參閱 IAM 使用者指南。

## 報告儲存的 Amazon S3 儲存貯體政策

若要建立整個組織的合規報告，您用來呼叫 `StartReportCreation` API 的身分必須能夠存取美國東部（維吉尼亞北部）區域的 Amazon Simple Storage Service (Amazon S3) 儲存貯體來存放報告。標籤政策使用呼叫身分的登入資料，將合規報告交付至指定的儲存貯體。

如果用於呼叫 `StartReportCreation` API 的儲存貯體和身分屬於同一個帳戶，則此使用案例不需要其他 Amazon S3 儲存貯體政策。

如果與用於呼叫 `StartReportCreation` API 的身分相關聯的帳戶與擁有 Amazon S3 儲存貯體的帳戶不同，則必須將下列儲存貯體政策連接至儲存貯體。將每個*####*取代為您自己的資訊：

- *bucket_name* – 您的 Amazon S3 儲存貯體名稱

- *organization_id* – 組織的 ID
- *identity_ARN* – 用來呼叫 StartReportCreation API 的 IAM 身分 ARN

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CrossAccountTagPolicyACL",
            "Effect": "Allow",
            "Principal": {
                "AWS": "identity_ARN"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::bucket_name"
        },
        {
            "Sid": "CrossAccountTagPolicyBucketDelivery",
            "Effect": "Allow",
            "Principal": {
                "AWS": "identity_ARN"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::bucket_name/AwsTagPolicies/organization_id/*"
        }
    ]
}
```

# 評估帳戶的合規性

您可以使用其有效的標籤政策來評估組織中 帳戶的合規性。

> **Important**
>
> 未標記的資源由於不合規而無法出現在結果中。
> 若要尋找帳戶中未標記的資源，請使用 AWS 資源總管 搭配使用 的查詢**tag:none**。如需詳細資訊，請參閱AWS 資源總管 《 使用者指南》中的搜尋未標記的資源。

有效的標籤政策會指定套用至帳戶的標記規則。有效的標籤政策是帳戶繼承的任何標籤政策的彙總，加上直接連接到帳戶的任何標籤政策。當您將標籤政策連接至組織根時，該標籤政策會套用至組織中的所有帳戶。當您將標籤政策連接到組織單位 (OU) 時，它適用於屬於 OUs 的所有帳戶和 OU。

> **Note**
>
> 如果您尚未建立標籤政策，請參閱AWS Organizations 《 使用者指南》中的標籤政策入門。

若要尋找不合規標籤，您必須具有下列許可：

- `organizations:DescribeEffectivePolicy`
- `tag:GetResources`
- `tag:TagResources`
- `tag:UntagResources`

評估帳戶對其有效標籤政策的合規性 （ 主控台 ）

1. 登入您要檢查其合規性的帳戶時，請開啟標籤政策主控台。
2. 有效標籤政策區段會顯示政策上次更新的時間，以及定義的標籤索引鍵。您可以展開標籤索引鍵，以查看其值、案例處理，以及是否針對特定資源類型強制執行值的相關資訊。

   > **Note**
   >
   > 如果您已登入 管理帳戶，則需要選擇帳戶以查看其有效的政策並檢視合規資訊。

3. 在具有不合規標籤的資源區段中，指定 AWS 區域 要搜尋哪些不合規標籤。您也可以選擇依資源類型搜尋。然後選擇搜尋資源。

   即時結果會顯示在搜尋結果區段中。若要變更每個頁面或要顯示的資料欄傳回的結果數量，請選擇設定圖示。
4. 在搜尋結果中，選取具有不合規標籤的資源。
5. 在列出資源標籤的對話方塊中，選擇超連結以開啟資源建立 AWS 服務 所在的 。從該主控台更正不合規標籤。

> **Tip**
>
> 如果您不確定哪些標籤不合規，請前往標籤政策主控台中帳戶的有效標籤政策區段。您可以展開標籤索引鍵以檢視其標記規則。

6. 重複尋找和更正標籤的程序，直到您關心的帳戶資源在每個區域中都符合規範。

### 尋找不合規標籤 (AWS CLI， AWS API)

使用以下命令和操作來尋找不合規的標籤：

- AWS Command Line Interface (AWS CLI):
  - aws resourcegroupstaggingapi get-resources
  - aws resourcegroupstaggingapi tag-resources
  - aws resourcegroupstaggingapi untag-resources

  如需在 中使用標籤政策的完整程序 AWS CLI，請參閱《 AWS Organizations 使用者指南》中的使用標籤政策 AWS CLI。
- AWS Resource Groups Tagging API:
  - GetResources
  - TagResources
  - UntagResources

### 後續步驟

建議您重複尋找和修正合規問題的程序。繼續，直到您關注的帳戶資源符合每個區域中的有效標籤政策。

尋找和更正不合規標籤是基於多種原因的反覆程序，包括下列項目：

- 您的組織使用標籤政策可能會隨著時間演進。
- 建立資源時，需要一些時間才能在組織中實現變更。
- 每當建立新資源或將新標籤指派給資源時，合規都可以變更。
- 每當標籤政策連接至或從中分離時，帳戶的有效標籤政策都會更新。每當發生變更，以標記帳戶繼承的政策時，也會更新有效的標籤政策。

如果您以組織中的管理帳戶身分登入，您也可以產生報告。此報告會顯示組織帳戶中所有已標記資源的相關資訊。如需詳細資訊，請參閱評估整個組織的合規。

# 評估整個組織的合規

您可以評估組織對其有效標籤政策的合規性。您可以產生報告，列出整個組織中帳戶中所有已標記的資源，以及每個資源是否符合有效的標籤政策。

> **Important**
>
> 未標記的資源由於不合規而無法出現在結果中。
> 若要尋找帳戶中未標記的資源，請使用 AWS 資源總管 搭配使用 的查詢**tag:none**。如需詳細資訊，請參閱AWS 資源總管 《 使用者指南》中的搜尋未標記的資源。

您只能從組織的管理帳戶產生報告us-east-1 AWS 區域 。產生報告的帳戶必須能夠存取美國東部 （維吉尼亞北部） 區域中的 Amazon S3 儲存貯體。儲存貯體必須具有連接的儲存貯體政策，如 Amazon S3 儲存貯體政策中所示，以存放報告。

若要產生整個組織的合規報告，您必須具有下列許可：

- `organizations:DescribeEffectivePolicy`
- `tag:GetComplianceSummary`
- `tag:StartReportCreation`
- `tag:DescribeReportCreation`
- `s3:ListAllMyBuckets`
- `s3:GetBucketAcl`
- `s3:GetObject`
- `s3:PutObject`

如需顯示這些許可的範例 IAM 政策，請檢閱評估整個組織合規的許可。

產生整個組織的合規報告 （主控台）

1. 開啟標籤政策主控台。
2. 選擇此組織根標籤，並在頁面底部附近，選擇產生報告。

3. 在產生報告畫面上，指定要存放報告的位置。
4. 選擇開始匯出。

當報告完成時，您可以從組織根標籤上的不合規報告區段下載報告。

> **備註**
>
> 每 48 小時會評估整個組織的合規。這會導致下列情況：
>
> - 標籤政策或資源的變更最多可能需要 48 小時才會顯示在整個組織的合規報告中。例如，假設您有一個標籤政策為某個資源類型定義新的標準化標籤。沒有此標籤的該類型的資源在報告中最多可顯示為合規 48 小時。
> - 雖然您可以隨時產生報告，但在下一次評估完成之前，報告結果不會更新。
> - NoncompliantKeys 欄列出資源上不符合有效標籤政策的標籤金鑰。
> - KeysWithNonCompliantValues 資料欄列出在資源上具有不正確案例處理或不合規值的有效政策中定義的金鑰。
> - 如果您關閉 AWS 帳戶 作為組織成員的 ，它可以繼續出現在標籤合規報告中長達 90 天。

產生整個組織的合規報告 (AWS CLI， AWS API)

使用以下命令和操作來產生整個組織的合規報告、檢查其狀態，並檢視報告：

- AWS Command Line Interface AWS CLI):
  - aws resourcegroupstaggingapi start-report-creation
  - aws resourcegroupstaggingapi describe-report-creation
  - aws resourcegroupstaggingapi get-compliance-summary

  如需在 中使用標籤政策的完整程序 AWS CLI，請參閱《 AWS Organizations 使用者指南》中的使用標籤政策 AWS CLI。
- AWS API：
  - StartReportCreation
  - DescribeReportCreation
  - GetComplianceSummary

# 使用無伺服器工作流程和 Amazon EventBridge 監控標籤變更

Amazon EventBridge 支援 AWS 資源上的標籤變更。使用此 EventBridge 類型，您可以建置 EventBridge 規則以符合標籤變更，並將事件路由至一或多個目標。例如，目標可能是叫用自動化工作流程的 AWS Lambda 函數。本主題提供使用 Lambda 建置經濟實惠的無伺服器解決方案的教學課程，以安全地處理 AWS 資源上的標籤變更。

## 標籤變更會產生 EventBridge 事件

EventBridge 提供近乎即時的系統事件串流，描述資源的變更 AWS 。許多 AWS 資源都支援標籤，這些標籤是自訂、使用者定義的屬性，可輕鬆整理和分類 AWS 資源。標籤的常見使用案例是成本分配分類、存取控制安全性和自動化。

使用 EventBridge，您可以監控標籤的變更，並追蹤資源上的 AWS 標籤狀態。先前，為了實現類似的功能，您可能已經持續輪詢 APIs和協調多個呼叫。現在，任何標籤的變更，包括個別服務 APIs、標籤編輯器和標記 API，都會在資源事件時啟動標籤變更。下列範例顯示標籤變更提示的典型 EventBridge 事件。它會顯示新的、已更新或刪除的標籤索引鍵及其相關聯的值。

```
{
  "version": "0",
  "id": "bddcf1d6-0251-35a1-aab0-adc1fb47c11c",
  "detail-type": "Tag Change on Resource",
  "source": "aws.tag",
  "account": "123456789012",
  "time": "2018-09-18T20:41:38Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaaa"
  ],
  "detail": {
    "changed-tag-keys": [
      "a-new-key",
      "an-updated-key",
      "a-deleted-key"
    ],
    "tags": {
      "a-new-key": "tag-value-on-new-key-just-added",
      "an-updated-key": "tag-value-was-just-changed",
      "an-unchanged-key": "tag-value-still-the-same"
    },
```

```
    "service": "ec2",
    "resource-type": "instance",
    "version": 3,
  }
}
```

所有 EventBridge 事件都有相同的最上層欄位：

- 版本 – 根據預設，此值在所有事件中都會設為 0（零）。
- id – 為每個事件產生唯一的值。這有助於追蹤事件，因為它們會在規則移動到目標並進行處理。
- details-type – 識別與 source 欄位結合出現在詳細資訊欄位中的欄位和值。
- source – 識別做為事件來源的服務。標籤變更的來源為 aws.tag。
- time – 事件的時間戳記。
- region – 識別 AWS 區域 事件的來源。
- 資源 – 此 JSON 陣列包含 Amazon Resource Name (ARNs)，可識別事件中涉及的資源。這是標籤已變更的資源。
- 詳細資訊 – JSON 物件，其內容會根據事件類型而有所不同。對於資源上的標籤變更，會包含下列詳細欄位：
  - changed-tag-keys – 此事件變更的標籤索引鍵。
  - service – 資源所屬的服務。在此範例中，服務為 ec2，即 Amazon EC2。
  - resource-type – 服務的資源類型。在此範例中，它是 Amazon EC2 執行個體。
  - 版本 – 標籤集的版本。版本從 1 開始，並在標籤變更時遞增。您可以使用 版本來驗證標籤變更事件的順序。
  - 標籤 – 變更後連接至資源的標籤。

如需詳細資訊，請參閱「Amazon EventBridge 使用者指南」中的「Amazon EventBridge 事件模式」。

透過使用 EventBridge，您可以根據不同的欄位建立符合特定事件模式的規則。我們示範如何在教學課程中執行此操作。此外，我們會示範如何在指定的標籤未連接至執行個體時自動停止 Amazon EC2 執行個體。我們使用 EventBridge 欄位來建立模式，以符合啟動 Lambda 函數之執行個體的標籤事件。

## Lambda 和無伺服器

AWS Lambda 遵循無伺服器範例，在雲端中執行程式碼。只有在需要時才執行程式碼，而不考慮伺服器。您只需為所使用的確切運算時間付費。即使稱為無伺服器，也不表示沒有伺服器。在此內容中，無

伺服器表示您不需要佈建、設定或管理用來執行程式碼的伺服器。 會為您 AWS 執行所有這些操作，因此您可以專注於程式碼。如需 Lambda 的詳細資訊，請參閱AWS Lambda 產品概觀。

# 教學課程：自動停止缺少必要標籤的 Amazon EC2 執行個體

隨著資源集區和 AWS 帳戶 您管理 AWS 的資源，您可以使用標籤來更輕鬆地分類資源。標籤通常用於成本分配和安全性等關鍵使用案例。若要有效管理 AWS 資源，您的資源需要一致標記。通常，當佈建資源時，它會取得所有適當的標籤。不過，稍後的程序可能會導致標籤變更，從公司標籤政策產生偏離。透過監控標籤的變更，您可以發現標籤偏離並立即回應。這可讓您更有信心，取決於您的資源進行適當分類的程序將產生所需的結果。

下列範例示範如何監控 Amazon EC2 執行個體上的標籤變更，以確認指定的執行個體是否持續擁有所需的標籤。如果執行個體的標籤變更，且執行個體不再具有所需的標籤，則會叫用 Lambda 函數來自動關閉執行個體。為什麼要這麼做？ 它可確保所有資源都根據您的公司標籤政策進行標記，以實現有效的成本分配，或能夠根據屬性型存取控制 (ABAC) 信任安全性。

> **Important**
>
> 我們強烈建議您在不會意外關閉重要執行個體的非生產帳戶中執行此教學課程。
> 本教學課程的範例程式碼刻意限制此案例的影響，僅限於執行個體 IDs 清單上的執行個體。您必須使用您願意為測試關閉IDs 來更新清單。這有助於確保您不會意外關閉 區域中的每個執行個體 AWS 帳戶。
> 測試之後，請確定您的所有執行個體都根據公司的標記策略進行標記。然後，您可以移除程式碼，將函數限制為清單上的執行個體 IDs。

此範例使用 JavaScript和 16Node.js.x 版本的 。此範例使用範例 AWS 帳戶 ID 123456789012 和 AWS 區域 美國東部 （維吉尼亞北部） (`us-east-1`)。將它們取代為您自己的測試帳戶 ID 和區域。

> **Note**
>
> 如果您的主控台預設使用不同的區域，請務必在每次變更主控台時，在此教學課程中切換您使用的區域。此教學課程失敗的常見原因是在兩個不同的區域中具有執行個體和函數。

如果您使用與 不同的區域`us-east-1`，請確定將下列程式碼範例中的所有參考變更為您選擇的區域。

主題

## 步驟 1. 建立 Lambda 函式

建立 Lambda 函數

1. 開啟 AWS Lambda 管理主控台。
2. 選擇建立函數，然後選擇從頭開始撰寫。
3. 針對 Function name (函數名稱)，輸入 **`AutoEC2Termination`**。
4. 針對 執行時間，請選擇 Node.js 16.x。
5. 將所有其他欄位保留在其預設值，然後選擇建立函數。
6. 在`AutoEC2Termination`詳細資訊頁面的程式碼索引標籤上，開啟 index.js 檔案以檢視其程式碼。

   - 如果開啟具有 index.js 的索引標籤，您可以選擇該索引標籤中的編輯方塊來編輯其程式碼。
   - 如果具有 index.js 的索引標籤未開啟，請在導覽窗格中的 AutoEC2Terminator 資料夾下按兩下 index.js 檔案。然後選擇開啟。
7. 在 index.js 索引標籤中，將下列程式碼貼到編輯器方塊中，取代任何已存在的程式碼。

   將 值取代`RegionToMonitor`為您要在其中執行此函數的區域。

```
// Set the following line to specify which Region's instances you want to monitor
// Only instances in this Region are succesfully stopped on a match

const RegionToMonitor = "us-east-1"

// Specify the instance ARNs to check.
// This limits the function for safety to avoid the tutorial shutting down all
 instances in account
// The first ARN is a "dummy" that matches the test event you create in Step 3.
// Replace the second ARN with one that matches a real instance that you want to
 monitor and that you can
```

```
// safely stop

const InstanceList = [
    "i-0000000aaaaaaaaaa",
    "i-05db4466d02744f07"
];

// The tag key name and value that marks a "valid" instance. Instances in the
 previous list that
// do NOT have the following tag key and value are stopped by this function

const ValidKeyName = "valid-key";
const ValidKeyValue = "valid-value";

// Load and configure the AWS SDK
const AWS = require('aws-sdk');
// Set the AWS Region
AWS.config.update({region: RegionToMonitor});
// Create EC2 service object.
const ec2 = new AWS.EC2({apiVersion: '2016-11-15'});

exports.handler = (event, context, callback) => {

  // Retrieve the details of the reported event.
  var detail = event.detail;
  var tags = detail["tags"];
  var service = detail["service"];
  var resourceType = detail["resource-type"];
  var resource = event.resources[0];
  var resourceSplit = resource.split("/");
  var instanceId = resourceSplit[resourceSplit.length - 1];

  // If this event is not for an EC2 resource, then do nothing.
  if (!(service === "ec2")) {
    console.log("Event not for correct service -- no action (", service, ")" );
    return;
  }

  // If this event is not about an instance, then do nothing.
  if (!(resourceType === "instance")) {
    console.log("Event not for correct resource type -- no action (", resourceType,
 ")" );
    return;
  }
```

```
 // CAUTION - Removing the following 'if' statement causes the function to run
against
 //           every EC2 instance in the specified Region in the calling AWS ##.
 //           If you do this and an instance is not tagged with the approved tag
key
 //           and value, this function stops that instance.

 // If this event is not for the ARN of an instance in our include list, then do
nothing.
 if (InstanceList.indexOf(instanceId)<0) {
   console.log("Event not for one of the monitored instances -- no action (",
resource, ")");
   return;
 }

 console.log("Tags changed on monitored EC2 instance (",instanceId,")");

 // Check attached tags for expected tag key and value pair
 if ( tags.hasOwnProperty(ValidKeyName) && tags[ValidKeyName] == "valid-value"){
   // Required tags ARE present
   console.log("The instance has the required tag key and value -- no action");
   callback(null, "no action");
   return;
 }

 // Required tags NOT present
 console.log("This instance is missing the required tag key or value -- attempting
to stop the instance");

 var params = {
   InstanceIds: [instanceId],
   DryRun: true
 };

 // call EC2 to stop the selected instances
 ec2.stopInstances(params, function(err, data) {
   if (err && err.code === 'DryRunOperation') {
     // dryrun succeeded, so proceed with "real" stop operation
     params.DryRun = false;
     ec2.stopInstances(params, function(err, data) {
       if (err) {
         console.log("Failed to stop instance");
         callback(err, "fail");
```

```
        } else if (data) {
          console.log("Successfully stopped instance", data.StoppingInstances);
          callback(null, "Success");
        }
      });
    } else {
      console.log("Dryrun attempt failed");
      callback(err);
    }
  });
};
```

8. 選擇部署以儲存變更，並啟用新版本的函數。

此 Lambda 函數會檢查 Amazon EC2 執行個體的標籤，如 EventBridge 中的標籤變更事件所報告。在此範例中，如果事件中的執行個體缺少所需的標籤索引鍵，`valid-key`或該標籤沒有值 `valid-value`，則函數會嘗試停止執行個體。您可以變更此邏輯檢查，或您自己特定使用案例的標籤需求。

在瀏覽器中保持 Lambda 主控台視窗開啟。

## 步驟 2. 設定所需的 IAM 許可

在函數成功執行之前，您必須授予函數停止 EC2 執行個體的許可。 AWS 提供的角色lambda_basic_execution沒有該許可。在本教學課程中，您會修改連接至函數執行角色的預設 IAM 許可政策，該角色名為 `AutoEC2Termination-role-`*`uniqueid`*。本教學課程所需的最低額外許可為 `ec2:StopInstances`。

如需建立 Amazon EC2 特定 IAM 政策的詳細資訊，請參閱《IAM 使用者指南》中的 Amazon EC2：允許啟動或停止 EC2 執行個體，並以程式設計方式在主控台中修改安全群組。

建立 IAM 許可政策並將其連接至 Lambda 函數的執行角色

1. 在不同的瀏覽器索引標籤或視窗中，開啟 IAM 主控台的角色頁面。
2. 開始輸入角色名稱 **`AutoEC2Termination`**，並在它出現在清單中時，選擇角色名稱。
3. 在角色的摘要頁面上，選擇許可索引標籤，然後選擇已連接的一個政策的名稱。
4. 在政策的摘要頁面上，選擇編輯政策。
5. 在視覺化編輯器索引標籤上，選擇新增其他許可。
6. 在 Service (服務) 欄位中，選擇 EC2。

7. 針對動作，選擇 StopInstances。您可以在搜尋列**Stop**中輸入 ，然後在出現StopInstances時選擇 。
8. 針對資源，選擇所有資源，選擇檢閱政策，然後選擇儲存變更。

   這會自動建立新的政策版本，並將該版本設定為預設值。

   您的最終政策看起來應該類似於下列範例。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "ec2:StopInstances",
            "Resource": "*"
        },
        {
            "Sid": "VisualEditor1",
            "Effect": "Allow",
            "Action": "logs:CreateLogGroup",
            "Resource": "arn:aws:logs:us-east-1:123456789012:*"
        },
        {
            "Sid": "VisualEditor2",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
            "Resource": "arn:aws:logs:us-east-1:123456789012:log-group:/aws/lambda/
AutoEC2Termination:*"
        }
    ]
}
```

## 步驟 3。對您的 Lambda 函數進行初步測試

在此步驟中，您會將測試事件提交至 函數。Lambda 測試功能的運作方式是提交手動提供的測試事件。函數會處理測試事件，就像事件來自 EventBridge。您可以定義具有不同值的多個測試事件，以執

行程式碼的所有不同部分。在此步驟中，您會提交測試事件，指出 Amazon EC2 執行個體的標籤已變更，且新標籤不包含必要的標籤索引鍵和值。

測試您的 Lambda 函數

1. 使用 Lambda 主控台返回視窗或索引標籤，並開啟 AutoEC2Termination 函數的測試索引標籤。
2. 選擇建立新事件。
3. 事件名稱輸入 **SampleBadTagChangeEvent**。
4. 在事件 JSON 中，將文字取代為範例事件，如下列範例文字所示。您不需要修改帳戶、區域或執行個體 ID，此測試事件才能正常運作。

```
{
  "version": "0",
  "id": "bddcf1d6-0251-35a1-aab0-adc1fb47c11c",
  "detail-type": "Tag Change on Resource",
  "source": "aws.tag",
  "account": "123456789012",
  "time": "2018-09-18T20:41:38Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaaa"
  ],
  "detail": {
    "changed-tag-keys": [
      "valid-key"
    ],
    "tags": {
      "valid-key": "NOT-valid-value"
    },
    "service": "ec2",
    "resource-type": "instance",
    "version": 3
  }
}
```

5. 選擇 **關閉** ，然後選擇 **測試** 。

   測試似乎失敗，但沒關係。

   您應該會在回應下的執行結果索引標籤中看到下列錯誤。

```
{
```

```
  "errorType": "InvalidInstanceID.NotFound",
  "errorMessage": "The instance ID 'i-0000000aaaaaaaaaa' does not exist",
  ...
}
```

發生錯誤是因為測試事件中指定的執行個體不存在。

執行結果索引標籤上的資訊，在 函數日誌 區段中，示範您的 Lambda 函數成功嘗試停止 EC2 執行個體。不過，它失敗，因為程式碼一開始會嘗試停止執行個體DryRun的操作，這表示執行個體 ID 無效。

```
START RequestId: 390c1f8d-0d9b-4b44-b087-8de64479ab44 Version: $LATEST
2022-11-30T20:17:30.427Z    390c1f8d-0d9b-4b44-b087-8de64479ab44    INFO    Tags
 changed on monitored EC2 instance ( i-0000000aaaaaaaaaa )
2022-11-30T20:17:30.427Z    390c1f8d-0d9b-4b44-b087-8de64479ab44    INFO    This
 instance is missing the required tag key or value -- attempting to stop the
 instance
2022-11-30T20:17:31.206Z    390c1f8d-0d9b-4b44-b087-8de64479ab44    INFO    Dryrun
 attempt failed
2022-11-30T20:17:31.207Z    390c1f8d-0d9b-4b44-b087-8de64479ab44    ERROR   Invoke
 Error     {"errorType":"InvalidInstanceID.NotFound","errorMessage":"The instance
 ID 'i-0000000aaaaaaaaaa' does not
 exist","code":"InvalidInstanceID.NotFound","message":"The instance ID
 'i-0000000aaaaaaaaaa' does not
 exist","time":"2022-11-30T20:17:31.205Z","requestId":"a5192c3b-142d-4cec-
bdbc-685a9b7c7abf","statusCode":400,"retryable":false,"retryDelay":36.87870631147607,"stack
["InvalidInstanceID.NotFound: The instance ID 'i-0000000aaaaaaaaaa' does
 not exist","    at Request.extractError (/var/runtime/node_modules/aws-sdk/
lib/services/ec2.js:50:35)","    at Request.callListeners (/var/runtime/
node_modules/aws-sdk/lib/sequential_executor.js:106:20)","    at Request.emit
 (/var/runtime/node_modules/aws-sdk/lib/sequential_executor.js:78:10)","    at
 Request.emit (/var/runtime/node_modules/aws-sdk/lib/request.js:686:14)","    at
 Request.transition (/var/runtime/node_modules/aws-sdk/lib/request.js:22:10)","
    at AcceptorStateMachine.runTo (/var/runtime/node_modules/aws-sdk/lib/
state_machine.js:14:12)","    at /var/runtime/node_modules/aws-sdk/lib/
state_machine.js:26:10","    at Request.<anonymous> (/var/runtime/node_modules/aws-
sdk/lib/request.js:38:9)","    at Request.<anonymous> (/var/runtime/node_modules/
aws-sdk/lib/request.js:688:12)","    at Request.callListeners (/var/runtime/
node_modules/aws-sdk/lib/sequential_executor.js:116:18)"]}
END RequestId: 390c1f8d-0d9b-4b44-b087-8de64479ab44
```

6. 若要證明程式碼不會在使用正確的標籤時嘗試停止執行個體，您可以建立並提交另一個測試事件。

選擇程式碼來源上方的測試索引標籤。主控台會顯示您現有的 SampleBadTagChangeEvent 測試事件。

7. 選擇建立新事件。
8. 針對 Event name (事件名稱)，輸入 **SampleGoodTagChangeEvent**。
9. 在第 17 行中，刪除 **NOT-** 以將值變更為 **valid-value**。
10. 在測試事件視窗頂端，選擇儲存，然後選擇測試。

輸出會顯示下列項目，示範 函數辨識有效標籤，且不會嘗試關閉執行個體。

```
START RequestId: 53631a49-2b54-42fe-bf61-85b9e91e86c4 Version: $LATEST
2022-12-01T23:24:12.244Z    53631a49-2b54-42fe-bf61-85b9e91e86c4    INFO    Tags
 changed on monitored EC2 instance ( i-0000000aaaaaaaaaa )
2022-12-01T23:24:12.244Z    53631a49-2b54-42fe-bf61-85b9e91e86c4    INFO    The
 instance has the required tag key and value -- no action
END RequestId: 53631a49-2b54-42fe-bf61-85b9e91e86c4
```

在瀏覽器中保持 Lambda 主控台開啟。

## 步驟 4. 建立啟動函數的 EventBridge 規則

現在，您可以建立符合事件的 EventBridge 規則，並指向 Lambda 函數。

若要建立 EventBridge 規則

1. 在不同的瀏覽器索引標籤或視窗中，開啟 EventBridge 主控台至建立規則頁面。
2. 針對名稱，輸入 **ec2-instance-rule**，然後選擇下一步。
3. 向下捲動至建立方法，然後選擇自訂模式 (JSON 編輯器)。
4. 在編輯方塊中，貼上下列模式文字，然後選擇下一步。

```
{
  "source": [
    "aws.tag"
  ],
  "detail-type": [
    "Tag Change on Resource"
  ],
  "detail": {
    "service": [
```

```
      "ec2"
    ],
    "resource-type": [
      "instance"
    ]
  }
}
```

此規則符合 Amazon EC2 執行個體Tag Change on Resource的事件，並叫用您在下一個步驟中指定為目標的任何項目。

5. 接著，新增您的 Lambda 函數做為目標。在目標 1 方塊中的選取目標下，選擇 Lambda 函數。
6. 在函數下，選擇您先前建立的 AutoEC2Termination 函數，然後選擇下一步。
7. 在設定標籤頁面上，選擇下一步。然後在檢閱和建立頁面上，選擇建立規則。這也會自動授予 EventBridge 調用指定 Lambda 函數的許可。

## 步驟 5. 測試完整的解決方案

您可以建立 EC2 執行個體並觀察變更標籤時會發生的情況，以測試最終結果。

使用實際執行個體測試監控解決方案

1. 開啟執行個體頁面的 Amazon EC2 主控台。
2. 建立 Amazon EC2 執行個體。啟動之前，請先使用 鍵valid-key和 值 附加標籤valid-value。如需有關如何建立和啟動執行個體的資訊，請參閱《Amazon EC2 使用者指南》中的步驟 1：啟動執行個體。在程序中，若要啟動執行個體，請在步驟 3 中輸入名稱標籤，也選擇新增其他標籤，選擇新增標籤，然後輸入 的金鑰 **valid-key**和 的值**valid-value**。如果此執行個體僅用於本教學課程的目的，且您打算在完成執行個體之後刪除此執行個體，則可以不使用金鑰對繼續。當您到達步驟 1 結尾時，請返回本教學課程；您不需要執行步驟 2：連線至執行個體。
3. 從主控台複製 InstanceId。
4. 從 Amazon EC2 主控台切換至 Lambda 主控台。選擇 AutoEC2Termination 函數，選擇程式碼索引標籤，然後選擇 index.js 索引標籤來編輯程式碼。
5. 貼上您從 Amazon EC2 主控台複製的值，InstanceList以變更 中的第二個項目。請確定該RegionToMonitor值符合包含您貼上之執行個體的 區域。
6. 選擇部署以啟用您的變更。函數現在已準備好透過指定區域中該執行個體的標籤變更來啟用。
7. 從 Lambda 主控台切換至 Amazon EC2 主控台。
8. 刪除 valid-key 標籤或變更該金鑰的值，以變更連接至執行個體的標籤。

> **Note**
>
> 如需如何在執行中的 Amazon EC2 執行個體上變更標籤的詳細資訊，請參閱《Amazon EC2 使用者指南》中的在個別資源上新增和刪除標籤。

9. 等待幾秒鐘，然後重新整理主控台。執行個體應該將其執行個體狀態變更為停止，然後變更為停止。
10. 使用您的 函數從 Amazon EC2 主控台切換到 Lambda 主控台，然後選擇監控索引標籤。
11. 選擇日誌索引標籤，然後在最近調用表格中，選擇 LogStream 欄中的最新項目。

    Amazon CloudWatch 主控台會開啟日誌事件頁面，以取得 Lambda 函數的最後一次調用。最後一個項目看起來應該類似於下列範例。

```
2022-11-30T12:03:57.544-08:00    START RequestId: b5befd18-2c41-43c8-
a320-3a4b2317cdac Version: $LATEST
2022-11-30T12:03:57.548-08:00    2022-11-30T20:03:57.548Z b5befd18-2c41-43c8-
a320-3a4b2317cdac INFO Tags changed on monitored EC2 instance ( arn:aws:ec2:us-
west-2:123456789012:instance/i-1234567890abcdef0 )
2022-11-30T12:03:57.548-08:00    2022-11-30T20:03:57.548Z b5befd18-2c41-43c8-
a320-3a4b2317cdac INFO This instance is missing the required tag key or value --
 attempting to stop the instance
2022-11-30T12:03:58.488-08:00    2022-11-30T20:03:58.488Z b5befd18-2c41-43c8-
a320-3a4b2317cdac INFO Successfully stopped instance [ { CurrentState: { Code: 64,
 Name: 'stopping' }, InstanceId: 'i-1234567890abcdef0', PreviousState: { Code: 16,
 Name: 'running' } } ]
2022-11-30T12:03:58.546-08:00    END RequestId: b5befd18-2c41-43c8-
a320-3a4b2317cdac
```

## 教學課程摘要

本教學課程示範如何建立 EventBridge 規則，以比對 Amazon EC2 執行個體資源事件上的標籤變更。規則指向 Lambda 函數，如果執行個體沒有所需的標籤，該函數會自動關閉執行個體。

Amazon EventBridge 支援 AWS 資源上的標籤變更，開啟了在許多資源中建置事件驅動型自動化的可能性 AWS 服務。將此功能與 結合 AWS Lambda ，為您提供工具來建置無伺服器解決方案，以安全地存取 AWS 資源、隨需擴展，而且符合成本效益。

tag-change-on-resource EventBridge 事件的其他可能使用案例包括：

- 如果有人從不尋常的 IP 地址存取您的資源，請啟動警告 – 使用標籤來存放存取您的資源的每個訪客的來源 IP 地址。標籤的變更會產生 CloudWatch 事件。您可以使用該事件，將來源 IP 地址與有效 IP 地址清單進行比較，並在來源 IP 地址無效時啟用警告電子郵件。
- 監控資源的標籤型存取控制是否有變更 – 如果您使用屬性（標籤）型存取控制 (ABAC) 設定資源的存取權，您可以使用標籤的任何變更所產生的 EventBridge 事件來提示安全團隊進行稽核。

# 對標籤變更進行故障診斷

當您嘗試在 Find resources to tag (尋找要加標籤的資源) 查詢結果中對所選資源套用或變更標籤時若發生錯誤，以下檢查清單可能有所幫助。

- 資源可能已經有最大數量的標籤。一般而言，資源最多可有 50 個使用者定義的標籤。 AWS 產生的標籤不會計入 50 個標籤上限。其他使用者可能會同時新增標籤到相同資源，而這可能導致資源的標籤數達到上限。
- 有些服務會對建立標籤允許不同字元集 (或對允許的字元集進行限制)。如果您使用特殊字元新增或變更標籤，請檢閱資源服務文件中的標籤需求，以確認服務允許這些字元。
- 您可能沒有修改資源標籤的許可。如果您沒有檢視資源上現有標籤的許可，則無法變更資源的標籤。
- 您可能沒有變更資源的許可。另一個管理員可能已限制對資源中繼資料進行變更。
- 另一個使用者或程序可能已編輯或刪除該資源。例如，假設資源在建立 AWS CloudFormation 堆疊時已啟動。如果堆疊已刪除或不再處於作用中狀態，則資源可能不再可用。
- 如果資源已離線或終止，或如果對資源的其他更新 (如軟體升級) 進行中，則標籤變更會不可行。
- 如果您在標籤變更完成之前關閉瀏覽器索引標籤或變更頁面，標籤變更可能會失敗。讓標籤變更完成，並等待成功或失敗橫幅顯示在頁面上，之後再離開頁面。
- 雖然 有速率限制 AWS Resource Groups Tagging API，但您標記的服務可能會施加不同的限制，您可能會在資源群組標記 API 限制之前達到。

# 重試失敗的標籤變更

如果標籤變更在至少一個所選資源上失敗，標籤編輯器會在頁面底部顯示紅色橫幅。橫幅會顯示所發生每種失敗類型的錯誤訊息。對於每個錯誤，橫幅會識別標籤編輯器無法變更標籤的特定資源。在您檢閱錯誤並進行故障診斷之後，請選擇資源上的重試失敗標籤變更，以僅重試標籤變更失敗的那些資源的變更。

# 標籤編輯器中的安全性

的雲端安全性 AWS 是最高優先順序。身為 AWS 客戶，您可以從資料中心和網路架構中受益，該架構旨在滿足最安全敏感組織的需求。

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

- 雲端的安全性 – AWS 負責保護在 AWS 服務 中執行的基礎設施 AWS 雲端。 AWS 也為您提供可安全使用的服務。在 AWS 合規計畫中，第三方稽核員會定期測試並驗證我們的安全功效。如需適用於標籤編輯器之合規計劃的詳細資訊，請參閱AWS 合規計劃範圍內的服務。
- 雲端安全性 – 您的責任取決於您使用 AWS 服務 的 。您也必須對其他因素負責，包括資料的機密性、您公司的要求和適用法律和法規。

本文件可協助您了解如何在使用標籤編輯器時套用共同責任模型。下列主題說明如何設定標籤編輯器以符合您的安全和合規目標。

主題

- 標籤編輯器中的資料保護
- 標籤編輯器的身分和存取管理
- 在標籤編輯器中記錄和監控
- 標籤編輯器的合規驗證
- 標籤編輯器中的彈性
- 標籤編輯器中的基礎設施安全性

## 標籤編輯器中的資料保護

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

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

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

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

## 資料加密

標記資訊不會加密。雖然未加密，標籤可以包含做為安全策略一部分使用的資訊，因此控制誰可以存取資源上的標籤非常重要。控制誰可以修改標籤尤其重要，因為此類存取可用於提升許可。

### 靜態加密

標籤編輯器沒有額外的隔離服務或網路流量方式。如適用，請使用 AWS 特定隔離。您可以在虛擬私有雲端 (VPC) 中使用標籤編輯器 API 和主控台，以協助最大化隱私權和基礎設施安全。

### 傳輸中加密

標籤編輯器資料會在傳輸到服務的內部資料庫以進行備份時加密。這不是使用者可設定的。

### 金鑰管理

標籤編輯器目前未與 整合 AWS Key Management Service ，且不支援 AWS KMS keys。

## 網際網路流量隱私權

標籤編輯器使用 HTTPS 進行標籤編輯器使用者與 之間的所有傳輸 AWS。標籤編輯器使用傳輸層安全性 (TLS) 1.3，但也支援 TLS 1.2。

# 標籤編輯器的身分和存取管理

AWS Identity and Access Management (IAM) 是一種 AWS 服務 ，可協助管理員安全地控制對 AWS 資源的存取。IAM 管理員可控制誰可以進行身分驗證 （ 登入 ） 和授權 （ 具有許可 ） 來使用標籤編輯器資源。IAM 是 AWS 服務 您可以免費使用的 。

主題



## 目標對象

使用方式 AWS Identity and Access Management (IAM) 會有所不同，取決於您在標籤編輯器中執行的工作。

服務使用者 – 如果您使用標籤編輯器服務來執行您的任務，則您的管理員會為您提供所需的登入資料和許可。當您使用更多標籤編輯器功能來執行工作時，您可能需要額外的許可。了解存取許可的管理方式可協助您向管理員請求正確的許可。如果您無法存取標籤編輯器中的功能，請參閱 標籤編輯器身分和存取的故障診斷。

服務管理員 – 如果您在公司負責標籤編輯器資源，您可能擁有標籤編輯器的完整存取權。您的任務是判斷您的服務使用者應存取哪些標籤編輯器功能和資源。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。若要進一步了解您的公司如何使用 IAM 搭配標籤編輯器，請參閱標籤編輯器如何與 IAM 搭配使用。

IAM 管理員 – 如果您是 IAM 管理員，建議您了解撰寫政策以管理標籤編輯器存取權的詳細資訊。若要檢視您可以在 IAM 中使用的標籤編輯器身分型政策範例，請參閱 標籤編輯器身分型政策範例。

## 使用身分驗證

身分驗證是您 AWS 使用身分憑證登入 的方式。您必須以 AWS 帳戶根使用者身分、IAM 使用者身分或擔任 IAM 角色身分進行身分驗證 （ 登入 AWS)。

您可以使用透過身分來源提供的憑證，以聯合身分 AWS 身分身分身分登入 。 AWS IAM Identity Center (IAM Identity Center) 使用者、您公司的單一登入身分驗證，以及您的 Google 或 Facebook 登入資料，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。當您使用聯合 AWS 身分存取 時，您會間接擔任角色。

視您身分的使用者類型而定，您可以登入 AWS Management Console 或 AWS 存取入口網站。如需登入的詳細資訊 AWS，請參閱AWS 登入 《 使用者指南》中的如何登入您的 AWS 帳戶 。

如果您以 AWS 程式設計方式存取 ， AWS 會提供軟體開發套件 (SDK) 和命令列界面 (CLI)，以使用您的登入資料以密碼編譯方式簽署您的請求。如果您不使用 AWS 工具，則必須自行簽署請求。如需使用建議的方法自行簽署請求的詳細資訊，請參閱《IAM 使用者指南》中的適用於 API 請求的AWS Signature 第 4 版。

無論您使用何種身分驗證方法，您可能都需要提供額外的安全性資訊。例如， AWS 建議您使用多重要素驗證 (MFA) 來提高帳戶的安全性。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 IAM 中的AWS 多重要素驗證。

## AWS 帳戶 根使用者

當您建立 時 AWS 帳戶，您會從一個登入身分開始，該身分可完整存取 帳戶中的所有 AWS 服務 和資源。此身分稱為 AWS 帳戶 Theroot 使用者，可透過使用您用來建立帳戶的電子郵件地址和密碼登入來存取。強烈建議您不要以根使用者處理日常任務。保護您的根使用者憑證，並將其用來執行只能由根使用者執行的任務。如需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 中具有單一個人或應用程式特定許可 AWS 帳戶 的身分。建議您盡可能依賴臨時憑證，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。您無法以群組身分簽署。您可以使用群組來一次為多名使用者指定許可。群組可讓管理大量使用者許可的程序變得更為容易。例如，您可以擁有一個名為 IAMAdmins 的群組，並給予該群組管理 IAM 資源的許可。

使用者與角色不同。使用者只會與單一人員或應用程式建立關聯，但角色的目的是在由任何需要它的人員取得。使用者擁有永久的長期憑證，但角色僅提供臨時憑證。如需更多資訊，請參閱《IAM 使用者指南》中的 IAM 使用者的使用案例。

## 角色

IAM 角色是 中具有特定許可 AWS 帳戶 的身分。它類似 IAM 使用者，但不與特定的人員相關聯。若要暫時在 中擔任 IAM 角色 AWS Management Console，您可以從使用者切換至 IAM 角色（主控台）。您可以透過呼叫 AWS CLI 或 AWS API 操作或使用自訂 URL 來擔任角色。如需使用角色的方法詳細資訊，請參閱《IAM 使用者指南》中的擔任角色的方法。

使用臨時憑證的 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，並獲授予由角色定義的許可。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 (聯合) 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 (信任的主體) 存取您帳戶的資源。角色是授予跨帳戶存取權的主要方式。不過，對於某些 AWS 服務，您可以直接將政策連接到資源（而不是使用角色做為代理）。如需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 中的跨帳戶資源存取。
- 跨服務存取 – 有些 AWS 服務 使用其他 中的功能 AWS 服務。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。
  - 轉送存取工作階段 (FAS) – 當您使用 IAM 使用者或角色在 中執行動作時 AWS，您會被視為委託人。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 使用呼叫 的委託人許可 AWS 服務，並結合 AWS 服務 請求向下游服務提出請求。只有當服務收到需要與其他 AWS 服務 或 資源互動才能完成的請求時，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》。
  - 服務角色 – 服務角色是服務擔任的 IAM 角色，可代表您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需詳細資訊，請參閱《IAM 使用者指南》中的建立角色以委派許可權給 AWS 服務。
  - 服務連結角色 – 服務連結角色是連結至 的服務角色類型 AWS 服務。服務可以擔任代表您執行動作的角色。服務連結角色會出現在您的 中 AWS 帳戶 ，並由服務擁有。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 – 您可以使用 IAM 角色來管理在 EC2 執行個體上執行之應用程式的臨時登入資料，以及提出 AWS CLI 或 AWS API 請求。這是在 EC2 執行個體內儲存存取金鑰的較好方式。若要將 AWS 角色指派給 EC2 執行個體，並將其提供給其所有應用程式，您可以建立連接至執行個體的執行個體描述檔。執行個體設定檔包含該角色，並且可讓 EC2 執行個體上執行的程式取得臨時憑證。如需詳細資訊，請參閱《IAM 使用者指南》中的使用 IAM 角色來授予許可權給 Amazon EC2 執行個體上執行的應用程式。

## 使用政策管理存取權

您可以透過建立政策並將其連接至身分或資源 AWS 來控制 AWS 中的存取。政策是 中的物件，當與身分或資源建立關聯時， AWS 會定義其許可。當委託人（使用者、根使用者或角色工作階段）發出請求時， 會 AWS 評估這些政策。政策中的許可決定是否允許或拒絕請求。大多數政策會以 JSON 文件 AWS 的形式存放在 中。如需 JSON 政策文件結構和內容的詳細資訊，請參閱 IAM 使用者指南中的 JSON 政策概觀。

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。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。若要授予使用者對其所需資源執行動作的許可，IAM 管理員可以建立 IAM 政策。然後，管理員可以將 IAM 政策新增至角色，使用者便能擔任這些角色。

IAM 政策定義該動作的許可，無論您使用何種方法來執行操作。例如，假設您有一個允許 `iam:GetRole` 動作的政策。具有該政策的使用者可以從 AWS Management Console AWS CLI、 或 API AWS 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。如需了解如何建立身分型政策，請參閱《IAM 使用者指南》中的透過客戶管理政策定義自訂 IAM 許可。

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。受管政策是獨立的政策，您可以連接到 中的多個使用者、群組和角色 AWS 帳戶。受管政策包括 AWS 受管政策和客戶受管政策。如需了解如何在受管政策及內嵌政策之間選擇，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

的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中指定主體。委託人可以包含帳戶、使用者、角色、聯合身分使用者或 AWS 服務。

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

## 存取控制清單 (ACL)

存取控制清單 (ACL) 可控制哪些主體 (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 S3 AWS WAF和 Amazon VPC 是支援 ACLs的服務範例。如需進一步了解 ACL，請參閱 Amazon Simple Storage Service 開發人員指南中的存取控制清單 (ACL) 概觀。

## 其他政策類型

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

- 許可界限 – 許可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。如需許可界限的詳細資訊，請參閱 IAM 使用者指南中的 IAM 實體許可界限。
- 服務控制政策 SCPs) – SCPs是 JSON 政策，可指定 中組織或組織單位 (OU) 的最大許可 AWS Organizations。 AWS Organizations 是一種用於分組和集中管理您企業擁有 AWS 帳戶 的多個的服務。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，包括每個實體 AWS 帳戶根使用者。如需 Organizations 和 SCP 的詳細資訊，請參閱《AWS Organizations 使用者指南》中的服務控制政策。
- 資源控制政策 (RCP) - RCP 是 JSON 政策，可用來設定您帳戶中資源的可用許可上限，採取這種方式就不需要更新附加至您所擁有的每個資源的 IAM 政策。RCP 會限制成員帳戶中資源的許可，並可能影響身分的有效許可，包括 AWS 帳戶根使用者，無論它們是否屬於您的組織。如需 Organizations 和 RCPs的詳細資訊，包括 AWS 服務 支援 RCPs的 清單，請參閱AWS Organizations 《 使用者指南》中的資源控制政策 RCPs)。
- 工作階段政策 – 工作階段政策是一種進階政策，您可以在透過撰寫程式的方式建立角色或聯合使用者的暫時工作階段時，做為參數傳遞。所產生工作階段的許可會是使用者或角色的身分型政策和工作階段政策的交集。許可也可以來自資源型政策。所有這類政策中的明確拒絕都會覆寫該允許。如需詳細資訊，請參閱 IAM 使用者指南中的工作階段政策。

### 多種政策類型

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

## 標籤編輯器如何與 IAM 搭配使用

使用 IAM 管理標籤編輯器的存取權之前，您應該了解哪些 IAM 功能可與標籤編輯器搭配使用。若要取得標籤編輯器和其他 如何使用 IAM AWS 服務 的高階檢視，請參閱《AWS 服務 IAM 使用者指南》中的 與 IAM 搭配使用。

主題

- 標籤編輯器身分型政策
- 資源型政策
- 以標籤為基礎的授權
- 標籤編輯器 IAM 角色

### 標籤編輯器身分型政策

使用 IAM 身分型政策，除了允許或拒絕動作的條件之外，您還可以指定允許或拒絕的動作和資源。標籤編輯器支援特定動作、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。政策動作通常具有與相關聯 AWS API 操作相同的名稱。有一些例外狀況，例如沒有相符的 API 操作的僅限許可動作。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動作的許可。

標籤編輯器中的政策動作在動作之前使用下列字首：`tag:`。標籤編輯器動作完全在主控台中執行，但在日誌項目`tag`中具有字首。

例如，若要授予某人使用 `tag:TagResources` API 操作標記資源的許可，請在其政策中包含 `tag:TagResources`動作。政策陳述式必須包含 `Action` 或 `NotAction` 元素。標籤編輯器會定義自己的動作集，描述您可以使用此服務執行的任務。

若要在單一陳述式中指定多個標記動作，請以逗號分隔它們，如下所示。

```
"Action": [
      "tag:action1",
      "tag:action2",
      "tag:action3"
```

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

```
"Action": "tag:Get*"
```

若要查看標籤編輯器動作的清單，請參閱服務授權參考中的標籤編輯器的動作、資源和條件索引鍵。

資源

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。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 (例如列出操作)，請使用萬用字元 (*) 來表示陳述式適用於所有資源。

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

標籤編輯器沒有任何自己的資源。反之，它會操作連接到其他 所建立資源的中繼資料 （ 標籤 ） AWS 服務。

條件索引鍵

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

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

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

您也可以在指定條件時使用預留位置變數。例如，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。如需更多資訊，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條件索引鍵。若要查看所有 AWS 全域條件索引鍵，請參閱《IAM 使用者指南》中的AWS 全域條件內容索引鍵。

標籤編輯器不會定義任何服務特定的條件索引鍵。

範例

若要檢視標籤編輯器身分型政策的範例，請參閱 標籤編輯器身分型政策範例。

## 資源型政策

標籤編輯器不支援以資源為基礎的政策，因為它未定義任何自己的資源。

## 以標籤為基礎的授權

以標籤為基礎的授權是稱為屬性型存取控制 (ABAC) 的安全策略的一部分。

若要根據資源的標籤控制對資源的存取，您可以使用 `aws:RequestTag/`*`key-name`*、`aws:ResourceTag/`*`key-name`*或 條件索引鍵，在政策的條件元素中提供標籤資訊。`aws:TagKeys`建立或更新資源時，您可以將標籤套用至資源。

若要檢視身分型政策範例，以根據該資源上的標籤來限制存取資源，請參閱根據標籤檢視群組。如需屬性型存取控制 (ABAC) 的詳細資訊，請參閱《IAM 使用者指南》中的 ABAC for AWS？。

## 標籤編輯器 IAM 角色

IAM 角色是 中具有特定許可 AWS 帳戶 的實體。標籤編輯器沒有或使用服務角色。

搭配標籤編輯器使用臨時憑證

在標籤編輯器中，您可以使用臨時登入資料來使用聯合身分登入、擔任 IAM 角色，或擔任跨帳戶角色。您可以透過呼叫 AssumeRole或 等 AWS STS API 操作來取得臨時安全登入資料GetFederationToken。

服務連結角色

服務連結角色 AWS 服務 允許 存取其他服務中的資源，以代表您完成 動作。

標籤編輯器沒有或使用服務連結角色。

服務角色

此功能可讓服務代表您擔任服務角色。

標籤編輯器沒有或使用服務角色。

## 標籤編輯器身分型政策範例

根據預設， IAM 主體，例如角色和使用者，沒有建立或修改標籤的許可。他們也無法使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 或 AWS APIs執行任務。IAM 管理員必須建立 IAM 政策，授予主體對所需特定資源執行特定 API 操作的許可。然後，管理員必須將這些政策連接到需要這些許可的主體。

如需使用這些範例 JSON 政策文件建立 IAM 身分型政策的說明，請參閱《IAM 使用者指南》中的在 JSON 標籤上建立政策。

主題

- 政策最佳實務
- 使用標籤編輯器主控台和資源群組標記 API
- 允許使用者檢視他們自己的許可
- 根據標籤檢視群組

### 政策最佳實務

以身分為基礎的政策會判斷是否有人可以在您的帳戶中建立、存取或刪除標籤編輯器資源。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 受管政策並邁向最低權限許可 – 若要開始將許可授予您的使用者和工作負載，請使用 AWS 受管政策來授予許多常見使用案例的許可。它們可在您的 中使用 AWS 帳戶。我們建議您定義特定於使用案例 AWS 的客戶受管政策，以進一步減少許可。如需更多資訊，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 套用許可的更多相關資訊，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。如果透過特定 使用服務動作，您也

可以使用條件來授予存取服務動作的權限 AWS 服務，例如 AWS CloudFormation。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，可協助您撰寫安全且實用的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的使用 IAM Access Analyzer 驗證政策。
- 需要多重要素驗證 (MFA)：如果您的案例需要 IAM 使用者或 中的根使用者 AWS 帳戶，請開啟 MFA 以增加安全性。如需在呼叫 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》https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_configure-api-require.html中的透過 MFA 的安全 API 存取。

如需 IAM 中最佳實務的相關資訊，請參閱 IAM 使用者指南中的 IAM 安全最佳實務。

## 使用標籤編輯器主控台和資源群組標記 API

若要存取標籤編輯器主控台和資源群組標記 API，您必須擁有一組最低許可。這些許可必須允許您列出和檢視連接到 中資源的標籤的詳細資訊 AWS 帳戶。如果您建立比最低必要許可更嚴格的身分型政策，主控台和 API 命令將無法如預期對具有該政策的 IAM 主體運作。

為了確保這些主體仍然可以使用標籤編輯器，請將下列政策（或包含下列政策所列許可的政策）連接至實體。如需詳細資訊，請參閱《IAM 使用者指南》中的新增許可到使用者。

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

如需授予標籤編輯器和資源群組標記 API 存取權的詳細資訊，請參閱 授予使用標籤編輯器的許可。

## 允許使用者檢視他們自己的許可

此範例會示範如何建立政策，允許 IAM 使用者檢視附加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完成此動作的許可，或使用 AWS CLI 或 AWS API 以程式設計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": "*"
        }
    ]
}
```

### 根據標籤檢視群組

您可以在身分型政策中使用條件，根據標籤控制對標籤編輯器資源的存取。此範例示範如何建立允許檢視資源的政策，在此範例中是資源群組。不過，只有在群組標籤project具有與連接至呼叫主體的project標籤相同的值時，才會授予許可。

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

您可以將此政策連接到您帳戶中的 使用者。如果具有標籤索引鍵project和標籤值的使用者alpha嘗試檢視資源群組，則群組也必須加上標籤project=alpha。否則使用者會被拒絕存取。條件標籤鍵 project 符合 Project 和 project，因為條件索引鍵名稱不區分大小寫。如需詳細資訊，請參閱 IAM 使用者指南中的 IAM JSON 政策元素：條件。

## 標籤編輯器身分和存取的故障診斷

使用下列資訊來協助您診斷和修正使用標籤編輯器和 IAM 時可能遇到的常見問題。

主題

- 我無權在標籤編輯器中執行動作
- 我未獲得執行 iam:PassRole 的授權

### 我無權在標籤編輯器中執行動作

如果 AWS Management Console 告訴您未獲授權執行 動作，則必須聯絡管理員尋求協助。您的管理員是為您提供簽署憑證的人員。

當使用者mateojackson嘗試使用主控台檢視資源上的標籤，但沒有tag:GetTagKeys許可時，會發生下列範例錯誤。

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

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

### 我未獲得執行 iam:PassRole 的授權

如果您收到錯誤，表示您無權執行iam:PassRole動作，則必須更新您的政策，以允許您將角色傳遞給標籤編輯器。

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

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

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

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

如果您需要協助，請聯絡您的 AWS 管理員。您的管理員提供您的簽署憑證。

## 在標籤編輯器中記錄和監控

所有標籤編輯器動作都會登入 AWS CloudTrail。

### 使用 CloudTrail 記錄標籤編輯器 API 呼叫

標籤編輯器已與 整合 AWS CloudTrail，此服務提供使用者、角色或標籤編輯器 AWS 服務 中 所採取動作的記錄。CloudTrail 會將標籤編輯器的所有 API 呼叫擷取為事件，包括從標籤編輯器主控台和從

程式碼呼叫到資源群組標記 API 的呼叫。如果您建立追蹤，您可以啟用 CloudTrail 事件持續交付至 Amazon S3 儲存貯體，包括標籤編輯器的事件。即使您未設定追蹤，依然可以透過 CloudTrail 主控台中的事件歷史記錄檢視最新事件。使用 CloudTrail 收集的資訊，您可以判斷對標籤編輯器提出的請求、提出請求的 IP 地址、提出請求的人員、提出請求的時間，以及其他詳細資訊。

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

## CloudTrail 中的標籤編輯器資訊

建立帳戶 AWS 帳戶 時，您的 上會啟用 CloudTrail。當活動在標籤編輯器或標籤編輯器主控台中發生時，該活動會與事件歷史記錄中的其他 AWS 服務 事件一起記錄在 CloudTrail 事件中。您可以在 中檢視、搜尋和下載最近的事件 AWS 帳戶。如需詳細資訊，請參閱「使用 CloudTrail 事件歷史記錄檢視事件」。

若要持續記錄 中的事件 AWS 帳戶，包括標籤編輯器的事件，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。追蹤會記錄 AWS 分割區中所有 區域的事件，並將日誌檔案交付至您指定的 Amazon S3 儲存貯體。此外，您可以設定其他 AWS 服務 來進一步分析 CloudTrail 日誌中收集的事件資料，並對其採取行動。如需詳細資訊，請參閱下列資源：

- 為您的 建立追蹤 AWS 帳戶
- CloudTrail 支援的服務和整合
- 設定 CloudTrail 的 Amazon SNS 通知
- 接收多個區域的 CloudTrail 日誌檔案及接收多個帳戶的 CloudTrail 日誌檔案

CloudTrail 會記錄所有標籤編輯器動作，並記錄在標籤編輯器 API 參考中。主控台中的標籤編輯器動作會由 CloudTrail 記錄，並以 `tagging.amazonaws.com`顯示為事件`eventSource`。

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

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

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

## 了解標籤編輯器日誌檔案項目

追蹤是一種組態，能讓事件以日誌檔案的形式交付到您指定的 Amazon S3 儲存貯體。CloudTrail 日誌檔案包含一或多個日誌專案。一個事件為任何來源提出的單一請求，並包含請求動作、請求的日期和時間、請求參數等資訊。CloudTrail 日誌檔案並非依公有 API 呼叫追蹤記錄的堆疊排序，因此不會以任何特定順序出現。

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


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAEXAMPLEEXAMPLE:botocore-session-1661372702",
        "arn": "arn:aws:sts::123456789012:assumed-role/cli-role/botocore-
session-1661372702",
        "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": "2022-08-24T20:25:03Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-08-24T20:27:14Z",
    "eventSource": "tagging.amazonaws.com",
    "eventName": "TagResources",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "72.21.198.65",
    "userAgent": "aws-cli/2.7.14 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/
resourcegroupstaggingapi.tag-resources",
    "requestParameters": {
        "resourceARNList": [
            "arn:aws:events:us-east-1:123456789012:rule/SecretsManagerMonitorRule"
```

```
        ],
        "tags": {
            "owner": "alice"
        }
    },
    "responseElements": {
        "failedResourcesMap": {}
    },
    "requestID": "8f9ea891-4125-460c-802f-26c11EXAMPLE",
    "eventID": "b2c9322a-aad7-424b-8f0b-423daEXAMPLE",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "tagging.us-east-1.amazonaws.com"
    }
}
```


## 標籤編輯器的合規驗證

若要了解 是否 AWS 服務 在特定合規計劃的範圍內，請參閱AWS 服務 合規計劃範圍內然後選擇您感興趣的合規計劃。如需一般資訊，請參閱 AWS Compliance Programs。

您可以使用 下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱在 中下載報告 AWS Artifact。

使用 時的合規責任 AWS 服務 取決於資料的敏感度、您公司的合規目標，以及適用的法律和法規。AWS 提供下列資源以協助合規：

- 安全合規與治理 - 這些解決方案實作指南內容討論了架構考量，並提供部署安全與合規功能的步驟。
- HIPAA 合格服務參考 – 列出 HIPAA 合格服務。並非所有 AWS 服務 都符合 HIPAA 資格。
- AWS 合規資源 – 此工作手冊和指南的集合可能適用於您的產業和位置。
- AWS 客戶合規指南 – 透過合規的角度了解共同的責任模型。本指南摘要說明保護 的最佳實務，AWS 服務 並將指南映射到跨多個架構的安全控制 （ 包括國家標準和技術研究所 (NIST)、支付卡產業安全標準委員會 (PCI) 和國際標準化組織 (ISO))。
- AWS Config 開發人員指南中的使用規則評估資源 – AWS Config 服務會評估資源組態符合內部實務、產業準則和法規的程度。

- AWS Security Hub – 這 AWS 服務 可讓您全面檢視其中的安全狀態 AWS。Security Hub 使用安全控制，可評估您的 AWS 資源並檢查您的法規遵循是否符合安全業界標準和最佳實務。如需支援的服務和控制清單，請參閱「Security Hub 控制參考」。
- Amazon GuardDuty – 這可透過監控您的環境是否有可疑和惡意活動，來 AWS 服務 偵測對您 AWS 帳戶、工作負載、容器和資料的潛在威脅。GuardDuty 可滿足特定合規架構所規定的入侵偵測需求，以協助您因應 PCI DSS 等各種不同的合規需求。
- AWS Audit Manager – 這 AWS 服務 可協助您持續稽核 AWS 用量，以簡化您管理風險的方式，以及符合法規和產業標準的方式。

## 標籤編輯器中的彈性

標籤編輯器會對內部服務資源執行自動備份。這些備份無法由使用者設定。備份會加密，包括靜態和傳輸中。標籤編輯器將客戶資料存放在 Amazon DynamoDB 中。

AWS 全球基礎設施是以 AWS 區域 和 可用區域為基礎建置。 AWS 區域 提供多個實體隔離和隔離的可用區域，這些區域與低延遲、高輸送量和高度備援聯網連接。透過可用區域，您所設計與操作的應用程式和資料庫，就能夠在可用區域之間自動容錯移轉，而不會發生中斷。可用區域的可用性、容錯能力和擴充能力，均較單一或多個資料中心的傳統基礎設施還高。

如果您意外刪除標籤，請聯絡 AWS 支援 中心。

如需 AWS 區域 和 可用區域的詳細資訊，請參閱AWS 全球基礎設施。

## 標籤編輯器中的基礎設施安全性

標籤編輯器不提供隔離服務或網路流量的其他方式。如適用，請使用 AWS 特定隔離。您可以在虛擬私有雲端 (VPC) 中使用標籤編輯器 API 和主控台，以協助最大化隱私權和基礎設施安全。

您可以使用 AWS 已發佈的 API 呼叫，透過網路存取標籤編輯器。使用者端必須支援下列專案：

- Transport Layer Security (TLS)。我們需要 TSL 1.2 並建議 TSL 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，必須使用與 AWS Identity and Access Management (IAM) 主體相關聯的存取金鑰 ID 和秘密存取金鑰來簽署請求。或者，您可以使用 AWS Security Token Service (AWS STS) 產生暫時性安全登入資料來簽署請求。

**標籤編輯器不支援以資源為基礎的政策。**

您可以從任何網路位置呼叫 Tag Editor API 操作，但 Tag Editor 確實支援以資源為基礎的存取政策，其中可能包含根據來源 IP 地址的限制。您也可以使用標籤編輯器政策來控制來自特定 Amazon Virtual Private Cloud (Amazon VPC) 端點或特定 VPCs存取。實際上，此方法只會隔離網路中特定 VPC 對指定資源 AWS 的網路存取。

# Service Quotas

下表提供有關標籤編輯器服務配額的資訊。

這些配額目前無法使用 Service Quotas 主控台調整。請聯絡 支援。

| 名稱 | 預設 |
| --- | --- |
| 每個資源連接的標籤 | 50 個使用者定義的標籤 (AWS 產生的標籤不會計入此限制。) |
| 標籤金鑰名稱 | UTF-8 中最少 1 個，最多 128 個 Unicode 字元。<br><br>允許的字元包括字母、數字、空格和下列字元：<br><br>`_ . : / = + - @`<br><br>金鑰名稱不能以 開頭，`aws:`因為保留該字首以供 AWS 使用。<br><br>**Note**<br>有些 AWS 服務 有額外的字元或長度限制。如需詳細資訊，請參閱特定服務的文件。 |
| 標籤值 | UTF-8 中最少 0 個，最多 256 個 Unicode 字元。<br><br>允許的字元包括字母、數字、空格和下列字元：<br><br>`_ . : / = + - @` |

| 名稱 | 預設 | |
|---|---|---|
| | **Note**<br>有些 AWS 服務 有額外的字元或長度限制。如需詳細資訊，請參閱特定服務的文件。 | |
| 呼叫 GetResources API 操作的速率 | 每秒最多 15 個呼叫 | |
| 呼叫下列 API 操作的速率：<br>• TagResources<br>• UntagResources<br>• GetTagKeys<br>• GetTagValues | 每秒最多 5 個呼叫 | |

# 標籤編輯器文件歷史記錄

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| 標籤編輯器主控台中的 AWS Resource Groups 標籤管理已移至 AWS 資源總管 主控台 | AWS 已將標籤編輯器標籤管理功能從 AWS Resource Groups 主控台移至 AWS 資源總管 主控台。若要進一步了解如何在 Resource Explorer 中管理資源標籤，請參閱 Resource Explorer 使用者指南中的管理資源。 | 2025 年 4 月 10 日 |
| 更新了評估整個組織合規性的許可 | 更新評估整個組織合規的許可，以包含協助存取合規報告的許可。 | 2024 年 8 月 28 日 |
| 已更新內容 | 更新主題標題和重組內容，以提高可讀性和可探索性。 | 2024 年 7 月 25 日 |
| 從 標記內容已 AWS 一般參考 移至本指南 | 有關標記 AWS 資源的主題已從 AWS 一般參考 移至本指南。 | 2023 年 3 月 24 日 |
| IAM 最佳實務更新 | 更新了指南以符合 IAM 最佳實務。如需更多詳細資訊，請參閱 IAM 中的安全最佳實務。 | 2023 年 1 月 3 日 |
| 將標籤編輯器文件移至自己的指南 | 標籤編輯器文件現在提供在其自己的使用者指南中，而不是屬於 AWS Resource Groups 使用者指南的一部分。 | 2022 年 12 月 13 日 |
| 檢查標籤政策的合規性 | 使用 建立並連接標籤政策到帳戶之後 AWS Organizations，您可以在組織帳戶中的資源上找到不合規的標籤。 | 2019 年 11 月 26 日 |

| | | |
|---|---|---|
| 標籤編輯器現在支援尋找未標記的資源 | 您現在可以在標籤編輯器中搜尋未針對特定標籤索引鍵套用標籤值的資源。 | 2019 年 6 月 18 日 |
| 標籤編輯器主控台移出 AWS Systems Manager 主控台 | 標籤編輯器主控台現在獨立於 Systems Manager 主控台。雖然您仍然可以在 Systems Manager 左側導覽列中找到標籤編輯器主控台的指標，但您可以直接從 左上方的下拉式功能表開啟標籤編輯器主控台 AWS Management Console。 | 2019 年 6 月 5 日 |
| 舊版標籤編輯器工具已無法使用 | 已移除對舊版、傳統或舊版標籤編輯器的提及；這些工具已不再提供 AWS。請改用標籤編輯器。 | 2019 年 5 月 14 日 |
| 標籤編輯器現在支援跨多個區域的標記資源 | 標籤編輯器現在可讓您跨多個區域搜尋和管理資源標籤，並且預設會將您目前的區域新增至資源查詢。 | 2019 年 5 月 2 日 |
| 標籤編輯器現在支援將查詢結果匯出至 CSV | 您可以在 Find Resources to tag (尋找要加標籤的資源) 頁面上，將查詢的結果匯出為 CSV 格式的檔案。標籤編輯器查詢結果中會顯示新的區域欄。標籤編輯器現在可讓您搜尋特定標籤索引鍵具有空白值的資源。標籤索引鍵值會在您輸入現有索引鍵中的唯一值時自動完成。 | 2019 年 4 月 2 日 |

| | | |
|---|---|---|
| 標籤編輯器現在支援將所有資源類型新增至查詢 | 您最多可以在單一操作中對個別資源類型套用 20 個標籤，或者您可以選擇 All resource types (所有資源類型) 以查詢區域中的所有資源類型。自動完成已新增至查詢的 Tag key (標籤索引鍵) 欄位，以協助在資源間實現一致的標籤索引鍵。如果標籤變更在某些資源上失敗，您可以僅在標籤變更失敗的資源上變更重試標籤變更。 | 2019 年 3 月 19 日 |
| 標籤編輯器現在支援搜尋中的多種資源類型 | 您可以在單一操作中對最多 20 個資源類型套用標籤。您也可以選擇在搜尋結果中顯示的欄位，包含在您的搜尋結果中找到的每個唯一標籤索引鍵或從結果選取資源的欄位。 | 2019 年 2 月 26 日 |