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

什麼是標籤編輯器？

標籤編輯器可讓您有效管理標籤。標籤是作為中繼資料的索引鍵和值對，用於組織您的 AWS 資源。對於大多數 AWS 資源，您可以在建立資源時選擇新增標籤。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 中的秘密 AWS Secrets Manager。

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

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**
>
> 雖然標籤索引鍵區分大小寫， 對IAM資源IAM有其他驗證，以防止套用只有大小寫差異的標籤索引鍵。建議您不要使用僅與外殼不同的金鑰。反之，您可以使用 Service Control 政策 （ SCPs ），該政策可讓您集中控制組織中IAM使用者和IAM角色的可用許可上限。

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 – 部分服務支援使用標籤編輯器主控台進行標籤。
- 資源群組標記 API – 大多數 服務也支援使用 進行標記AWS Resource Groups Tagging API。

> **Note**
>
> 您也可以使用 AWS Service Catalog TagOptions Library 輕鬆管理已佈建產品的標籤。TagOption 是 Service Catalog 中管理的鍵值對。它不是 AWS 標籤，而是作為根據 建立 AWS 標籤的範本 TagOption。

您可以在 AWS中標記所有成本累計服務的資源。對於下列 服務， AWS 建議 AWS 服務 支援標記的較新替代方案，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 AWS 資源互動的資訊，請參閱 IAM 使用者指南 中的使用標籤來控制IAM對 和 的存取。

最佳做法和策略

這些部分提供有關標記 AWS 資源和使用標籤編輯器時的最佳實踐和策略的資訊。

標記最佳做法

為 AWS 資源建立標記策略時，請遵循最佳做法：

- 不要在標籤中添加個人身份信息（PII）或其他機密或敏感信息。許多 AWS 服務都可以使用標籤，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 Resource Groups 標記可API讓您以程式設計方式控制標籤，讓自動管理、搜尋和篩選標籤和資源變得更加容易。
- 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。

標籤命名最佳做法

這些是我們建議您搭配標籤使用的一些最佳作法和命名慣例。

AWS 標籤的關鍵名稱區分大小寫，因此請確保使用一致。例如，標籤鍵`CostCenter`和`costcenter`是不同的。一個標籤索引鍵可能會設定為財務分析和報表的成本配置標記，而另一個標籤鍵可能不會設定為相同的用途。

許多標籤由各種預先定義 AWS 或自動創建 AWS 服務。許多AWS 產生的標籤會使用全部小寫的金鑰名稱，以連字號分隔名稱中的文字，以及前綴後跟冒號，以識別標籤的來源服務。例如，請參閱下列內容：

- `aws:ec2spot:fleet-request-id`是用來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`是標識創建資源的 AWS CloudFormation 堆棧的標籤。
- `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命名標籤：

- 單詞使用全部小寫。
- 使用連字號來分隔單字。

- 使用前綴後跟冒號來識別組織名稱或縮寫名稱。

例如，對於名稱為虛擬的公司 AnyCompany，您可以定義標籤，例如：

- anycompany:cost-center以識別內部成本中心代碼。
- anycompany:environment-type識別環境是否為開發、測試或生產環境。
- anycompany:application-id以識別為其建立資源的應用程式。

前置詞可確保標籤可以清楚地識別由您的組織定義，而不是由您可能正在使用的第三方工具 AWS 或第三方工具所定義。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。
- 標籤鍵必須至少為 1，且 UTF -8 中最多 128 個 Unicode 字元。
- 標籤值必須至少為 0，且 UTF -8 中最多 256 個 Unicode 字元。
- 允許的字元可能因服 AWS 務而異。如需有關可用來標記特定 AWS 服務中資源的字元的詳細資訊，請參閱其說明文件。通常，允許的字符是字母，數字，UTF-8 中可表示的空格，以及以下字符：_.：/= +-@。
- 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。使用此 AWS Resource Groups 服務，您可以根據一或多個標籤或部分標籤來建立 AWS 資源群組。您也可以根據群組在 AWS CloudFormation 堆疊中的複本來建立群組。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 和詳細的帳單報告可讓您按標籤劃分 AWS 成本。一般而言，您會使用成本中心/業務單位、客戶或專案等商業標籤，將成本與傳統的 AWS 成本配置維度產生關聯。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，您可以將 AWS產生的`createdBy`標籤用於成本分配目的，以協助考量可能未分類的資源。`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 Billing and Cost Management 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。在這個案例中，Amazon 彈性運算雲端 (AmazonEC2) 執行個體標籤是識別執行個體以選擇退出此動作的簡單方法。對於尋找和刪除過時或滾動 Amazon EBS 快照的指令碼，快照標籤可以新增額外的搜尋條件維度。 out-of-date

存取控制的標籤

IAM策略支援以標籤為基礎的條件，可讓您根據特定標籤或標籤值來IAM限制權限。例如，IAM使用者或角色權限可以包括根據其標記限制對特定環境 (例如開發、測試或生產環境) 的EC2API呼叫的條

件。您可以使用相同的策略來限制對特定 Amazon Virtual Private Cloud (AmazonVPC) 網路的API呼叫。Support 以標籤為基礎的資源層級IAM權限是服務特定的。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。如需有關使用標籤來控制 AWS 資源API存取權的詳細資訊，請參閱《使用指南》IAM中的適IAM用AWS 服務。

標記管理

有效的標記策略使用標準化標籤，並以程式設計方式在 AWS 資源之間一致地套用 您可以在 AWS 環境中使用被動和主動方法來管理標籤。

- 反應式控管用於使用 Resource Groups 標API記和自訂指令碼等工具來尋找未正確標記的資源。AWS Config 規則若要手動尋找資源，您可以使用標籤編輯器和詳細的帳單報告。
- 主動式控管使用 Service Catalog AWS CloudFormation、中的標籤原則或資IAM源層級權限等工具 AWS Organizations，確保在資源建立時一致地套用標準化標籤。

  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 Resource Groups 標記API來搜尋 AWS 環境的標籤，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 • 應用程式 ID – 識別與特定應用程式相關的資源 • 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 • 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 • 擁有者 – 識別資源的負責人 • 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 • 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 • 環境 – 區分開發、測試和生產資源 • 版本 – 協助區分資源或應用程式的版本	• 安全性 — 判斷需求，例如加密或啟用 Amazon VPC 流程日誌；識別需要額外審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	

開始使用標籤編輯器

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

若要一次將標籤新增至或編輯或刪除多個資源的標籤，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 [Resource Groups 與標籤編輯器]。在左側的導覽窗格中，選擇「標籤編輯器」。
   - 使用直接鏈接：AWS 標籤編輯器主控台。

並不是所有資源都可以套用標籤。有關標籤編輯器支援哪些資源的資訊，請參閱「支援的資源類型」中的「標籤編輯器」標記欄。AWS Resource Groups 使用者指南。如果不支持您要標記的資源類型，讓 AWS 通過在控制台窗口的左下角選擇反饋知道。

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

在開始標記資源之前，請確保您有一個活躍的 AWS 帳戶 具有現有資源和適當的權限來標記資源和創建組。

主題

- 註冊一個 AWS 帳戶
- 建立具有管理存取權的使用者
- 建立 資源

註冊一個 AWS 帳戶

如果您沒有 AWS 帳戶，請完成下列步驟來建立一個步驟。

若要註冊成為 AWS 帳戶

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

   部分註冊程序需接收來電，並在電話鍵盤輸入驗證碼。

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

AWS 註冊過程完成後，會向您發送確認電子郵件。您可以隨時前往 https://aws.amazon.com/並選擇「我的帳戶」，檢視目前的帳戶活動並管理您的帳戶。

建立具有管理存取權的使用者

在您註冊一個 AWS 帳戶，保護您的 AWS 帳戶根使用者，啟用 AWS IAM Identity Center，並建立系統管理使用者，這樣您就不會將 root 使用者用於日常工作。

保護您的 AWS 帳戶根使用者

1. 登入 AWS Management Console通過選擇 Root 用戶並輸入您的帳戶所有者 AWS 帳戶 電子郵件地址。在下一頁中，輸入您的密碼。

   如需使用 root 使用者登入的說明，請參閱以 root 使用者身分登入 AWS 登入 使用者指南。
2. 為您的 root 使用者開啟多因素驗證 (MFA)。

   如需指示，請參閱為您的MFA裝置啟用虛擬裝置 AWS 帳戶 使用者指南中的 root IAM 使用者 (主控台)。

建立具有管理存取權的使用者

1. 啟用IAM身分識別中心。

   如需指示，請參閱啟用 AWS IAM Identity Center 中的 AWS IAM Identity Center 使用者指南。
2. 在IAM身分識別中心中，將管理存取權授與使用者。

   若要取得有關使用 IAM Identity Center 目錄 做為您的身分識別來源，請參閱以預設值設定使用者存取 IAM Identity Center 目錄 中的 AWS IAM Identity Center 使用者指南。

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 使用者登入URL，請使用建立IAM身分識別中心使用者時傳送至您電子郵件地址的登入資訊。

  如需使用IAM身分識別中心使用者登入的說明，請參閱登入 AWS 存取入口網站 AWS 登入 使用者指南。

指派存取權給其他使用者

1. 在 IAM Identity Center 中，建立遵循套用最低權限權限的最佳作法的權限集。

   如需指示，請參閱 AWS IAM Identity Center 使用者指南。
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。

   如需相關指示，請參閱 AWS IAM Identity Center 使用者指南。

建立 資源

你必須有資源 AWS 帳戶 標記。如需有關支援資源類型的詳細資訊，請參閱「支援的資源類型」下的「標籤編輯器標記」欄。AWS Resource Groups 使用者指南。

設定許可

要充分利用標籤編輯器，您可能需要額外的權限來標記資源或查看資源的標籤鍵和值。這些權限分為下列類別：

- 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」主控台所需的權限。

如果您是系統管理員，您可以透過 AWS Identity and Access Management (IAM) 服務。您必須先建立IAM角色、使用者或群組，然後以所需的權限套用原則。如需有關建立和附加IAM原則的資訊，請參閱使用原則。

個別服務的權限

> **Important**
>
> 本節說明如果您想要標記其他資源時所需的權限 AWS 服務控制台和 APIs.

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

使用「標籤編輯器」主控台所需的權限

若要使用標籤編輯器主控台列出和標記資源，必須將下列權限新增至中的使用者政策陳述式IAM。您可以添加 AWS 由下列項目維護及保持最新的受管理策略 AWS，或者您可以建立和維護自己的自訂原則。

使用 AWS 標籤編輯器權限的受管策略

標籤編輯器支援下列項目 AWS 受管理的策略，您可以用來提供一組預先定義的權限給您的使用者。您可以將這些受管理的政策附加到任何角色、使用者或群組，就像您建立的任何其他原則一樣。

ResourceGroupsandTagEditorReadOnlyAccess

此原則會授與連結的IAM角色或使用者權限，以呼叫兩者的唯讀作業 AWS Resource Groups 和標籤編輯器。若要讀取資源的標籤，您還必須透過個別原則擁有該資源的權限。在以下重要注意事項中了解更多信息。

ResourceGroupsandTagEditorFullAccess

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

Important

先前的兩個原則授與呼叫「標籤編輯器」作業和使用「標籤編輯器」主控台的權限。但是，您不僅必須具有調用操作的權限，還必須具有對您嘗試訪問其標籤的特定資源的適當權限。若要授與該標籤存取權，您還必須附加下列其中一個原則：

- 所以此 AWS 受管理政策 ReadOnlyAccess授予每個服務資源的唯讀操作的權限。 AWS 自動使此政策保持最新狀態 AWS 服務 因為他們變得可用。
- 許多服務提供服務特定唯讀 AWS 受管理的政策，您可以用來限制只存取該服務所提供的資源。例如，Amazon EC2 提供 AmazonEC2ReadOnlyAccess.
- 您可以建立自己的原則，針對您希望使用者存取的少數服務和資源，僅授與特定唯讀作業的存取權。此原則會使用允許清單策略或拒絕清單策略。

  允許清單策略利用預設拒絕存取的事實，直到您在原則中明確允許存取為止。因此，您可以使用類似下列範例的原則。

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

或者，您可以使用拒絕列表策略，允許訪問除了明確阻止的資源以外的所有資源。這需要一個單獨的策略，該策略適用於允許訪問的相關用戶。接著，下列範例政策會拒絕存取 Amazon 資源名稱 (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權限

- `tag:*`(此權限允許所有「標籤編輯器」動作。 如果您想要限制使用者可使用的動作，您可以使用特定動作或以逗號分隔的動作清單來取代星號。)
- `tag:GetResources`
- `tag:TagResources`
- `tag:UntagResources`
- `tag:getTagKeys`
- `tag:getTagValues`
- `resource-explorer:*`
- `resource-groups:SearchResources`
- `resource-groups:ListResourceTypes`

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

授與使用標籤編輯器的權限

若要新增原則以使用 AWS Resource Groups 和標籤編輯器的角色，請執行以下操作。

1. 開啟主IAM控台至 [角色] 頁面。
2. 尋找您要授與「標籤編輯器」權限的角色。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索引標籤上，貼上下列原則陳述式。

```
{
  "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**
>
> 此範例原則陳述式會授與僅執行「標籤編輯器」動作的權限。

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

現在原則已儲存於中IAM，您可以將其附加至其他主參與者，例如角色、群組或使用者。如需如何將原則新增至主參與者的詳細資訊，請參閱IAM使用者指南中的新增和移除IAM身分識別權限。

基於標籤的授權和訪問控制

AWS 服務 支持以下內容：

- 以動作為基礎的策略 — 例如，您可以建立允許使用者執行`GetTagKeys`或`GetTagValues`作業的策略，但不允許其他使用者執行。
- 策略中的資源層級權限 — 許多服務支援用ARNs來指定策略中的個別資源。

- 以標籤為基礎的授權 — 許多服務支援在策略條件下使用資源標籤。例如，您可以建立一個策略，允許使用者完全存取與使用者具有相同標記的群組。如需詳細資訊，請參閱用ABAC途 AWS? 在 AWS Identity and Access Management 使用者指南。
- 暫時認證 — 使用者可以扮演具有允許標籤編輯器作業之策略的角色。

標籤編輯器不使用任何服務連結角色。

有關標籤編輯器如何與之整合的詳細資訊 AWS Identity and Access Management (IAM)，請參閱「」中的下列主題。AWS Identity and Access Management 用戶指南：

- AWS 與之合作的服務 IAM
- 標籤編輯器的動作、資源和條件鍵
- 控制存取 AWS 資源:使用策略

尋找要標記的資源

使用標籤編輯器，您可以建立查詢，以尋找一或多 AWS 區域 個可用於標記的資源。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。若要取得更多資訊，請參閱《AWS Resource Groups 使用指南》中支援的資源類型中的「標籤編輯器標籤」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. (選擇性) 選擇要 AWS 區域 在其中搜尋要標記的資源。依預設，會使用您目前的地區。對於此程序，請選擇 us-east-1 和 us-west-2。
3. 從 [資源類型] 下拉式清單中選擇至少一種資源類型。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)。對於此程序，請選擇:AWS:EC2: 執行個體和:: S3:AWS: 儲存貯體。
4. (選擇性) 在「標籤」欄位中，輸入標籤金鑰或標籤索引鍵與值配對，將目前中的資源限制 AWS 區域 為僅使用指定值標記的資源。當您輸入標籤鍵時，目前「區域」中相符的標籤鍵會顯示在清單中。您可以從清單中選擇標籤鍵。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。標籤值是選擇性的，但會進一步縮小查詢結果的範圍。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，因此查詢只會傳回同時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，以尋找所選項目中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值為空的資源，請選擇 (空值)。

> **Note**
>
> 在您找到具有指定標籤的資源之前，必須先將這些資源套用至目前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)。結果會以表格的形式顯示在 [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. (選擇性) 若要設定「標籤編輯器」在資源搜尋結果中顯示的欄，請在資源搜尋結果中選擇「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。如果您想要查看表格中的所有文字，請選取「自動換行」核取方塊。

   開啟您要標籤編輯器在您的結果中顯示的欄。您可以針對搜尋結果中出現的每個標記或搜尋結果的選取子集顯示一欄。找到要標記的資源後，您可以隨時執行此操作。若要啟用欄位，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的現有標籤，這些標籤位於「尋找要標記查詢的資源」結果中。

如果您按照上一節所述啟用了任何「標籤」欄，則可以在搜尋結果中查看每個資源的該標籤目前的值。

> **Note**
>
> 本主題說明如何編輯個別資源的標籤。您也可以同時批量編輯多個選定資源的標籤。如需詳細資訊，請參閱 使用標籤編輯器管理標籤。

若要在搜尋結果表格中以內嵌方式編輯標籤

1. 選擇您要編輯的資源上的標籤值。

   > **Note**
   >
   > - 如果所選資源目前沒有包含所選索引鍵的標籤，則值會顯示為 (未標記)。
   > - 如果所選資源確實具有包含所選鍵的標籤，但沒有值，則值會顯示為「—」。

2. 您可以輸入新值，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]，從這個資源刪除標籤。

若要檢視個別資源的所有標籤

1. 在「尋找要標記查詢的資源」的結果中，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「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」來開啟此視窗。

   > **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。

將結果匯出至 .csv 檔案

您可以將尋找資源的結果匯出以標記查詢為逗號分隔值 (.csv) 檔案。.csv 檔案包含資源名稱、服務、地區、資源IDs、標籤總數，以及集合中每個唯一標籤鍵的欄。.csv 檔案可協助您為組織中的資源開發標記策略，或判斷跨資源標記時有重疊或不一致的位置。

1. 在「搜尋要標記查詢的資源」的結果中，選擇「將資源匯出至」CSV。

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。

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。標籤編輯器會顯示任何附加至資源的標籤。它也會顯示這些標籤是透過標籤編輯器、資源的服務主控台或使用API.

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

> **其他管理標籤的方式**
>
> 本主題討論使用中的標籤編輯器來標記資源 AWS Management Console。 但是，您也可以管理您的標籤 AWS 資源通過使用以下工具：
>
> - 您可以使用中的命令，在 shell 提示符下鍵入或腳本`resourcegroupstaggingapi`命令 AWS Command Line Interface (AWS CLI).
> - 您可以創建和運行 PowerShell 指令碼使用 AWS Resource Groups API在中標記 AWS Tools for PowerShell Core.
> - 您可以使用任何可用的程序創建和運行程序 AWS SDKs透過使用資源群組標記 APIs，例如 Python APIs 的標記或 Java APIs 的標記。

當您新增、移除或編輯現有的標籤時，您只會變更在要標記查詢的尋找資源結果中選取的那些資源的標籤。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，該查詢會傳回您要標記的多個資源。
2. 在「尋找要標記查詢的資源」的結果表格中，選取要新增標籤的資源旁邊的核取方塊。在表格頂端的篩選資源中輸入文字字串，以篩選部分資源名稱、ID、標籤鍵或標籤值。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。雖然您的原始查詢傳回了更多資源，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，您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。您無法新增包含與所選資源中已存在的標籤金鑰相符的金鑰的新標籤。

6. 完成新增標籤後，請選擇 [檢視] 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。不要離開頁面或在同一個瀏覽器標籤中打開其他頁面。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未成功，請參閱疑難排解標籤變更。解決標籤變更失敗後 (例如權限不足)，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關鍵字，但您可以刪除標籤並使用新名稱建立標籤來取代原始標籤關鍵字。這會刪除所選資源上具有該索引鍵的所有標籤。

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

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傳回了更多資源，但是您只會變更您在步驟 1 中選取的資源的標籤。
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**。

   如果您選取的資源對同一索引鍵具有不同的值，則選取的資源具有不同的標籤值會顯示在「標籤值」欄位中。在這種情況下，將游標放在方塊中會開啟一個下拉式清單，其中列出所選資源中此標籤鍵的所有可用值。

   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讓資源之間的標籤值保持一致。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，會新增具有該值**QA**的**Team**標籤。
5. 完成標籤變更後，請選擇 [檢視] 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。不要離開頁面或在同一個瀏覽器標籤中打開其他頁面。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未成功，請參閱疑難排解標籤變更。解決標籤變更失敗的根本原因後 (例如權限不足)，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”。

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關鍵字，因此如果需要編輯標籤關鍵字，您可以移除標籤並將其取代為新標籤。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。雖然原始查詢可能傳回了更多資源，但是您只會變更您在步驟 1 中選取的資源的標籤。
4. 選擇您要刪除的任何標籤旁的 Remove tag (移除標籤)。在此過程中，我們刪除**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。不要離開頁面或在同一個瀏覽器標籤中打開其他頁面。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。解決標籤變更失敗的根本原因後 (例如權限不足)，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”。

在IAM權限原則中使用標籤

AWS Identity and Access Management (IAM) 是您用來建立和管理權限原則的權限原則，以決定誰可以存取您的 AWS 資源。 AWS 服務 每次嘗試存取 AWS 服務或讀取或寫入 AWS 資源，都是由IAM原則控制的存取。

這些政策可讓您提供對資源的精細存取權。您可以用來微調此存取權限的其中一項功能是原則的Condition元素。此元素可讓您指定必須符合要求的條件，以判斷要求是否可以繼續。您可以使用Condition元素檢查以下內容：

- 附加至提出要求之使用者或角色的標籤。
- 附加到作為請求對象的資源的標籤。

基於標籤和屬性的訪問控制

標籤可能是您 AWS 存取控制策略的重要組成部分。有關在以屬性為基礎的存取控制 (ABAC) 策略中使用標籤作為屬性的資訊，請參閱《使用指南》中的〈使用標籤控制 AWS 資源的存取〉和〈使用標籤控制使用IAMIAM者和角色的存取〉。

有一個全面的教程，顯示如何使用IAM教程中的標籤授予對不同項目和組的訪問權限：根據用AWS Identity and Access Management 戶指南中的標籤定義訪問 AWS 資源的權限。

如果您使用SAML基於身份提供者（IdP）進行單次登錄，則可以將標籤附加到提供用戶訪問權限的假定角色。若要AWS Identity and Access Management 取得更多資訊，請參閱《使用指南》ABAC中的IAM自學課程：使用SAML階段作業標籤

與標籤相關的條件鍵

下表說明您可以在IAM權限原則中用來根據標記控制存取的條件索引鍵。這些條件鍵可讓您執行下列作業：

- 比較呼叫作業的主體上的標籤。
- 將提供給作業的標籤做為參數進行比較。
- 比較附加到操作將訪問的資源的標籤。

如需有關條件索引鍵及其使用方式的完整詳細資訊，請參閱條件索引鍵名稱欄中連結的頁面。

條件鍵名稱	描述
aws:PrincipalTag	將附加至發出要求之主體 (IAM角色或使用者) 的標籤與您在原則中指定的標籤進行比較。
aws:RequestTag	將作為參數傳送至要求的標籤索引鍵值配對，與您在原則中指定的標籤索引鍵值配對進行比較。
aws:ResourceTag	將附加至資源的索引鍵值配對與您在策略中指定的標籤索引鍵值配對進行比較。
aws:TagKeys	僅比較要求中的標籤索引鍵與您在原則中指定的金鑰。

使用標籤的IAM範例原則

Example 範例 1：強制使用者在建立資源時附加特定標籤

下列範例IAM權限原則顯示如何強制建立或修改IAM原則標籤的使用者在金鑰中加入標籤Owner。此外，此原則要求標籤的值設定為與目前附加至呼叫主體之Owner標籤相同的值。若要使用此策略，所有主參與者都必須附加Owner標籤，且必須防止使用者修改該標籤。如果在未包含Owner標籤的情況下嘗試建立或修改原則，則原則不相符且不允許該作業。

```
{
    "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 示例 2：使用標籤將資源的訪問限制為其「所有者」

只有在呼叫主EC2體的標籤值與執行個體相同的`project`標記值時，下列範例IAM權限政策才允許使用者停止執行中的 Amazon 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}"}
      }
    }
  ]
}
```

這個範例是以屬性為基礎的存取控制 () ABAC 的範例。如需使用IAM原則實作以標籤為基礎之存取控制策略的詳細資訊和其他範例，請參閱《使AWS Identity and Access Management 用指南》中的下列主題：

- 使用標籤控制 AWS 資源的存取
- 使用標籤控制使用IAM者和角色的存取權，以及
- IAM教學課程：根據標籤定義存取 AWS 資源的權限 — 顯示如何使用多個標記授與不同專案和群組的存取權。

AWS Organizations 標籤策略

標籤原則是您在其中建立的一種原則類型 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。若要使用標籤原則，建議您遵循中的標籤原則入門中所述的工作流程 AWS Organizations 使用者指南。如該頁面所述，建議的工作流程包括尋找和更正不符合標籤。若要完成這些工作，請使用「標籤編輯器」主控台。

先決條件和許可

您必須符合需求並設定必要權限，才能在「標籤編輯器」中評估標籤原則的符合性。

主題

- 評估標籤原則符合性的先決條件
- 評估帳戶合規性的權限
- 評估整個組織合規性的權限
- 報告儲存的 Amazon S3 儲存貯體政策

評估標籤原則符合性的先決條件

評估標籤原則的符合性需要下列事項：

- 您必須先啟用中的功能 AWS Organizations，以及建立和附加標籤原則。如需詳細資訊，請參閱中的下列頁面 AWS Organizations 用戶指南：
  - 管理標籤原則的先決條件和權限
  - 啟用標籤原則
  - 開始使用標籤原則
- 若要尋找帳戶資源上的不符合標籤，您需要該帳戶的登入認證以及中評估帳戶合規性的權限列出的權限。
- 若要評估整個組織的合規性，您需要組織管理帳戶的登入認證以及中列出的權限。評估整個組織合規性的權限 您只能要求符合性報告 AWS 區域 美國東部 (維吉尼亞北部)。

評估帳戶合規性的權限

在帳號的資源上尋找不符合標籤需要下列權限：

- organizations:DescribeEffectivePolicy— 取得帳號有效標籤政策的內容。
- tag:GetResources— 取得不符合附加標籤原則的資源清單。
- tag:TagResources— 新增或更新標籤。您也需要服務特定權限才能建立標籤。例如，若要在 Amazon 彈性運算雲端 (AmazonEC2) 中標記資源，您需要的許可ec2:CreateTags。
- tag:UnTagResources— 移除標籤。您也需要服務特定權限才能移除標記。例如，若要取消標記 Amazon 中的資源EC2，您需要的ec2:DeleteTags許可。

下面的例子 AWS Identity and Access Management (IAM) 策略提供評估帳號標籤符合性的權限。

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

如需有關IAM策略和權限的詳細資訊，請參閱《使IAM用者指南》。

評估整個組織合規性的權限

評估整個組織是否符合標籤原則需要下列權限：

- organizations:DescribeEffectivePolicy— 取得附加至組織、組織單位 (OU) 或帳戶之標籤原則的內容。
- tag:GetComplianceSummary— 取得組織中所有帳號中不合規資源的摘要。
- tag:StartReportCreation— 將最近相容性評估的結果匯出至檔案。每 48 小時評估一次全組織的合規性。
- 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`— 檢查接收合規報告之 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`— 將合規報告放置在指定的 Amazon S3 儲存貯體中。

下列範例IAM原則提供評估整個組織合規性的權限。替換每個 *placeholder* 使用您自己的信息：

- *bucket_name* -您的 Amazon S3 存儲桶名稱
- *organization_id* — 您組織的 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策略和權限的詳細資訊，請參閱《使IAM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，您用來呼叫的身分StartReportCreationAPI必須能夠存取美國東部 (維吉尼亞北部) 區域中的 Amazon 簡單儲存服務 (Amazon S3) 儲存貯體，才能存放報告。標籤原則會使用呼叫身分識別的認證，將符合性報告傳送至指定值區。

如果用於呼叫的儲存貯體和身分StartReportCreationAPI屬於同一個帳戶，則此使用案例不需要額外的 Amazon S3 儲存貯體政策。

如果與用來呼叫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附加至儲存貯體。StartReportCreation API替換每個 *placeholder* 使用您自己的信息：

- *bucket_name* -您的 Amazon S3 存儲桶名稱
- *organization_id* — 您組織的 ID
- *## _ ARN* — 用ARN於調用的IAM身份 StartReportCreation API

```
{
    "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策略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 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 使用指南》中的搜尋未標籤資源。

有效標籤策略會指定套用至帳號的標記規則。有效的標籤策略是帳戶繼承的任何標籤策略的彙總，以及直接附加到帳戶的任何標籤策略。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。當您將標籤原則附加至組織單位 (OU) 時，它會套用至屬於 OU 的所有帳戶。OUs

> **Note**
>
> 如果您尚未建立標籤策略，請參閱《AWS Organizations 使用指南》中的標籤策略入門。

若要尋找不相容的標籤，您必須具備下列權限：

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

評估帳號是否符合其有效標籤策略 (主控台)

1. 登入您要檢查其合規性的帳戶後，開啟「標籤策略」主控台。
2. [有效標籤原則] 區段會顯示上次更新原則的時間，以及已定義的標籤金鑰。您可以展開標籤鍵，以查看有關其值、案例處理以及是否針對特定資源類型強制執行這些值的資訊。

   > **Note**
   >
   > 如果您已登入管理帳戶，則必須選擇帳戶才能查看其有效政策並檢視合規性資訊。

3. 在「具有不相容標籤的資源」區段中，指定 AWS 區域 要搜尋不相容標籤的標籤。或者，您也可以依資源類型進行搜尋。然後選擇搜尋資源。

   即時結果會顯示在「搜尋結果」區段中。若要變更每頁傳回的結果數目或要顯示的欄數，請選擇設定圖示。
4. 在搜尋結果中，選取含有不相容標籤的資源。
5. 在列出資源標籤的對話方塊中，選擇超連結以開啟建立資源的 AWS 服務 位置。從該主控台修正不符合標籤。

   > **Tip**
   >
   > 如果您不確定哪些標籤不相容，請前往「標籤策略」主控台中該帳戶的「有效標籤政策」區段。您可以展開標籤關鍵字以檢視其標籤規則。

6. 重複尋找和更正標籤的程序，直到您關心的帳號資源在每個區域都符合規定為止。

若要尋找不相容的標籤 (AWS CLI、 AWS API)

使用下列指令和作業來尋找不相容的標籤：

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

  如需中使用標籤原則的完整程序 AWS CLI，請參閱《使用指南》 AWS CLI中的〈使用標籤策略〉。AWS Organizations
- AWS Resource Groups Tagging API:
  - GetResources
  - TagResources
  - UntagResources

後續步驟

我們建議您重複尋找並更正合規性問題的程序。繼續操作，直到您關心的帳號資源符合每個區域中的有效標籤政策為止。

由於多種原因，尋找和更正不相容標籤是一種反覆的程序，其中包括：

- 貴組織對標籤政策的使用可能會隨著時間的推移而發展。
- 建立資源時，需要花費一些時間才能在組織中實現變更。
- 在建立新資源或將新標籤指定給資源時，符合性可隨時變更。
- 每當標籤策略附加或從其中分離時，帳號的有效標籤策略就會更新。每當發生變更以標記帳號繼承的策略時，也會更新有效的標籤策略。

如果您以組織中的管理帳戶身分登入，也可以產生報告。此報告顯示組織帳號中所有已標記資源的相關資訊。如需更多詳細資訊，請參閱 評估整個組織的合規性。

評估整個組織的合規性

您可以評估組織的有效標籤原則是否符合性。您可以產生一份報告，其中列出組織帳號中所有已標記的資源，以及每個資源是否符合有效標籤策略。

> **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 與使用**tag:none**. 如需詳細資訊，請參閱在 AWS 資源總管 用戶指南。

您可以從組織的管理帳戶中產生報告 us-east-1 AWS 區域 只有。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儲存貯體政策，如 Amazon S3 儲存貯體政策所示，才能存放報告。

若要產生整個組織的規範遵循報告，您必須具備下列權限：

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

如需顯示這些權限的範例IAM原則，請檢閱評估整個組織合規性的權限。

若要產生整個組織的符合性報告 (主控台)

1. 開啟「標籤策略」主控台。
2. 選擇 [這個組織根] 索引標籤，接近頁面底部的 [產生報告]。
3. 在「產生報告」畫面上，指定報告的儲存位置。
4. 選擇 [開始匯出]。

報告完成後，您可以從「組織根」標籤上的「不符合性報告」區段下載報告。

> **備註**
>
> 每 48 小時評估一次全組織的合規性。這會導致以下結果：

- 標籤原則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符合性報告中。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。該類型沒有此標記的資源最多可在 48 小時內在報告中顯示為符合標準。
- 雖然您可以隨時產生報告，但在下次評估完成之前，不會更新報告結果。
- 此NoncompliantKeys欄會列出資源上與有效標籤策略不相容的標籤索引鍵。
- 此資KeysWithNonCompliantValues料欄會列出資源上有效策略中定義的金鑰，其中包含不正確的大小寫處理方式或不相容值。
- 如果您關閉 AWS 帳戶 身為組織的成員，最多可持續出現在標籤符合性報告中 90 天。

若要產生整個組織的符合性報告 (AWS CLI, AWS API)

使用下列指令和作業來產生整個組織的符合性報告、檢查其狀態，以及檢視報告：

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

  如需在中使用標籤原則的完整程序 AWS CLI，請參閱在中使用標籤原則 AWS CLI 中的 AWS Organizations 用戶指南。
- AWS API:
  - StartReportCreation
  - DescribeReportCreation
  - GetComplianceSummary

使用無伺服器工作流程和 Amazon 監控標籤變更 EventBridge

Amazon EventBridge 支持對 AWS 資源進行標籤更改。使用此 EventBridge 類型，您可以建立 EventBridge規則以符合標籤變更，並將事件路由到一或多個目標。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 建置符合成本效益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。

標籤變更產生 EventBridge 事件

EventBridge 提供描述 AWS 資源變更的近乎即時的系統事件串流。許多 AWS 資源都支援標籤，這些標籤是自訂的使用者定義屬性，可輕鬆組織和分類 AWS 資源。標籤的常見使用案例包括成本分配分類、存取控制安全性和自動化。

使用 EventBridge，您可以監視標籤的變更，並追蹤資 AWS 源上的標籤狀態。以前，為了實現類似的功能，您可能會持續輪詢APIs和協調多個呼叫。現在，對標籤進行任何變更，包括個別服務APIs、標籤編輯器和標籤都API會在資源事件上啟動標籤變更。下列範例顯示標籤變更提示的典型 EventBridge 事件。它會顯示新的、更新或已刪除的標籤鍵，以及它們的關聯值。

```
{
  "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 事件都有相同的頂層欄位：

- version — 依預設，此值在所有事件中都設定為 0 (零)。
- id — 針對每個事件產生唯一值。這對於追蹤事件在規則之間移動到目標並進行處理時很有幫助。
- 詳細資訊類型 — 與source欄位結合識別出現在詳細資訊欄位中的欄位和值。
- 來源 — 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。
- 區域 — 識別事件 AWS 區域 的起始位置。
- 資源 — 此JSON陣列包含 Amazon 資源名稱 (ARNs)，可識別事件中涉及的資源。這是標籤已更改的資源。
- detail — 一個JSON對象，其內容是根據事件類型不同。對於資源的標籤變更，包括下列詳細欄位：
  - changed-tag-keys— 此事件所變更的標籤鍵。
  - 服務 — 資源所屬的服務。在這個例子中，服務是ec2，這是 Amazon EC2。
  - 資源類型 — 服務的資源類型。在這個例子中，它是一個 Amazon EC2 實例。
  - 版本 — 標籤組的版本。版本從 1 開始，並在標籤更改時遞增。您可以使用該版本來驗證標籤變更事件的順序。
  - 標籤 — 變更後附加至資源的標籤。

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，您可以根據不同欄位建立符合特定事件模式的規則。我們在教程中演示如何執行此操作。此外，我們還會展示如果指定的標籤未附加到EC2執行個體，Amazon 執行個體如何自動停止。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。您只在需要時才執行程式碼，而不必考慮伺服器。您只需為使用的確切運算時間付費。即使它被稱為無服務器，但並不意味著沒有服務器。在此情況下，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。 AWS 為你做所有這些，所以你可以專注於你的代碼。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

作為你的池 AWS 資源和 AWS 帳戶 您可以管理的增長，您可以使用標籤來更輕鬆地對資源進行分類。標籤通常用於關鍵使用案例，例如成本分配和安全性。為了有效管理 AWS 資源，您的資源需要一致地標記。通常，當資源佈建時，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，導致與公司標籤政策偏離。通過監控標籤的更改，您可以發現標籤漂移並立即響應。這使您更有信心，相信依賴於您的資源進行正確分類的過程將產生所需的結果。

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繼續具有必要的標籤。如果執行個體的標籤發生變更，且執行個體不再具有必要的標籤，則會叫用 Lambda 函數以自動關閉執行個體。你為什麼要這樣做？ 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，或者能夠信任基於屬性的訪問控制（ ）ABAC的安全性。

Important

我們強烈建議您在非生產帳戶中執行本教學課程，在此帳戶不會意外關閉重要的執行個體。本教學課程中的範例程式碼有意將此案例的影響限制為只有執行個體清單上的執行個體IDs。您必須使用願意關閉以進行測試的實例IDs更新列表。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，請確定所有執行個體都已根據貴公司的標記策略加上標籤。然後，您可以移除將函數限制為僅限於清單IDs上執行個體的程式碼。

這個例子使用 JavaScript 以及第 16.x 版本的 Node.js。 範例使用範例 AWS 帳戶 識別碼 123456789012 和 AWS 區域 美國東部 (維吉尼亞北部) (us-east-1)。使用您自己的測試帳戶 ID 和區域取代這些項目。

Note

如果您的主機使用不同的區域做為預設值，請務必在每次變更主機時切換您在本教學課程中使用的區域。本教程失敗的一個常見原因是在兩個不同的區域中具有實例和功能。

如果您使用的區域不同於us-east-1，請務必將下列程式碼範例中的所有參照變更為您選擇的 Region。

主題

- 步驟 1. 建立 Lambda 函式

步驟 1. 建立 Lambda 函式

建立 Lambda 函數

1. 開啟 AWS Lambda 管理主控台。
2. 選擇創建功能，然後選擇從頭開始作者。
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為預設值，然後選擇 [建立函數]。
6. 在`AutoEC2Termination`詳細資料頁面的 [程式碼] 索引標籤上，開啟 index.js 檔案以檢視其程式碼。

   - 如果開啟了包含 index.js 的頁籤，您可以選擇該頁籤中的編輯方塊來編輯其程式碼。
   - 如果未開啟含有 index.js 的索引標籤，請再按一下功能窗格中「自動」EC2Terminator 資料夾下方的 index.js 檔案。然後選擇「開啟」。
7. 在 index.js 選項卡中，將以下代碼粘貼到編輯器框中，替換已存在的任何內容。

   將值`RegionToMonitor`替換為您要在其中運行此函數的區域。

```
// 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，並使新版本的功能啟用。

這個 Lambda 函數會檢查 Amazon EC2 執行個體的標籤，如中的標籤變更事件所報告的 EventBridge。在此範例中，如果事件中的執行個體遺失必要的標籤鍵，`valid-key`或者該標記沒有該值`valid-value`，則函數會嘗試停止執行個體。您可以針對您自己的特定使用案例變更此邏輯檢查或標籤需求。

讓 Lambda 主控台視窗在瀏覽器中保持開啟狀態。

步驟 2. 設定所需的IAM權限

在函數成功執行之前，您必須授予函數停止執行個EC2體的權限。所以此 AWS 提供的角色 lambda_basic_execution沒有該權限。在本教學課程中，您會修改附加至名為之函數執行角色的預設IAM權限原則`AutoEC2Termination-role-`*`uniqueid`*。本教學課程所需的最低額外權限為`ec2:StopInstances`。

如需有關建立 Amazon EC2 特定IAM政策的詳細資訊，請參閱 AmazonEC2：允許啟動或停止EC2執行個體，以程式設計方式和IAM使用者指南中的主控台修改安全群組。

若要建立IAM權限原則並將其附加至 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`**，當它出現在清單中時，選擇角色名稱。
3. 在角色的 [摘要] 頁面上，選擇 [權限] 索引標籤，然後選擇已附加原則的名稱。
4. 在策略的 [摘要] 頁面上，選擇 [編輯策略]。
5. 在可視化編輯器索引標籤上，選擇新增其他權限。
6. 對於「服務」，請選擇EC2。

7. 對於「動作」，請選擇StopInstances。您可以**Stop**在搜索欄中鍵入，然後選擇出現的StopInstances時間。
8. 對於資源，請選擇 [所有資源]，選擇 [檢閱原則]，然後選擇 [儲存變更]。

   這會自動建立原則的新版本，並將該版本設定為預設版本。

   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，您將測試事件提交給您的函數。Lambda 測試功能的運作方式是提交手動提供的測試事件。該函數處理測試事件，就像事件來自一樣 EventBridge。您可以使用不同的值定義多個測試事件，

以便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，而且新標籤不包含所需的標籤金鑰和值。

若要測試您的 Lambda 函數

1. 使用 Lambda 主控台返回視窗或索引標籤，然後開啟自動EC2Termination功能的 [測試] 索引標籤。
2. 選擇 [建立新活動]。
3. 事件名稱輸入 **SampleBadTagChangeEvent**。
4. 在「事件」中JSON，以下列範例文字中顯示的範例事件取代文字。您不需要修改帳戶、地區或執行個體 ID，此測試事件即可正常運作。

```
{
  "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 test 事件中指定的實例不存在。

[函數記錄] 區段中 [執行結果] 索引標籤上的資訊說明您的 Lambda 函數成功嘗試停止執行個EC2體。但是，它失敗，因為程式碼一開始會嘗試停止執行個體的DryRun作業，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. 若要證明程式碼在使用正確的標籤時不會嘗試停止執行個體，您可以建立並提交另一個測試事件。

   選擇代碼源上方的測試選項卡。主控台會顯示您現有的SampleBadTagChangeEvent測試事件。
7. 選擇 [建立新活動]。
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] 事件視窗的頂端，選擇 [儲存]，然後選擇 [測試]。

    輸出會顯示下列內容，示範函數可辨識有效的標籤，而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
```

    讓 Lambda 主控台在瀏覽器中保持開啟狀態。

步驟 4. 建立啟動函數的 EventBridge 規則

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

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「建立規則」頁面的EventBridge 主控台。
2. 輸入名稱做為「名稱」**ec2-instance-rule**，然後選擇「下一步」。
3. 向下滾動到創建方法，然後選擇自定義模式（JSON編輯器）。
4. 在編輯方塊中，貼上下列樣式文字，然後選擇 [下一步]。

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

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

此規則會比對 Amazon EC2 執行個體的`Tag Change on Resource`事件，並在下一個步驟中叫用您指定為 Target 的任何事件。

5. 接下來，將您的 Lambda 函數新增為目標。在「目標 1」方塊中的「選取目標」下，選擇 Lambda 函數。
6. 在 [功能] 底下，選擇您先前建立的 [自動] EC2Termination 功能，然後選擇 [下一步]。
7. 在 [設定標記] 頁面上，選擇 [下一步]。然後在 [檢閱並建立] 頁面上，選擇 [建立規則]。這也會自動授與叫用 EventBridge 指定 Lambda 函數的權限。

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其標籤時會發生什麼情況，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 Amazon 主EC2控台前往執行個體頁面。
2. 創建一個 Amazon EC2 實例。在啟動它之前，請附加一個帶有鍵`valid-key`和值的標籤`valid-value`。如需如何建立和啟動執行個體的詳細資訊，請參閱 Amazon EC2 使用者指南中的步驟 1：啟動執行個體。在程序若要啟動執行個體，請在步驟 3 中輸入「名稱」標籤，同時選擇「新增其他標籤」，選擇「新增標籤」，然後輸入的「機碼」**valid-key** 與「值」**valid-value**。如果此執行個體僅用於本教學課程的目的，且您計劃在完成此執行個體之後刪除此執行個體，則您可以不使用 key pair 繼續。當您到達步驟 1 的結尾時，請返回本教學課程；您不需要執行步驟 2：Connect 至執行個體。
3. InstanceId從控制台複製。
4. 從 Amazon EC2 控制台切換到 Lambda 主控台。選擇您的自動EC2Termination功能，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. `InstanceList`透過貼上您從 Amazon EC2 主控台複製的值來變更中的第二個項目。請確定`RegionToMonitor`值與包含您貼上之例證的「區域」(Region) 相符。

6. 選擇「部署」使變更處於作用中狀態。該功能現在可以通過對指定區域中的該實例進行標籤更改來激活。
7. 從 Lambda 主控台切換到 Amazon EC2 主控台。
8. 刪除有效的金鑰標籤或變更該機碼的值，以變更附加至執行個體的標籤。

> **Note**
>
> 有關如何在執行中的 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。執行個體應變更其執行個體狀態為 [停止]，然後變更為 [已停止
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「記錄」標籤，然後在「最近的呼叫」表格中選擇欄中最近的項目。LogStream

    Amazon 主 CloudWatch 控台會開啟「日誌事件」頁面，以查看最後一次叫用 Lambda 函數。最後一個項目看起來應類似下列範例。

```
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
```

教程摘要

本教學課程示範如何建立 EventBridge 規則，以符合 Amazon EC2 執行個體資源事件上的標籤變更。該規則指向一個 Lambda 函數，如果實例沒有必要的標籤，該函數會自動關閉該實例。

Amazon 對標籤更改的 EventBridge 支持 AWS 資源為許多人打開了構建事件驅動自動化的可能性 AWS 服務。 將此功能與 AWS Lambda 為您提供工具來建置可存取的無伺服器解決方案 AWS 資源安全、隨需擴充，且符合成本效益。

該 tag-change-on-resource EventBridge 事件的其他可能用例包括：

- 如果有人從不尋常的 IP 位址存取您的資源，則啟動警告 — 使用標籤來儲存存取您資源的每位訪客的來源 IP 位址。對標籤的變更會產生 CloudWatch 事件。您可以使用該事件將來源 IP 位址與有效 IP 位址清單進行比較，並在來源 IP 位址無效時啟用警告電子郵件。
- 監視資源的以標籤為基礎的存取控制是否發生變更 — 如果您已使用以屬性 (標籤) 為基礎的存取控制 (ABAC) 設定資源的存取權，則可以使用標籤的任何變更所產生的 EventBridge事件來提示安全性團隊進行稽核。

排解標籤變更

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，資源最多可以有 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權限。如果您沒有檢視資源現有標籤的權限，就無法變更資源的標籤。
- 您可能沒有變更資源的權限。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，假設資源是在建立 AWS CloudFormation 堆疊的過程中啟動的。如果堆疊已刪除或不再處於使用中狀態，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，則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。
- 雖然有費率限制 AWS Resource Groups Tagging API，但是您標記的服務可能會強加一個單獨的限制，您可能會在 Resource Groups 標記API限制之前達到此限制。

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。標題會針對每種發生的失敗類型顯示錯誤訊息。對於每個錯誤，橫幅會識別標籤編輯器無法在其上進行標籤變更的特定資源。檢閱並疑難排解錯誤後，請選擇 [在資源上重試失敗的標籤變更]，以僅對標籤變更失敗的資源重試變更。

標籤編輯器的安全性

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

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

- 雲端本身的安全 – AWS 負責保護在 AWS 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。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規範遵循計劃的詳細資訊，請參閱符合性計劃範圍內的AWS服務。
- 雲端內部的安全：您的責任取決於所使用的 AWS 服務。您也必須對其他因素負責，包括資料的機密性、您公司的請求和適用法律和法規。

本文件可協助您瞭解如何在使用標籤編輯器時套用共同的責任模型。下列主題說明如何設定標籤編輯器，以符合安全性和合規性目標。

主題

標籤編輯器中的資料保護

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

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

- 對每個帳戶使用多重要素驗證 (MFA)。
- 使用SSL/TLS與之溝通 AWS 的費用。我們需要 TLS 1.2 並推薦 TLS 1.3。
- 設定API和使用者活動記錄 AWS CloudTrail。 如需使用 CloudTrail 軌跡進行擷取的相關資訊 AWS 活動，請參閱使用 CloudTrail 系統線 AWS CloudTrail 使用者指南。
- 使用 AWS 加密解決方案，以及其中的所有默認安全控制 AWS 服務.
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Amazon S3 的敏感資料。
- 如果您在訪問時需要 FIPS 140-3 驗證的加密模塊 AWS 透過指令行介面或API使用FIPS端點。如需有關可用FIPS端點的詳細資訊，請參閱聯邦資訊處理標準 (FIPS) 140-3。

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

資料加密

標籤資訊不會加密。雖然未加密，但標籤可能包含作為安全策略的一部分使用的資訊，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，因為這種訪問可以用來提升一個人的權限。

靜態加密

沒有其他方法可隔離標籤編輯器專屬的服務或網路流量。如果適用，請使用 AWS 特定的隔離。您可以在虛擬私有雲 (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架構安全性。

傳輸中加密

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

金鑰管理

標籤編輯器目前未與 AWS Key Management Service 並且不支持 AWS KMS keys.

網際網路流量隱私權

標籤編輯器用HTTPS於標籤編輯器使用者和 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 管理員會控制誰可以進行身分驗證 （ 登入 ） 和授權 （ 具有許可 ），以使用標籤編輯器資源。IAM 是 AWS 服務 您可以免費使用的 。

主題

物件

使用 AWS Identity and Access Management （ IAM ） 的方式會有所不同，具體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 Tag Editor 服務來執行您的任務，則您的管理員會為您提供所需的憑證和許可。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 疑難排解標籤編輯器身分識別。

服務管理員 – 如果您在公司負責 Tag Editor 資源，您可能擁有 Tag Editor 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。然後，您必須向IAM管理員提交請求，以變更服務使用者的許可。請檢閱此頁面上的資訊，以了解 的基本概念IAM。若要進一步了解貴公司如何IAM搭配標籤編輯器使用 ，請參閱 標籤編輯器如何使用 IAM。

IAM 管理員 – 如果您是IAM管理員，您可能想要了解如何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 中使用的標籤編輯器身分型政策範例IAM，請參閱 標籤編輯器身分識別原則範例。

使用身分驗證

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角色來驗證 （ 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 憑證，都是聯合身分的範例。當您以聯合身分登入時，您的管理員先前會使用 IAM角色設定身分聯合。當您 AWS 使用聯合來存取 時，您會間接擔任 角色。

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

如果您以 AWS 程式設計方式存取 ， AWS 會提供軟體開發套件 （ SDK ） 和命令列介面 （ CLI ），以使用您的憑證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。如需使用建議方法自行簽署請求的詳細資訊，請參閱 IAM 使用者指南 中的簽署 AWS API請求。

無論您使用何種身分驗證方法，您可能都需要提供額外的安全性資訊。例如， AWS 建議您使用多重要素身分驗證 （ MFA ） 來提高帳戶的安全性。若要進一步了解，請參閱AWS IAM Identity Center 使用者指南中的多重要素驗證，以及使用者指南中的使用多重要素驗證 （ MFA ） AWS。 IAM

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，該身分可完全存取 帳戶中的所有 AWS 服務 和資源。此身分稱為 AWS 帳戶 根使用者，透過您用來建立帳戶的電子郵件地址和密碼登入來存取。強烈建議您不要以根使用者處理日常任務。保護您的根使用者憑證，並將其用來執行只能由根使用者執行的任務。如需需要您以根使用者身分登入的任務完整清單，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。在可能的情況下，我們建議您依賴臨時憑證，而不是建立具有密碼和存取金鑰等長期憑證IAM的使用者。不過，如果您有特定的使用案例需要IAM使用者長期憑證，建議您輪換存取金鑰。如需詳細資訊，請參閱 IAM 使用者指南 中的定期輪換需要長期憑證的使用案例存取金鑰。

IAM 群組是指定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，您可以擁有名為 的群組IAMAdmins，並授予該群組管理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。若要進一步了解，請參閱 IAM 使用者指南 中的何時建立IAM使用者 （ 而非角色 ）。

角色

IAM 角色是 中具有特定許可 AWS 帳戶 的身分。它類似於IAM使用者，但與特定人員無關。您可以透過 AWS Management Console 切換IAM角色 暫時在 中擔任角色。 https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_switch-role-console.html您可以呼叫 AWS CLI 或 AWS API 操作，或使用自訂 來擔任角色URL。如需使用角色方法的詳細資訊，請參閱 IAM 使用者指南 中的擔任角色的方法。

IAM 具有臨時憑證的角色在下列情況下很有用：

- 聯合身分使用者存取 — 如需向聯合身分指派許可，請建立角色，並為角色定義許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並獲授予由角色定義的許可。如需聯合角色的相關資訊，請參閱 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，您可以設定許可集。若要控制身分在身分驗證後可以存取的內容，IAMIdentity Center 會將許可集與 中的角色相關聯IAM。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。
- 臨時IAM使用者許可 – IAM使用者或角色可以擔任IAM角色，暫時接受特定任務的不同許可。
- 跨帳戶存取 – 您可以使用 IAM角色，允許不同帳戶中的某人（受信任的委託人）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。不過，使用某些 AWS 服務，您可以將政策直接連接至資源（而不是使用角色作為代理）。若要了解跨帳戶存取的角色和資源型政策之間的差異，請參閱 IAM 使用者指南 中的跨帳戶資源存取IAM。
- 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 服務中撥打電話時，該服務通常會在 Amazon 中執行應用程式EC2或在 Amazon S3 中儲存物件。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，您會被視為主體。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 請求向下游服務 AWS 服務 提出請求。FAS 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時，才會發出請求。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，請參閱轉送存取工作階段。
  - 服務角色 – 服務角色是服務代表您執行動作所擔任IAM的角色。IAM 管理員可以從 內部建立、修改和刪除服務角色IAM。如需詳細資訊，請參閱 使用者指南 中的建立角色以將許可委派給 AWS 服務 。 IAM
  - 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。服務連結角色會顯示在您的 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 上執行的應用程式 EC2 – 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憑證，以及提出 AWS CLI 或 AWS API請求。最好將存取金鑰存放在EC2執行個體中。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設定檔。執行個體設定檔包含 角色，並啟用在EC2執行個體上執行的程式，以取得臨時憑證。如需詳細資訊，請參閱 IAM 使用者指南 中的使用 IAM角色將許可授予在 Amazon EC2執行個體上執行的應用程式。

若要了解如何使用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至 AWS 身分或資源 AWS 來控制 中的存取。政策是 AWS 其中的物件，當與身分或資源建立關聯時， 會定義其許可。當主體 （ 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。大多數政策都以JSON文件 AWS 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，使用者可以擔任角色。

IAM 無論您用來執行操作的方法為何，政策都會定義動作的許可。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 AWS 取得角色資訊API。

身分型政策

身分型政策是JSON許可政策文件，您可以附加到身分，例如IAM使用者、使用者群組或角色。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。若要了解如何在受管政策或內嵌政策之間進行選擇，請參閱 IAM 使用者指南 中的在受管政策與內嵌政策之間進行選擇。

資源型政策

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

存取控制清單 （ ACLs ）

存取控制清單 （ ACLs ） 控制哪些主體 （ 帳戶成員、使用者或角色 ） 具有存取 資源的許可。ACLs 類似於資源型政策，雖然它們不使用JSON政策文件格式。

Amazon S3 AWS WAF和 Amazon VPC是支援 的服務範例ACLs。若要進一步了解 ACLs，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 – 許可界限是一項進階功能，您可以在其中設定身分型政策可授予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是在 中指定組織或組織單位 （ OU ） 最大許可JSON的政策 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。如果您啟用組織中的所有功能，則可以將服務控制政策 （ SCPs ） 套用至任何或所有帳戶。SCP 限制成員帳戶中實體的許可，包括每個 AWS 帳戶根使用者。如需 Organizations 和 的詳細資訊SCPs，請參閱 AWS Organizations 使用者指南 中的服務控制政策。
- 工作階段政策 – 工作階段政策是一種進階政策，您可以在透過編寫程式的方式建立角色或聯合使用者的暫時工作階段時，作為參數傳遞。所產生工作階段的許可會是使用者或角色的身分型政策和工作階段政策的交集。許可也可以來自資源型政策。所有這類政策中的明確拒絕都會覆寫該允許。如需詳細資訊，請參閱 IAM 使用者指南 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 決定是否在涉及多種政策類型時允許請求，請參閱 IAM 使用者指南 中的政策評估邏輯。

標籤編輯器如何使用 IAM

在使用IAM管理標籤編輯器的存取權限之前，您應該瞭解哪些IAM功能可用於標籤編輯器。若要取得標籤編輯器和其他使 AWS 服務 用方式的高階檢視IAM，請參閱AWS 服務《IAM使用者指南》IAM中的使用方式。

主題

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

標籤編輯器身分型原則

使用以IAM身分識別為基礎的策略，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。若要瞭解您在JSON策略中使用的所有元素，請參閱《使用IAM者指南》中的IAMJSON策略元素參考資料。

動作

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

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

政策會使用動作來授予執行相關聯動作的許可。

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

例如，若要授與某人使用該`tag:TagResources`API作業標記資源的權限，您可以在其策略中包含該`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一組動作，說明您可以使用此服務執行的工作。

若要在單一陳述式中指定多個標記動作，請以逗號分隔，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清單，請參閱服務授權參考中標籤編輯器的動作、資源和條件索引鍵。

資源

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

ResourceJSON原則元素會指定要套用動作的一或多個物件。陳述式必須包含 Resource 或 NotResource 元素。最佳做法是使用其 Amazon 資源名稱 (ARN) 指定資源。您可以針對支援特定資源類型的動作 (稱為資源層級許可) 來這麼做。

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

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

標籤編輯器沒有自己的任何資源。相反地，它會操作附加到由其他 AWS 服務人建立的資源的中繼資料 (標籤)。

條件索引鍵

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

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

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

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

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

標籤編輯器不會定義任何服務特定的條件金鑰。

範例

若要檢視以標籤編輯器身分為基礎的策略範例，請參閱。標籤編輯器身分識別原則範例

資源型政策

標籤編輯器不支援以資源為基礎的政策，因為它不會定義自己的任何資源。

以標籤為基礎的授權

基於標籤的授權是稱為基於屬性的訪問控制（ ）ABAC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、或條件索引鍵在策略的條aws:TagKeys件元素中aws:ResourceTag/*key-name*提供標籤資訊。aws:RequestTag/*key-name*您可以在建立或更新資源時將標籤套用至資源。

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，請參閱根據標記檢視群組。如需有關以屬性為基礎的存取控制 (ABAC) 的詳細資訊，請參閱什麼ABAC用途？ AWS在《IAM使用者指南》中。

標籤編輯器IAM角色

IAM角色是您 AWS 帳戶 中具有特定權限的實體。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認證

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

服務連結角色

服務連結角色可 AWS 服務 讓您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。

標籤編輯器身分識別原則範例

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權限。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，以授與主體權限，才能在所需的指定資源上執行特定 API 操作。然後管理員必須將這些原則附加至需要這些權限的主參與者。

如需使用這些 JSON 政策文件範例建立 IAM 身分型政策的指示，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
- 使用標籤編輯器主控台和 Resource Groups 標記 API
- 允許使用者檢視他們自己的許可
- 根據標記檢視群組

政策最佳實務

以身分識別為基礎的政策會決定某人是否可以建立、存取或刪除您帳戶中的「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 受管政策並朝向最低權限許可的目標邁進：如需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。
- 套用最低許可許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的權限。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。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。如需更多資訊，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。如需更多資訊，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。如需在呼叫 API 操作時請求 MFA，請將 MFA 條件新增至您的政策。如需更多資訊，請參閱 IAM 使用者指南中的設定 MFA 保護的 API 存取。

有關 IAM 中最佳實務的更多相關資訊，請參閱 IAM 使用者指南中的 IAM 最佳安全實務。

使用標籤編輯器主控台和 Resource Groups 標記 API

若要存取標籤編輯器主控台和 Resource Groups 標記 API，您必須擁有最少一組權限。這些權限必須允許您列出和檢視有關附加至您的資源之標籤的詳細資料AWS 帳戶。如果您建立的身分型政策限制比最低所需權限更嚴格，則控制台和 API 命令將無法按照具有該政策的 IAM 主體預期運作。

若要確保這些主體仍可使用「標籤編輯器」，請將下列原則 (或包含下列原則所列權限的原則) 附加至實體。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": "*"
    }
  ]
```

```
}
```

如需授與標籤編輯器和 Resource Groups 標記 API 存取權的詳細資訊，請參閱[授與使用標籤編輯器的權限](#)。

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，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": "*"
        }
    ]
}
```

根據標記檢視群組

您可以使用身分型原則中的條件，根據標籤控制對標籤編輯器資源的存取。此範例顯示如何建立允許檢視資源的策略 (在此範例中為資源群組)。不過，只有當群組標記project的值與附加至呼叫主體的project標籤值相同時，才會授與權限。

```
{
    "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，則該群組也必須加上標籤project=alpha。否則，用戶將被拒絕訪問。條件標籤鍵 project 符合 Project 和 project，因為條件索引鍵名稱不區分大小寫。如需更多資訊，請參閱《IAM 使用者指南》中的 IAM JSON 政策元素：條件。

疑難排解標籤編輯器身分識別

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

主題

- 我沒有在標籤編輯器中執行動作的授權
- 我沒有授權執行 iam：PassRole

我沒有在標籤編輯器中執行動作的授權

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。您的管理員是為您提供登入憑證的人員。

當使用者mateojackson嘗試使用主控台檢視資源的標籤，但沒有tag:GetTagKeys權限時，就會發生下列範例錯誤。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 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。

我沒有授權執行 iam：PassRole

如果您收到未獲授權執行iam:PassRole動作的錯誤訊息，您必須更新原則，才能將角色傳遞給標籤編輯器。

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

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

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

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

如需任何協助，請聯絡您的 AWS 管理員。您的管理員提供您的登入憑證。

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。

記錄標籤編輯器 API 呼叫 CloudTrail

標籤編輯器與服務整合AWS CloudTrail，可提供使用者、角色或標籤編輯器AWS 服務中所採取的動作記錄的服務。 CloudTrail 將標籤編輯器的所有 API 呼叫擷取為事件，包括來自標籤編輯器主控台

的呼叫，以及從 Resource Groups 標記 API 的程式碼呼叫。如果您建立追蹤，您可以啟用持續傳遞 CloudTrail 事件到 Amazon S3 儲存貯體，包括標籤編輯器的事件。如果您未設定追蹤，您仍然可以在 [事件歷程記錄] 中檢視 CloudTrail 主控台中最近的事件。使用收集的資訊 CloudTrail，您可以判斷向「標籤編輯器」提出的要求、提出要求的 IP 位址、提出要求的人員、提出要求的時間，以及其他詳細資訊。

若要取得有關的更多資訊 CloudTrail，請參閱AWS CloudTrail使用者指南。

標籤編輯器資訊 CloudTrail

CloudTrail 在您創建帳戶AWS 帳戶時啟用。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 CloudTrailAWS 服務事件一起記錄在事件中。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。

若要在您AWS 帳戶的中持續記錄事件 (包括標籤編輯器的事件)，請建立追蹤。追蹤可 CloudTrail 將日誌檔交付到 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，您可以設定其他，AWS 服務以進一步分析 CloudTrail 記錄中收集的事件資料並採取行動。如需詳細資訊，請參閱下列資源：

- 建立 AWS 帳戶 的追蹤
- CloudTrail 支援的服務和整合
- 設定 Amazon SNS 通知 CloudTrail
- 從多個區域接收 CloudTrail 日誌文件和從多個帳戶接收 CloudTrail 日誌文件

所有標籤編輯器動作均由記錄， CloudTrail 並記錄在標籤編輯器 API 參考中。控制台中的標籤編輯器動作由記錄 CloudTrail，並顯示`tagging.amazonaws.com`為事件`eventSource`。

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

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

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

瞭解標籤編輯器記錄檔項目

追蹤是一種組態，可讓事件以日誌檔的形式傳遞到您指定的 Amazon S3 儲存貯體。 CloudTrail 記錄檔包含一或多個記錄項目。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 日誌文件不是公共 API 調用的有序堆棧跟踪，因此它們不會以任何特定順序顯示。

下列範例顯示示範動作的 CloudTrail 記錄項目`TagResources`。

```
{
    "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"
    }
}
```


標籤編輯器的符合性驗證

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

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

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

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

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

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

標籤編輯器中的彈性

標籤編輯器執行內部服務資源的自動備份。使用者無法設定這些備份。備份在靜態和傳輸中都會加密。標籤編輯器會將客戶資料存放在 Amazon DynamoDB 中。

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

如果您不小心刪除了標籤，請聯絡AWS Support中心。

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。

標籤編輯器中的基礎結構

標籤編輯器不提供隔離服務或網路流量的其他方式。如果適用，請使用AWS特定的隔離。您可以在虛擬私有雲 (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架構安全性。

您可以使用AWS已發佈的 API 呼叫透過網路存取標籤編輯器。用戶端必須支援下列項目：

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

此外，請求必須使用存取金鑰 ID 和與 AWS Identity and Access Management (IAM) 主體相關聯的私密存取金鑰來簽署。或者，您可以使用 AWS Security Token Service (AWS STS) 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標籤編輯器 API 作業，但是「標籤編輯器」確實支援以資源為基礎的存取原則，其中可能包含以來源 IP 位址為基礎的限制。您也可以使用標籤編輯器政策來控制來自特定 Amazon Virtual Private Cloud 端 (Amazon VPC) 端點或特定 VPC 的存取。實際上，此方法僅將對特定資源的網路存取從網路內的特定 VPC 隔離出來AWS。

Service Quotas

下表提供「標籤編輯器」服務配額的相關資訊。

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

名稱	預設
每個資源附加的標籤	50 個使用者定義的標籤 (AWS 產生的標籤不會計入此限制)。
標籤鍵名稱	最少為 1，UTF-8 中最多 128 個萬國碼字符。 允許的字元包括字母、數字、空格和下列字元： `_ . : / = + - @` 密鑰名稱不能以開頭，`aws:`因為該前綴是保留供 AWS 使用的。 **Note** AWS 服務 有些則有一些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	最小值為 0，UTF-8 中最多 256 個萬國碼字元。 允許的字元包括字母、數字、空格和下列字元： `_ . : / = + - @`

名稱	預設	
	Note AWS 服務 有些則有一些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。	
呼叫作GetResourcesAPI業的速率	每秒最多 15 個通話	
調用以下API操作的速率： • TagResources • UntagResources • GetTagKeys • GetTagValues	每秒最多 5 個通話	

標籤編輯器文件記錄

變更	描述	日期
更新評估整個組織合規性的權限	已更新評估整個組織之符合性的權限，以包含協助存取規範遵循報告的權限。	2024年8月28日
已更新內容	更新了主題標題和重新整理的內容，以提高可讀性和可探索性。	2024年7月25日
標記內容 AWS 一般參考 移至本指南	有關標記的主題 AWS 資源已從 AWS 一般參考 本指南。	2023 年 3 月 24 日
IAM最佳實踐更新	更新指南以符合最IAM佳做法。如需詳細資訊，請參閱 IAM.	2023 年 1 月 3 日
將標籤編輯器文件移至自己的指南	標籤編輯器文件現在在其自己的使用者指南中提供，而不是 AWS Resource Groups 使用者指南。	2022 年 12 月 13 日
檢查是否符合標籤政策	使用建立標籤策略並將其附加至帳號之後 AWS Organizations，您可以在組織帳戶中的資源上找到不符合標籤。	2019 年 11 月 26 日
標籤編輯器現在支援尋找未標記的資源	您現在可以在「標籤編輯器」中搜尋未套用特定標籤鍵的標籤值的資源。	2019 年 6 月 18 日
標籤編輯器主控台移出 AWS Systems Manager 控制台	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	2019 年 6 月 5 日

	標，但您可以直接從左上角的下拉式功能表開啟「標籤編輯器」主控台 AWS Management Console.	
舊版的舊式標籤編輯器工具不再可用	舊版、傳統或舊版「標籤編輯器」的提及已移除；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標記資源	標籤編輯器現在可讓您跨多個區域搜尋和管理資源標籤，並且預設會將您目前的區域新增至資源查詢。	2019 年 5 月 2 日
標籤編輯器現在支援將查詢結果匯出至 CSV	您可以將 [尋找要標記的資源] 頁面上的查詢結果匯出至CSV格式化的檔案。標籤編輯器查詢結果中會顯示新的區域欄。標籤編輯器現在可讓您搜尋特定標籤索引鍵具有空白值的資源。標籤索引鍵值會在您輸入現有索引鍵中的唯一值時自動完成。	2019 年 4 月 2 日
標籤編輯器現在支援將所有資源類型新增至查詢	您最多可以在單一操作中對個別資源類型套用 20 個標籤，或者您可以選擇 All resource types (所有資源類型) 以查詢區域中的所有資源類型。自動完成已新增至查詢的 Tag key (標籤索引鍵) 欄位，以協助在資源間實現一致的標籤索引鍵。如果標籤變更在某些資源上失敗，您可以僅在標籤變更失敗的資源上變更重試標籤變更。	2019 年 3 月 19 日

標籤編輯器現在支援搜尋中的多種資源類型	您可以在單一操作中對最多 20 個資源類型套用標籤。您也可以選擇在搜尋結果中顯示的欄位，包含在您的搜尋結果中找到的每個唯一標籤索引鍵或從結果選取資源的欄位。	2019 年 2 月 26 日

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。