aws

管理員指南

AWS Service Catalog

AWS Service Catalog: 管理員指南

Table of Contents

什麼是 Service Catalog？

Service Catalog 可讓組織建立及管理已核准的 IT 服務目錄AWS。這些 IT 服務可以包括虛擬機器映像、伺服器、軟體、資料庫等所有內容，以完成多層應用程式架構。

Service Catalog 可讓組織集中管理常用部署的 IT 服務，並協助組織達成一致的控管並符合法規遵循需求。最終使用者可在機構所設的限制範圍內，迅速地只部署自己需要且經核准的 IT 服務。

Service Catalog 提供下列優點：

- 標準化

  藉由限制產品可啟動的位置和可使用的執行個體類型，加上其他許多組態方面的選項，對經核准的資產加以管理。如此便能讓在整個組織中佈建的產品達到標準化的形式。
- 自助服務的探索和啟動

  使用者可瀏覽自己具有存取權限的產品 (服務或應用程式) 清單、找出想要使用的產品、自行將產品啟動為佈建產品。
- 精細的存取控制

  管理員從其目錄中組合產品組合，新增要在佈建時使用的限制條件和資源標籤，然後透過 AWS Identity and Access Management (IAM) 使用者和群組授予產品組合的存取權。
- 可擴充性和版本控制

  管理員可將產品加入數量不受限制的產品組合中，無需建立另一個複本便能加以設限。將產品更新為新版本後，便會將更新擴及所有參考該產品的產品組合中的所有產品。

如需詳細資訊，請參閱 Service Catalog 詳細資訊頁面。

Service Catalog API 提供對所有使用者動作的程式設計控制，作為使用AWS Management Console. 如需詳細資訊，請參閱 Service Catalog 開發人員指南。

視頻：介紹 AWS Service Catalog

此影片 (7:27) 說明如何建立、組織和管理精選的AWS產品目錄，以及如何使用權限層級共用產品。因此，使用者可以快速佈建已核准的 IT 資源，而無需直接存取基礎AWS服務。

簡介 AWS Service Catalog

Service Catalog 概觀

當您開始使用 Service Catalog 時，您將受益於瞭解其元件，以及系統管理員和使用者的初始工作流程。

使用者

Service Catalog 支援下列類型的使用者：

- 目錄管理員 (管理員) — 管理產品目錄 (應用程式和服務)、將產品組織到產品組織中，並將存取權授與最終使用者。目錄管理員可準備AWS CloudFormation範本、設定限制和管理產品的 IAM 角色，以提供進階資源管理。
- 一般使用者 — 從其 IT 部門或管理員接收AWS認證，並使用AWS Management Console來啟動已授與其存取權的產品。有時僅僅稱為使用者，可以根據您的營運要求授予最終使用者不同許可。例如，使用者可能會有最大權限等級 (以啟動和管理他們使用的產品所需的所有資源)，或僅許可使用特定服務功能。

產品

產品是您想要在其上進行部署的 IT 服務AWS。產品包含一或多個AWS資源，例如 EC2 執行個體、儲存磁碟區、資料庫、監控組態和聯網元件或封裝產AWS Marketplace品。產品可以是執行 AWS Linux 的單一運算執行個體、在其自身環境中執行的完整設定多層 Web 應用程式，或是介於兩者之間的任何項目。

您可以透過匯入AWS CloudFormation範本來建立產品。 AWS CloudFormation範本定義產品所需的AWS資源、資源之間的關係，以及使用者在啟動產品以配置安全性群組、建立金鑰配對以及執行其他自訂時可插入的參數。

HashiCorp 地形開源和地形雲支持

AWS Service Catalog透過內部 HashiCorp Terraform 開放原始碼和 Terraform 雲端設定進行控管的快速自助佈建。AWS您可以使用 Service Catalog 做為單一工具，在其中大規模組織、控管和散發 Terraform 組態。AWS您可以存取 Service Catalog 的主要功能，包括編目標準化和預先核准的 Terraform 範本、存取控制、最低權限佈建、版本控制、標記，以及共用至數千個帳戶。AWS您的使用者會看到他們有權存取的產品和版本的簡單清單，然後只要一個動作即可部署這些產品。

若要深入瞭解並完成 Terraform 產品教學課程，請參閱。開始使用地形產品

佈建產品

AWS CloudFormation堆疊可讓您以單一單元的形式佈建、標記、更新和終止產品實例，讓您更輕鬆地管理產品的生命週期。AWS CloudFormation 堆疊包括以 JSON 或 YAML 格式撰寫的 AWS CloudFormation 範本，及其相關的資源集合。佈建產品是一個堆疊。當一般使用者啟動產品時，Service Catalog 佈建的產品執行個體就是一個堆疊，其中包含執行產品所需的資源。如需詳細資訊，請參閱 AWS CloudFormation 使用者指南。

產品組合

產品組合是包含組態資訊的產品集合。產品組合會協助管理可使用特定產品的人與其使用方法。透過 Service Catalog，您可以為組織中的每種使用者類型建立自訂產品組合，並選擇性地授與適當產品組合的存取權。當您新增新的產品版本至產品組合時，該版本會自動提供給所有使用者。

您也可以與其他AWS帳戶共用您的產品組合，並允許這些帳戶的管理員透過其他限制來分發您的產品組合，例如限制使用者可以建立的 EC2 執行個體。透過使用產品組合、許可、共享和限制，您可以確保使用者所啟動的產品經過正確設定，以符合組織的需要和標準。

版本控制

Service Catalog 可讓您管理目錄中產品的多個版本。此方法可讓您根據軟體更新或組態變更，新增範本和相關資源的新版本。

當您建立新版本的產品時，更新將自動散佈至所有可存取產品的使用者，讓使用者選擇使用何種版本的產品。使用者可快速、簡單的更新執行中的產品執行個體到新版本。

許可

授予使用者對產品組合的存取權限，並讓該使用者瀏覽產品組合以啟動其中包含的產品。您可以套用 AWS Identity and Access Management (IAM) 許可以控制誰可以檢視和修改您的目錄。您可以將 IAM 許可指派給 IAM 使用者、群組和角色。

當使用者啟動具有指派 IAM 角色的產品時，Service Catalog 會使用該角色來啟動產品的雲端資源AWS CloudFormation。透過為每個產品指派 IAM 角色，您可以避免授予使用者執行未核准作業的權限，並讓他們能夠使用目錄佈建資源。

限制

限制可控制您為產品部署特定AWS資源的方式。您可以使用它們來套用限制到產品以便監管或控制成本。AWS Service Catalog 的限制有所不同：啟動限制、通知限制和範本限制。

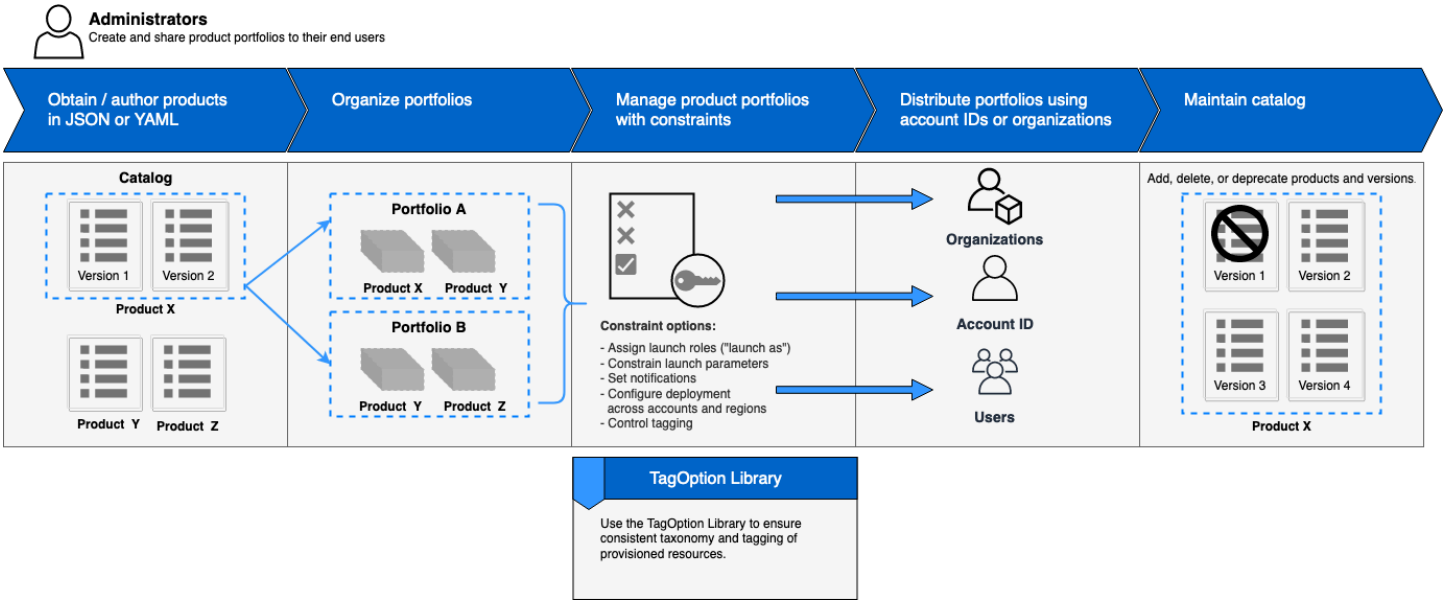
透過啟動限制，您可為產品組合中的產品指定角色。使用此角色可在啟動時佈建資源，以便您可以限制使用者權限，而不會影響使用者從目錄佈建產品的能力。

通知限制可讓您使用 Amazon SNS 主題取得有關堆疊事件的通知。

範本限制條件會限制組態參數，這些參數可讓使用者啟動產品時使用。(例如，EC2 執行個體類型或 IP 地址範圍)。透過範本限制，您可再次為產品使用通用的 AWS CloudFormation 範本，並以每套產品或產品組合的基礎套用限制到範本。

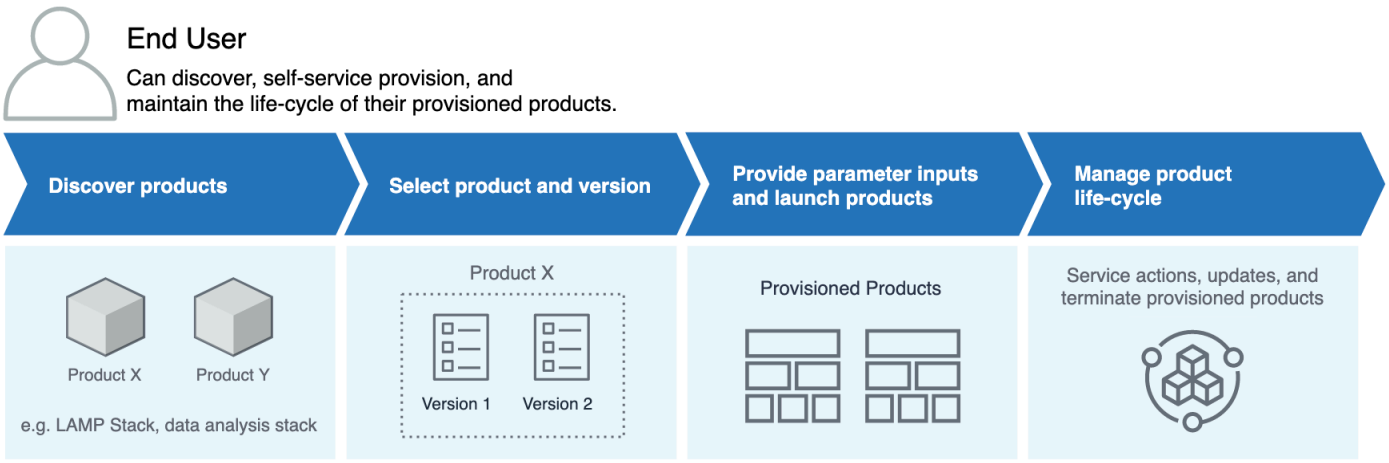
初始管理者工作流程

此圖表顯示管理員建立目錄的初始工作流程。



初始最終使用者工作流程

此圖表顯示一般使用者的初始工作流程。



AWS Service Catalog 預設服務配額

您的AWS帳戶具有下列預設配額AWS Organizations，限制，產品組合，產品，佈建的產品，地區，服務動作和 TagOptions.

您可以用Service Quotas來管理配額或要求提高配額。如需相關資訊Service Quotas，請參閱什麼是 Service Quotas？ 在《Service Quotas使用者指南》中。若要了解如何請求增加配額，請參閱請求增加配額。

AWS Organizations

- 每個組織的 AWS Service Catalog 委派管理員：50

限制條件配額

- 各產品組合各產品的限制條件：100

產品組合配額

- 各產品組合的使用者、群組、角色：100
- 各產品組合的產品：150
- 各產品組合的標籤：20
- 各產品組合的共用帳戶：5000
- 各標籤金鑰的標籤值：25

產品配額

- 各產品組的使用者、群組和角色：200
- 各產品的產品版本：100
- 各產品的標籤：20
- 各標籤金鑰的標籤值：25

佈建產品配額

- 各佈建產品的標籤：50

區域配額

- 產品組合：100
- 產品：350

服務動作配額

- 每個區域的服務動作：200
- 每個產品版本的服務動作關聯：25

TagOptions 配額

- TagOptions 每個資源：25
- 每個值 TagOption：25

設定 AWS Service Catalog

開始使用 AWS Service Catalog 之前，請完成以下工作。

主題

註冊 AWS 帳戶

如果您還沒有 AWS 帳戶，請完成以下步驟建立新帳戶。

註冊 AWS 帳戶

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

   部分註冊程序需接收來電，並在電話鍵盤輸入驗證碼。

   註冊 AWS 帳戶時，會建立 AWS 帳戶根使用者。根使用者有權存取該帳戶中的所有 AWS 服務和資源。作為最佳安全實務，將管理存取權指派給管理使用者，並且僅使用根使用者來執行需要根使用者存取權的任務。

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

建立管理使用者

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

保護您的 AWS 帳戶根使用者

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

   如需使用根使用者登入的說明，請參閱 AWS 登入使用者指南中的以根使用者身分登入。

2. 若要在您的根使用者帳戶上啟用多重要素驗證 (MFA)。

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

建立管理使用者

1. 啟用 IAM Identity Center。

   如需指示，請參閱 AWS IAM Identity Center 使用者指南中的啟用 AWS IAM Identity Center。

2. 在 IAM Identity Center 中，將管理權限授予管理使用者。

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

以管理員的身分登入

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

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

若要提供存取權，請新增權限至您的使用者、群組或角色：

- AWS IAM Identity Center 中的使用者和群組：

  建立權限合集。請遵循 AWS IAM Identity Center 使用者指南 的 建立權限合集 中的指示。

- 透過身分提供者在 IAM 中管理的使用者：

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

- IAM 使用者：
  - 建立您的使用者可擔任的角色。請遵循 IAM 使用者指南 的 為 IAM 使用者建立角色 中的指示。
  - (不建議) 將政策直接附加至使用者，或將使用者新增至使用者群組。請遵循 IAM 使用者指南 的 新增權限至使用者 (主控台) 中的指示。

授與權限給AWS Service Catalog管理員

身為目錄管理員，您需要存取AWS Service Catalog管理員主控台檢視和 IAM 許可，以便執行下列工作：

- 建立與管理產品組合
- 建立與管理產品
- 新增範本限制條件，以控制最終使用者啟動產品時的選項。
- 新增啟動限制以定義最終使用者啟動產品時AWS Service Catalog假設的 IAM 角色
- 將產品的存取權限授予最終使用者

您或管理 IAM 許可的管理員必須將政策附加到完成本教學課程所需的 IAM 使用者、群組或角色。

將許可授予目錄管理員

1. 開啟位於 https://console.aws.amazon.com/iam/ 的 IAM 主控台。
2. 在功能窗格中，選擇 [存取管理]，然後選擇 [使用者]。如果您已建立要做為目錄管理員使用的 IAM 使用者，請選擇使用者名稱，然後選擇 [新增權限]。若尚未建立，請按以下步驟建立使用者：
   a. 選擇新增使用者。
   b. 針對 User name (使用者名稱)，輸入 **`ServiceCatalogAdmin`**。
   c. 選擇 Programmatic access (程式設計存取) 和 AWS Management Console 存取。
   d. 選擇 Next: Permissions (下一步：許可)。
3. 選擇直接連接現有政策。
4. 選擇 [建立原則]，然後執行下列動作：
   a. 選擇 JSON 標籤。
   b. 複製下列範例原則，並將其貼到「策略文件」中：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateKeyPair",
                "iam:AddRoleToInstanceProfile",
```

```
                "iam:AddUserToGroup",
                "iam:AttachGroupPolicy",
                "iam:CreateAccessKey",
                "iam:CreateGroup",
                "iam:CreateInstanceProfile",
                "iam:CreateLoginProfile",
                "iam:CreateRole",
                "iam:CreateUser",
                "iam:Get*",
                "iam:List*",
                "iam:PutRolePolicy",
                "iam:UpdateAssumeRolePolicy"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

c. 選擇下一步：標籤。

d. (選擇性) 選擇 [新增標籤]，將索引鍵值配對與資源產生關聯。您最多可新增 50 個標籤。

> **Note**
>
> 標籤是您可以新增至資源的索引鍵值配對。這有助於識別、組織和搜尋資源。如需詳細資訊，請參閱《AWS 一般參考參考指南》中的標記AWS資源。

e. 選擇 下一步：檢閱。

f. 針對 Policy Name (政策名稱)，輸入 **`ServiceCatalogAdmin-AdditionalPermissions`**。

> **Important**
>
> 您必須授予管理員 Amazon S3 許可，才能AWS Service Catalog存取存放在 Amazon S3 中的範本。如需詳細資訊，請參閱 Amazon 簡單儲存服務使用者指南中的使用者政策範例。

g. 選擇建立政策。

5. 返回內有許可頁面的瀏覽器視窗，選擇 Refresh (重新整理)。

6. 在搜尋欄位中，輸入 **ServiceCatalog** 以篩選政策清單。
7. 選取**AWSServiceCatalogAdminFullAccess**和**ServiceCatalogAdmin-AdditionalPermissions**策略的核取方塊，然後選擇 [下一步：複查]。
8. 若是在更新使用者，請選擇 Add permissions (新增許可)。

   若是在建立使用者，請選擇 Create user (建立使用者)。可將登入資料下載或複製起來，再選擇 Close (關閉)。
9. 若要以目錄管理員身分登入，請使用帳戶專屬的 URL。若要尋找此 URL，請選擇導覽面板上的 Dashboard (儀表板)，並選擇 Copy Link (複製連結)。在瀏覽器中貼上連結，請使用在上述步驟中所建立或更新的 IAM 使用者的名稱和密碼。

將權限授予AWS Service Catalog最終用戶

您必須授予存取 AWS Service Catalog 最終使用者主控台檢視的權限，最終使用者才能使用 AWS Service Catalog。若要授與存取權，請將政策附加到使用者所使用的 IAM 使用者、群組或角色。在下列程序中，我們會將**AWSServiceCatalogEndUserFullAccess**政策附加至 IAM 群組。

將權限授予最終使用者群組

1. 開啟位於 https://console.aws.amazon.com/iam/ 的 IAM 主控台。
2. 在導覽窗格中，選擇 User groups (使用者群組)。
3. 選擇建立群組，然後執行下列動作：

   a. 在使用者群組名稱中，鍵入**Endusers**。

   b. 在搜尋欄位中，輸入 **AWSServiceCatalog** 以篩選政策清單。

   c. 選取**AWSServiceCatalogEndUserFullAccess**策略的核取方塊。您也可以改為選擇**AWSServiceCatalogEndUserReadOnlyAccess**。

   d. 選擇 Create Group (建立群組)。
4. 在導覽窗格中，選擇使用者 。
5. 選擇新增使用者，然後執行下列動作：

   a. 在 User name (使用者名稱) 中輸入使用者的名稱。

   b. 選取密碼-AWS 管理主控台存取權。

   c. 選擇 Next: Permissions (下一步：許可)。

   d. 選擇 將使用者新增至群組。

e. 選取 Endusers (最終使用者) 群組的核取方塊，然後依序選擇Next: Tags (下一步：標籤) 和 Next: Review (下一步：檢閱)。

f. 在 Review (檢閱) 頁面上，選擇 Create user (建立使用者)。下載或複製的登入資料，然後選擇 Close (關閉)。

安裝和設定 Terraform 佈建引擎

若要順利使用 Terraform 產品AWS Service Catalog，您必須在管理 Terraform 產品的同一帳戶中安裝並設定 Terraform 佈建引擎。若要開始使用，您可以使用提供的 Terraform 佈建引擎AWS，該引擎會安裝和設定 Terraform 佈建引擎所需的程式碼和基礎結構以使用。AWS Service Catalog一次性設定大約需要 30 分鐘。 AWS Service Catalog提供有關安裝和設定 Terraform 佈建引擎的指示的 GitHub 儲存庫。

佇列判定

當您呼叫佈建作業時，AWS Service Catalog準備有效負載訊息，以傳送至佈建引擎中的相關佇列。為了建立佇列的 ARN，請AWS Service Catalog進行下列假設：

- 佈建引擎位於產品擁有者的帳戶中
- 佈建引擎位於進行呼叫的相同區域 AWS Service Catalog
- 佈建引擎佇列遵循以下說明的命名結構描述

例如，如果使用帳戶 0000000000000 建立的產品`us-east-1`從帳戶 1111111111 呼叫，AWS Service Catalog則假設使用 ProvisionProduct 正確的 SQS ARN。`arn:aws:sqs:us-east-1:0000000000000:ServiceCatalogTerraformOSProvisionOperationQueue`

相同的邏輯適用於呼叫的 Lambda 函數`DescribeProvisioningParameters`。

將困惑的副手添加到您的 Terraform 配置引擎

混淆端點上的副上下文密鑰以限制**`lambda:Invoke`**操作的訪問

由AWS Service Catalog提供的引擎建立的參數剖析器 Lambda 函數具有存取政策，該政策僅授與AWS Service Catalog服務主體跨帳戶`lambda:Invoke`權限：

```
{
```

```
      "Version": "2012-10-17",
      "Statement": [
        {
          "Effect": "Allow",
          "Principal": {
            "Service": "servicecatalog.amazonaws.com"
          },
          "Action": "lambda:InvokeFunction",
          "Resource": "arn:aws:lambda:us-
east-1:account_id:function:ServiceCatalogTerraformOSParameterParser"
    }
  ]
}
```

這應該是唯一必要的權限，以便與AWS Service Catalog整合正常運作。但是，您可以使用「aws:SourceAccount混淆的副手」上下文鍵進一步限制此操作。AWS Service Catalog將訊息傳送至這些佇列時，會將佈建帳戶的 ID AWS Service Catalog 填入金鑰。當您打算透過產品組合共用來分發產品，並希望確保只有特定帳戶使用您的引擎時，這會很有幫助。

例如，您可以使用下列條件，將引擎限制為僅允許來自 000000000000 和 1111111111 的要求：

```
{
      "Version": "2012-10-17",
      "Statement": [
        {
          "Effect": "Allow",
          "Principal": {
            "Service": "servicecatalog.amazonaws.com"
          },
          "Action": "lambda:InvokeFunction",
          "Resource": "arn:aws:lambda:us-
east-1:account_id:function:ServiceCatalogTerraformOSParameterParser",
          "Condition": {
            "StringLike": {
              "aws:SourceAccount": ["000000000000", "111111111111"]
        }
      }
    }
  ]
}
```

混淆端點上的副上下文密鑰以限制sqs:SendMessage操作的訪問

由AWS Service Catalog提供的引擎建立的佈建作業導入 Amazon SQS 佇列具有存取政策，該政策僅授與跨帳戶 sqs:SendMessage (和關聯的 KMS) 許可給服務主體AWS Service Catalog：

```
{
      "Version": "2008-10-17",
      "Statement": [
        {
          "Sid": "Enable AWS Service Catalog to send messages to the queue",
          "Effect": "Allow",
          "Principal": {
            "Service": "servicecatalog.amazonaws.com"
          },
          "Action": "sqs:SendMessage",
          "Resource": [
            "arn:aws:sqs:us-
east-1:account_id:ServiceCatalogTerraformOSProvisionOperationQueue"
          ]
        },
        {
          "Sid": "Enable AWS Service Catalog encryption/decryption permissions when
 sending message to queue",
          "Effect": "Allow",
          "Principal": {
            "Service": "servicecatalog.amazonaws.com"
          },
          "Action": [
            "kms:DescribeKey",
            "kms:Decrypt",
            "kms:ReEncrypt",
            "kms:GenerateDataKey"
          ],
          "Resource": "arn:aws:kms:us-east-1:account_id:key/key_id"
    }
  ]
}
```

這應該是唯一必要的權限，以便與AWS Service Catalog整合正常運作。但是，您可以使用「aws:SourceAccount混淆的副手」上下文鍵進一步限制此操作。AWS Service Catalog將訊息傳送至這些佇列時，請使用佈建帳戶的 ID AWS Service Catalog 填入金鑰。當您打算透過產品組合共用來分發產品，並希望確保只有特定帳戶使用您的引擎時，這會很有幫助。

例如，您可以使用下列條件，將引擎限制為僅允許來自 000000000000 和 1111111111 的要求：

```
{
      "Version": "2008-10-17",
      "Statement": [
      {
        "Sid": "Enable AWS Service Catalog to send messages to the queue",
        "Effect": "Allow",
        "Principal": {
          "Service": "servicecatalog.amazonaws.com"
        },
        "Action": "sqs:SendMessage",
        "Resource": [
          "arn:aws:sqs:us-
east-1:account_id:ServiceCatalogTerraformOSProvisionOperationQueue"
        ],
        "Condition": {
          "StringLike": {
            "aws:SourceAccount": ["000000000000", "111111111111"]
          }
        }
      },
      {
        "Sid": "Enable AWS Service Catalog encryption/decryption permissions when
 sending message to queue",
        "Effect": "Allow",
        "Principal": {
          "Service": "servicecatalog.amazonaws.com"
        },
        "Action": [
          "kms:DescribeKey",
          "kms:Decrypt",
          "kms:ReEncrypt",
          "kms:GenerateDataKey"
        ],
        "Resource": "arn:aws:kms:us-east-1:account_id:key/key_id"
    }
  ]
}
```

開始

您可以使用入門程AWS Service Catalog式庫中架構良好的產品範本，或遵循其中一個入門自學課程中的步驟來開始使用。

在自學課程中，您會以目錄管理員和一般使用者的身分執行工作。身為目錄管理員，您可以建立學檔，然後建立產品。身為一般使用者，您確認可以存取一般使用者主控台並啟動產品。該產品是以下之一：

- 在 Amazon Linux 上執行的雲端開發環境，是以定義產品可使用之AWS資源的AWS CloudFormation範本為基礎。
- 在 Terraform 佈建引擎上執行的開放原始碼環境，並以 tar.gz 組態檔為基礎，該檔案定義了產品可使用的AWS資源。

> **Note**
>
> 在開始之前，請確保您已完成中的事務處理設定 AWS Service Catalog。

主題

入門資源庫

AWS Service Catalog 提供 Well-Architected 產品範本的入門資源庫，可讓您快速開始著手。您可以將入門資源庫產品組合中的任何產品複製到您自己的帳戶中，然後根據您的需求進行自訂。

主題

必要條件

在使用我們的入門資源庫中的範本之前，請確定您擁有下列項目：

- 使用 AWS CloudFormation 範本所需的許可。如需詳細資訊，請參閱使用 AWS Identity and Access Management 控制存取。
- 管理 AWS Service Catalog 所需的管理員許可。如需詳細資訊，請參閱 the section called “身分和存取權管理”。

進一步了解

如需 Well-Architected 架構的詳細資訊，請參閱AWS架構良好。

開始使用AWS CloudFormation產品

您可以使用入門程AWS Service Catalog式庫中其中一個架構良好的產品範本，或遵循入門教學課程中的步驟來開始使用。

在自學課程中，您會以目錄管理員和一般使用者的身分執行工作。身為目錄管理員，您可以建立 Porfolio，然後建立產品。身為一般使用者，您確認可以存取一般使用者主控台並啟動產品。該產品是在 Amazon Linux 上執行的雲端開發環境，並以定義產品可使用的AWS資源的AWS CloudFormation範本為基礎。

> **Note**
>
> 在開始之前，請確保您已完成中的事務處理設定 AWS Service Catalog。

主題

- 步驟 1：下載AWS CloudFormation範本
- 步驟 2：建立金鑰對
- 步驟 3：建立投資組合
- 步驟 4：在產品組合中建立新產品
- 步驟 5：新增範本約束以限制執行個體大小
- 步驟 6：新增啟動限制以指派 IAM 角色
- 步驟 7：將產品組合的存取權授予使用者
- 步驟 8：測試使用者體驗

步驟 1：下載AWS CloudFormation範本

您可以使用AWS CloudFormation範本來設定和佈建產品組合和產品。這些範本是可以使用 JSON 或 YAML 格式化的文字檔案，並說明您要佈建的資源。如需詳細資訊，請參閱 https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/template-formats.html 使用者指南中的AWS CloudFormation範本格式。您可以使用編AWS CloudFormation輯器或您選擇的文字編輯器來建立和儲存範本。在本教程中，我們提供了一個簡單的模板，因此您可以開始使用。範本會啟動針對安全殼層存取設定的單一 Linux 執行個體。

> **Note**
>
> 使用AWS CloudFormation範本需要特殊權限。開始之前，請確定您擁有正確的權限。如需詳細資訊，請參閱中的先決條件入門資源庫。

範本下載

本教學課程所提供的範例範本可在 https://awsdocs.s3.amazonaws.com/servicecatalog/development-environment.template 取得。`development-environment.template`

範本概觀

範例範本的文字如下所示：

```
{
  "AWSTemplateFormatVersion" : "2010-09-09",

  "Description" : "AWS Service Catalog sample template. Creates an Amazon EC2 instance
                   running the Amazon Linux AMI. The AMI is chosen based on the
 region
                   in which the stack is run. This example creates an EC2 security
                   group for the instance to give you SSH access. **WARNING** This
                   template creates an Amazon EC2 instance. You will be billed for
 the
                   AWS resources used if you create a stack from this template.",

  "Parameters" : {
    "KeyName": {
      "Description" : "Name of an existing EC2 key pair for SSH access to the EC2
 instance.",
      "Type": "AWS::EC2::KeyPair::KeyName"
```

```
    },

    "InstanceType" : {
      "Description" : "EC2 instance type.",
      "Type" : "String",
      "Default" : "t2.micro",
      "AllowedValues" : [ "t2.micro", "t2.small", "t2.medium", "m3.medium",
"m3.large",
        "m3.xlarge", "m3.2xlarge" ]
    },

    "SSHLocation" : {
      "Description" : "The IP address range that can SSH to the EC2 instance.",
      "Type": "String",
      "MinLength": "9",
      "MaxLength": "18",
      "Default": "0.0.0.0/0",
      "AllowedPattern": "(\\d{1,3})\\.(\\d{1,3})\\.(\\d{1,3})\\.(\\d{1,3})/(\\d{1,2})",
      "ConstraintDescription": "Must be a valid IP CIDR range of the form x.x.x.x/x."
   }
  },

  "Metadata" : {
    "AWS::CloudFormation::Interface" : {
      "ParameterGroups" : [{
        "Label" : {"default": "Instance configuration"},
        "Parameters" : ["InstanceType"]
      },{
        "Label" : {"default": "Security configuration"},
        "Parameters" : ["KeyName", "SSHLocation"]
      }],
      "ParameterLabels" : {
        "InstanceType": {"default": "Server size:"},
        "KeyName": {"default": "Key pair:"},
        "SSHLocation": {"default": "CIDR range:"}
      }
    }
  },

  "Mappings" : {
    "AWSRegionArch2AMI" : {
      "us-east-1"      : { "HVM64" : "ami-08842d60" },
      "us-west-2"      : { "HVM64" : "ami-8786c6b7" },
      "us-west-1"      : { "HVM64" : "ami-cfa8a18a" },
```

```
      "eu-west-1"      : { "HVM64" : "ami-748e2903" },
      "ap-southeast-1" : { "HVM64" : "ami-d6e1c584" },
      "ap-northeast-1" : { "HVM64" : "ami-35072834" },
      "ap-southeast-2" : { "HVM64" : "ami-fd4724c7" },
      "sa-east-1"      : { "HVM64" : "ami-956cc688" },
      "cn-north-1"     : { "HVM64" : "ami-ac57c595" },
      "eu-central-1"   : { "HVM64" : "ami-b43503a9" }
    }

  },

  "Resources" : {
    "EC2Instance" : {
      "Type" : "AWS::EC2::Instance",
      "Properties" : {
        "InstanceType" : { "Ref" : "InstanceType" },
        "SecurityGroups" : [ { "Ref" : "InstanceSecurityGroup" } ],
        "KeyName" : { "Ref" : "KeyName" },
        "ImageId" : { "Fn::FindInMap" : [ "AWSRegionArch2AMI", { "Ref" :
"AWS::Region" }, "HVM64" ] }
      }
    },

    "InstanceSecurityGroup" : {
      "Type" : "AWS::EC2::SecurityGroup",
      "Properties" : {
        "GroupDescription" : "Enable SSH access via port 22",
        "SecurityGroupIngress" : [ {
          "IpProtocol" : "tcp",
          "FromPort" : "22",
          "ToPort" : "22",
          "CidrIp" : { "Ref" : "SSHLocation"}
        } ]
      }
    }
  },

  "Outputs" : {
    "PublicDNSName" : {
      "Description" : "Public DNS name of the new EC2 instance",
      "Value" : { "Fn::GetAtt" : [ "EC2Instance", "PublicDnsName" ] }
    },
    "PublicIPAddress" : {
      "Description" : "Public IP address of the new EC2 instance",
```

```
      "Value" : { "Fn::GetAtt" : [ "EC2Instance", "PublicIp" ] }
    }
  }
}
```

範本資源

當產品啟動時，範本宣告要建立的資源。它由下列各部分組成：

- AWSTemplateFormatVersion(選用)-用來建立此AWS範本的「範本格式」版本。最新的模板格式版本是 2010 年 9 月 09 日，是目前唯一有效的值。
- 說明 (選擇性) — 範本的描述。
- 參數 (選用) — 您的使用者必須指定才能啟動產品的參數。範本包含每個參數的描述和限制，輸入的值必須符合這些限制。如需限制條件的詳細資訊，請參閱 使用 AWS Service Catalog 限制。

  此KeyName參數可讓您指定 Amazon Elastic Compute Cloud (Amazon EC2) key pair 名稱，最終使用AWS Service Catalog者在啟動產品時必須提供這個名稱。您將在下一個步驟中建立金鑰對。
- 中繼資料 (選用) — 提供有關範本其他資訊的物件。:: AWSCloudFormation: 介面鍵定義一般使用者主控台檢視如何顯示參數。`ParameterGroups` 屬性定義這些參數如何分組以及為這些群組加上標題。`ParameterLabels` 屬性定義容易記住的參數名稱。當使用者指定參數以啟動以此範本為基礎的產品時，最終使用者主控台檢視將在標題 `Server size:` 之下顯示標記為 `Instance configuration` 的參數，它在標題 `Key pair:` 之下顯示標記為 `CIDR range:` 及 `Security configuration` 的參數。
- 對應 (選用) — 索引鍵與關聯值的對映，可用來指定條件參數值，類似於查閱表。您可以使用「資源」和「輸出」區段中的 Fn:: FindInMap 內建函數來比對索引鍵與對應的值。上面的範本包括AWS區域清單和對應於每個區域的 Amazon 機器映像 (AMI)。 AWS Service Catalog根據使用者在中選取的AWS區域，使用此對應來決定要使用的 AMI AWS Management Console。
- 資源 (必要) — 堆疊資源及其屬性。您可以參考範本 [資源] 和 [輸出] 區段中的資源。在上述範本中，我們指定執行 Amazon Linux 的 EC2 執行個體，以及允許 SSH 存取執行個體的安全群組。EC2 執行個體資源的 [屬性] 區段會使用使用者輸入的資訊來設定執行個體類型和 SSH 存取的金鑰名稱。

  AWS CloudFormation使用目前的AWS區域從先前定義的對應中選取 AMI ID，並為其指派安全性群組。安全群組經過設定以允許從使用者指定的 CIDR IP 地址範圍對內存取連接埠 22。
- 輸出 (選用) — 告知使用者何時完成產品啟動的文字。提供的範本取得啟動執行個體的公有 DNS 名稱並顯示給使用者。使用者需要 DNS 名稱以使用 SSH 連接到執行個體。

如需有關「範本剖析」頁面的詳細資訊，請參閱AWS CloudFormation使用指南中的範本參考。

步驟 2：建立金鑰對

若要讓最終使用者能夠根據本教學的範例範本啟動產品，您必須建立 Amazon EC2 key pair。金鑰對是公開金鑰的結合，這些金鑰用於加密資料，私有金鑰則用於解密資料。如需有關金鑰配對的詳細資訊，請確保您已登入AWS主控台，然後參閱 Amazon EC2 Linux 執行個體使用者指南中的 Amazon EC2 金鑰配對。

本教學課程的 AWS CloudFormation 範本，`development-environment.template`，包括 `KeyName` 參數：

```
. . .
  "Parameters" : {
    "KeyName": {
      "Description" : "Name of an existing EC2 key pair for SSH access to the EC2
 instance.",
      "Type": "AWS::EC2::KeyPair::KeyName"
    },
. . .
```

最終使用者在使用 AWS Service Catalog 啟動以範本為基礎的產品時，必須指定金鑰對的名稱。

如果您已在偏好使用的帳戶中建立金鑰對，您可以跳至 步驟 3：建立投資組合。否則，請完成下列步驟。

建立一組金鑰對

1. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 請在導覽窗格的 Network & Security (網路與安全性) 下方，選擇 Key Pairs (金鑰對)。
3. 在 Key Pairs (金鑰對) 頁面上，選擇 Create Key Pair (建立金鑰對)。
4. 在 Key pair name (金鑰對名稱) 中輸入容易記住的名稱，然後選擇 Create (建立)。
5. 當主控台提示您儲存私有金鑰檔案時，將它儲存在安全的地方。

> **Important**
>
> 這是您儲存私有金鑰檔案的唯一機會。

步驟 3：建立投資組合

若要將產品提供給使用者，請從建立這些產品的產品組合開始。

建立產品組合

1. 在 https://console.aws.amazon.com/servicecatalog/ 開啟 Service Catalog 主控台。
2. 在左側導覽面板中，選擇學檔，然後選擇 [建立學檔]。
3. 輸入下列值：
   - 產品組合名 – **Engineering Tools**
   - 投資組合說明-**Sample portfolio that contains a single product.**
   - 擁有者 — **IT (it@example.com)**
4. 選擇建立。

步驟 4：在產品組合中建立新產品

創建投資組合後，您就可以在投資組合中創建產品。在本教學課程中，您將在工程工具組合內建立名為 Linux 桌面的產品，這是一個在 Amazon Linux 上執行的雲端開發環境。

若要在產品組合中建立產品

1. 若剛完成前一步驟，則已會顯示出 Portfolios (產品組合) 頁面。否則，請打開 https://console.aws.amazon.com/servicecatalog/。
2. 選擇並開啟您在步驟 2 中建立的工程工具組合。
3. 選擇上傳新產品。
4. 在「產品詳細資訊」區段的「建立產品」頁面上，輸入下列資訊：
   - Product name (產品名稱) – **Linux Desktop**
   - 產品描述 — **Cloud development environment configured for engineering staff. Runs AWS Linux.**
   - 擁有者 — **IT**
   - 分銷商 — (空白)
5. 在 [版本詳細資料] 頁面上，選擇 [使用 CloudFormation 範本]。然後選擇「指定 Amazon S3 範本 URL」，然後輸入以下內容：

- Select template (選擇範本) – **https://awsdocs.s3.amazonaws.com/servicecatalog/development-environment.template**
- 版本標題 — **v1.0**
- Description (描述) - **Base Version**

6. 在「Sup port 詳細資料」區段中，輸入下列資訊：

   - 電子郵件聯繫 — **ITSupport@example.com**
   - S@@ upport 鏈接-**https://wiki.example.com/IT/support**
   - S@@ upport 說明-**Contact the IT department for issues deploying or connecting to this product.**

7. 選擇「建立產品」。

步驟 5：新增範本約束以限制執行個體大小

限制在產品組合層級新增另一層產品控制。限制可以控制產品的啟動細節 (啟動限制) 或將規則新增至 AWS CloudFormation 範本 (範本限制條件)。如需詳細資訊，請參閱 使用 AWS Service Catalog 限制。

將範本限制新增至 Linux 桌面平台產品，以防止使用者在啟動時選取大型執行個體類型。開發環境範本可讓使用者選擇六種執行個體類型；此限制會將有效的執行個體類型限制為兩個最小的類型 `t2.micro` 和 `t2.small`。如需詳細資訊，請參閱 Amazon EC2 Linux 執行個體使用者指南中的 T2 執行個體。

若要將範本限制新增至 Linux 桌面平台產品

1. 在學檔詳細資訊頁面上，選擇限制條件，然後選擇建立限制條件。
2. 在「建立限制條件」頁面中，針對「產品」選擇「Linux 桌面」。然後，針對「條件約束」類型選擇「範本」
3. 在 [T 字面版面限制] 區段中，選擇 [文字編輯器]。
4. 將以下內容貼到文字編輯器中：

```
{
  "Rules": {
    "Rule1": {
      "Assertions": [
        {
```

```
          "Assert" : {"Fn::Contains": [["t2.micro", "t2.small"], {"Ref":
 "InstanceType"}]},
          "AssertDescription": "Instance type should be t2.micro or t2.small"
        }
      ]
    }
  }
}
```

5. 針對「限制」說明，輸入**`Small instance sizes`**。
6. 選擇建立。

步驟 6：新增啟動限制以指派 IAM 角色

啟動限制會指定 IAM 角色，該角色會在最終使用者啟動產品時AWS Service Catalog採用。

在此步驟中，您可以將啟動限制新增至 Linux 桌面產品，AWS Service Catalog以便使用構成產品AWS CloudFormation範本的 IAM 資源。

您指派給產品做為啟動限制的 IAM 角色必須具有下列權限

1. AWS CloudFormation
2. 產品AWS CloudFormation範本中的服務
3. 讀取服務擁有的 Amazon S3 儲存貯體中AWS CloudFormation範本的存取權限。

此啟動限制可讓一般使用者啟動產品，並在啟動後將其作為已佈建產品進行管理。如需詳細資訊，請參閱 AWS Service Catalog 啟動限制。

如果沒有啟動限制，您必須先向使用者授與其他 IAM 許可，才能使用 Linux 桌面平台產品。例如，該`ServiceCatalogEndUserAccess`政策授予存取使用者主控台檢視所需的AWS Service Catalog最低 IAM 許可。

使用啟動限制可讓您遵循將最終使用者 IAM 許可保持在最低限度的 IAM 最佳做法。如需詳細資訊，請參閱《IAM 使用者指南》中的授予最低權限。

新增啟動限制

1. 遵循 IAM 使用者指南中的 JSON 索引標籤上建立新政策的指示。
2. 貼上下列 JSON 政策文件：

- `cloudformation`— 允許創建，讀取，更新，刪除，列出和標籤AWS CloudFormation堆棧的AWS Service Catalog完整權限。
- `ec2`— 允許AWS Service Catalog完整許可列出、讀取、寫入、佈建和標記屬於AWS Service Catalog產品一部分的 Amazon 彈性運算雲端 (Amazon EC2) 資源。根據您要部署的AWS資源，此權限可能會變更。
- `ec2`— 為您的AWS帳戶建立新的受管政策，並將指定的受管政策附加到指定的 IAM 角色。
- `s3`— 允許存取擁有的 Amazon S3 儲存貯體AWS Service Catalog。若要部署產品，AWS Service Catalog需要存取佈建人工因素。
- `servicecatalog`— 允AWS Service Catalog許代表使用者列出、讀取、寫入、標記和啟動資源的權限。
- `sns`— 允AWS Service Catalog許列出、讀取、寫入和標記啟動限制的 Amazon SNS 主題。

> **Note**
>
> 視您要部署的基礎資源而定，您可能需要修改範例 JSON 政策。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStackEvents",
                "cloudformation:DescribeStacks",
                "cloudformation:GetTemplateSummary",
                "cloudformation:SetStackPolicy",
                "cloudformation:ValidateTemplate",
                "cloudformation:UpdateStack",
                "ec2:*",
                "servicecatalog:*",
                "sns:*"
            ],
            "Resource": "*"
        },
```

```
        {
         "Effect":"Allow",
         "Action":[
            "s3:GetObject"
         ],
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "s3:ExistingObjectTag/servicecatalog:provisioning":"true"
            }
         }
      }
   ]
}
```

3. 選擇下一步、標籤。
4. 選擇下一步，檢閱。
5. 在 [檢閱原則] 頁面中，針對 [名稱] 輸入**linuxDesktopPolicy**。
6. 選擇建立政策。
7. 在導覽窗格中，選擇角色。然後選擇 [建立角色] 並執行下列動作：
   a. 針對 [選取信任的實體]，選擇 [AWS服務]，然後在 [其他AWS服務的使用案例] 下選擇 Service Catalog 選取 Service Catalog 使用案例，然後選擇下一步。
   b. 搜尋linuxDesktopPolicy策略，然後選取核取方塊。
   c. 選擇下一步。
   d. 於角色名稱輸入 **linuxDesktopLaunchRole**。
   e. 選擇建立角色。
8. 開啟主AWS Service Catalog控台，網址為 https://console.aws.amazon.com/servicecatalog。
9. 選擇 Engineering Tools (工程工具) 產品組合。
10. 在學檔詳細資訊頁面上，選擇「條件約束」標籤，然後選擇「建立條件約束」。
11. 對於「產品」，請選擇 Linux 桌面平台，然後針對「條件約束類型」選擇「
12. 選擇選取 IAM 角色。接下來選擇 [linuxDesktopLaunch角色]，然後選擇 [建立]。

步驟 7：將產品組合的存取權授予使用者

現在您已建立產品組合並新增產品，可以將存取權授予最終使用者。

必要條件

如果尚未為終端使用者建立 IAM 群組，請參閱將權限授予AWS Service Catalog最終用戶。

提供存取產品組合

1. 在學檔詳細資訊頁面上，選擇「存取權」標籤。
2. 選擇 Grant access (授與存取權)。
3. 在群組索引標籤上，選取最終使用者 IAM 群組的核取方塊。
4. 選擇新增存取權限。

步驟 8：測試使用者體驗

若要確認使用者是否能成功存取一般使用者主控台檢視並啟動您的產品，請以使用者AWS身分登入並執行這些工作。

若要驗證最終使用者是否能存取最終使用者主控台

1. 遵循 IAM 使用者指南中的指示以 IAM 使用者身分登入。
2. 在選單列中，選擇您在其中建立學`Engineering Tools`檔的「AWS區域」。在此自學課程中，請選擇 us-east- 1 區域。
3. 在 https://console.aws.amazon.com/servicecatalog/ 打開AWS Service Catalog控制台以查看以下內容：

   - 產品 – 使用者可以使用的產品。
   - 佈建的產品 – 使用者已啟動的佈建產品。

確認使用者是否可以啟動 Linux 桌面平台產品

請注意，在本教學課程中，請選擇 us-east- 1 區域。

1. 在主控台的「產品」區段中，選擇「Linux 桌面平台」。
2. 選擇 [啟動產品] 以啟動設定產品的精靈。
3. 在「啟動：Linux 桌面平台」頁面上，輸入**`Linux-Desktop`**已佈建的產品名稱。
4. 在「參數」頁面上，輸入下列項目並選擇「下一步」：

   - 伺服器大小 — 選擇**`t2.micro`**。

- 金鑰對 – 選取您在 步驟 2：建立金鑰對 中建立的金鑰對。
- CIDR 範圍 — 輸入 IP 位址的有效 CIDR 範圍，以連線至執行個體。您可以使用默認值（0.0.0.0/0）允許從任何 IP 地址訪問，然後是您的 IP 地址，然後限制對您的 IP 地址的訪問，或者在兩者之間的訪問。**/32**

5. 選擇「啟動產品」以啟動堆疊。主控台會顯示適用於 Linux-Desktop 堆疊的堆疊詳細資訊頁面。產品的初始狀態為 「變更中」。此需要幾分鐘的時間讓 AWS Service Catalog 啟動產品。若要查看目前狀態，請重新整理瀏覽器。產品啟動後，狀態為 A 有效。

開始使用地形產品

AWS Service Catalog透過內部 HashiCorp Terraform 組態的控管功能，實現快速、自助式佈建。AWS您可以AWS Service Catalog作為單一工具使用，在其中大規模組織、控管和散佈 Terraform 組態。AWS AWS Service Catalog支援 Terraform 多項關鍵功能，包括編目標準化和預先核准的 Terraform 範本、存取控制、版本控制、標記，以及與其他帳戶共用。AWS在中AWS Service Catalog，您的使用者會看到他們有權存取的產品和版本的簡單清單，然後只要一個動作即可部署這些產品。

> **Note**
>
> 為了繼續支持 HashiCorp 技術，由於最近對 Terraform 的許可更AWS Service Catalog改，將 T erraform 開源的任何先前引用更改為外部。外部產品類型包括對地形社區版的支持，以前稱為 Terraform 開源。如需有關將現有 Terraform 開放原始碼產品和佈建產品移轉至外部產品類型的詳細資訊和指示，請參閱。將現有的 Terraform 開放原始碼產品和佈建的產品更新為外部產品類型

下列教學課程中的步驟將協助您開始使用中的 Terraform 產品。AWS Service Catalog

身為目錄管理員，您可以使用中央系統管理員帳戶 (Hub 帳戶)。Terrafrm 社群版和 Terraform 雲端產品都需要 Terraform 佈建引擎，您可以在和中瞭解更多相關資訊。Terraform 社群版的佈建引擎 (外部產品類型) 地形雲端的佈建引擎

在教學課程期間，您會在系統管理員帳戶中執行下列工作：

- 使用地形雲端或外部產品類型建立地形產品。Service Catalog 使用外部產品類型來支援 Terraform 社群版產品。
- 將產品與產品組合相關聯

- 建立啟動限制以允許您的使用者佈建產品
- 標記產品
- 與最終用戶帳戶共享產品組合和 Terraform 產品（支點帳戶）

在教學課程中，您可以使用 admin Hub 帳戶 (也是組織的管理帳戶) 中的組織共用選項來共用學檔。如需組織共用的詳細資訊，請參閱共用產品組合。

您在教學中建立的 Terraform 產品中包含的AWS資源是一個簡單的 Amazon S3 儲存貯體。

> **Note**
>
> 在開始之前，請确保您已完成中的事務處理設定 AWS Service Catalog。

主題

將現有的 Terraform 開放原始碼產品和佈建的產品更新為外部產品類型

為了繼續支持 HashiCorp 技術，由於最近對 Terraform 的許可更AWS Service Catalog改，將 Terraform 開源的任何先前引用更改為外部。外部產品類型包括對地形社區版的支持，以前稱為地形開源。 AWS Service Catalog不再支援 Terraform 開放原始碼作為任何新產品或佈建產品的有效產品類型。您只能更新或終止現有的 Terraform 開放原始碼資源，包括產品版本和佈建的產品。

如果您尚未這麼做，您必須依照本節中的指示，將所有現有的 Terraform 開放原始碼產品和佈建的產品轉換至外部產品。

1. 更新您現有的 Terraform 參考引擎，AWS Service Catalog以包含對外部和 Terraform 開放原始碼產品類型的支援。如需更新 Terraform 參考引擎的相關指示，請參閱我們GitHub 的儲存庫。
2. 使用新的外部產品類型，重新建立任何現有的 Terraform 開放原始碼產品。
3. 刪除任何使用 Terraform 開放原始碼產品類型的現有產品。
4. 重新佈建剩餘的資源以使用新的外部產品類型。
5. 終止任何使用 Terraform 開放原始碼產品類型的現有佈建產品。

轉換現有產品之後，請針對任何使用 tar.gz 組態檔的新產品使用「外部」產品類型。

AWS Service Catalog將根據需要通過此更改為客戶提供支持。如果這些變更需要為您的帳戶進行大量工作，或影響重要的產品工作負載，請聯絡您的客戶代表以請求協助。

先決條件：設定您的 Terraform 佈建引擎

在中建立 Terraform 產品的先決條件AWS Service Catalog，您必須在 Service Catalog 管理員帳戶 (Hub 帳戶) 中安裝並設定佈建引擎。Terraform 社群版產品 (使用外部產品類型) 和 Terraform 雲端產品 (使用 Terraform 雲端產品類型) 都需要佈建引擎。

> **Note**
>
> 引擎組態是一次性設定，大約需要 30 分鐘。

Terraform 社群版的佈建引擎 (外部產品類型)

AWS Service Catalog使用外部產品類型來支援 Terraform 社群版產品。外部產品類型也支援其他佈建工具，包括 Plumi、Ansible、Chef 等，以佈建引擎的組態為基礎。

對於AWS Service Catalog使用具有 Terraform 社群版本 HashiCorp的外部產品類型的產品，您必須在 AWS Service Catalog管理員帳戶 (Hub 帳戶) 中安裝並設定 Terraform 佈建引擎。 AWS管理此引擎及其資源。

AWS Service Catalog提供有關安裝和配置提供的 Terraform 佈建引擎的說AWS明的 GitHub 儲存庫。軟件庫包括以下信息：

- 所需的安裝工具

- 建立程式碼
- 部署到帳AWS戶
- 有關佈建工作流程、品質保證和限制的其他資訊

地形雲端的佈建引擎

對於AWS Service Catalog使用 Terraform 雲端產品類型與 Terraform 雲端 HashiCorp的產品，您必須在AWS Service Catalog管理員帳戶 (Hub 帳戶) 中安裝並設定 Terraform 佈建引擎。 HashiCorp 在遠程環境中管理此引擎。

HashiCorp 提供一個 GitHub 儲存庫，其中包含設定的 Terraform 雲端引擎的指示。AWS Service Catalog軟件庫包括以下信息：

- 所需的安裝工具
- 建立程式碼
- 部署到帳AWS戶
- 有關佈建工作流程、品質保證和限制的其他資訊

步驟 1：地形表單配置文件下載

您可以使用 Terraform 組態檔案來建立和佈建 HashiCorp Terraform 產品。這些組態為純文字檔案，描述您要佈建的資源。您可以使用您選擇的文字編輯器來建立、更新和儲存規劃。若要建立產品，您必須將地形組態上傳為 tar.gz 檔案。在此自學課程中，AWS Service Catalog提供簡單的組態檔案，以便您可以開始使用。該組態會建立一個 Amazon S3 儲存貯體。

配置文件下載

AWS Service Catalog提供範例simple-s3-bucket.tar.gz規劃檔供您在此自學課程中使用。

組態檔案概觀

範例組態檔案的文字如下：

```
variable "bucket_name" {
  type = string
}
provider "aws" {
}
```

```
resource "aws_s3_bucket" "bucket" {
  bucket = var.bucket_name
}
output regional_domain_name {
  value = aws_s3_bucket.bucket.bucket_regional_domain_name
}
```

組態資源

配置檔案會在AWS Service Catalog佈建產品時宣告要建立的資源。它由下列各部分組成：

- 變數 (選用) — 系統管理員使用者 (Hub 帳戶管理員) 可以指派來自訂組態的值定義。變數提供一致的介面來變更指定組態的行為方式。變數關鍵字之後的標籤是變數的名稱，該名稱在同一個模組中的所有變數中必須是唯一的。此名稱用於將外部值分配給變量，並從模塊內引用變量的值。
- 提供者 (選用) — 用於資源佈建的雲端服務提供者，也就是說AWS。 AWS Service Catalog僅支持AWS作為提供者。因此，Terraform 佈建引擎會覆寫任何其他列出的提供者。AWS
- 資源 (必要) — 用於佈建的AWS基礎結構資源。在本教學課程中，地形表單組態檔案會指定 Amazon S3。
- 輸出 (選用) — 傳回的資訊或值，類似於程式設計語言中的傳回值。您可以使用輸出資料，透過自動化工具配置基礎架構工作流程

步驟 2：建立地形產品

安裝 Terraform 佈建引擎之後，您就可以在中建立 HashiCorp Terraform 產品。AWS Service Catalog 在本教學中，您會建立包含簡單 Amazon S3 儲存貯體的 Terraform 產品。

建立地形產品

1. 在 https://console.aws.amazon.com/servicecatalog/ 開啟AWS Service Catalog主控台，然後以管理員使用者身分登入。
2. 瀏覽至 [管理] 區段，然後選擇 [產品清單]。
3. 選擇「建立產品」。
4. 在「產品詳細資料」區段的「建立產品」頁面上，選擇「外部」或「Terraform Cloud」產品類型。Service Catalog 使用外部產品類型來支援 Terraform 社群版產品。
5. 輸入下列產品詳細資訊：
   - Product name (產品名稱) – **`Simple S3 bucket`**

- 產品描述 — 包含 Amazon S3 存儲桶的地形產品。
- 擁有者 — **IT**
- 分銷商 — (空白)

6. 在 [版本詳細資料] 窗格中，選擇 [上傳範本檔案]，然後選擇 [選擇檔案]。選取您在其中下載的檔案步驟 1：地形表單配置文件下載。
7. 輸入下列資料：

   - 版本名稱 — **v1.0**
   - 版本說明 — **Base Version**

8. 在「Sup port 詳細資料」區段中，輸入下列項目，然後選擇「建立產品」。

   - 電子郵件聯繫 — **ITSupport@example.com**
   - S@@ upport 鏈接-**https://wiki.example.com/IT/support**
   - S@@ upport 說明-**Contact the IT department for issues deploying or connecting to this product.**

9. 選擇「建立產品」。

成功建立產品後，AWS Service Catalog會在產品頁面上顯示確認橫幅。

步驟 3：建立AWS Service Catalog投資組合

您可以在AWS Service Catalog管理員帳戶 (Hub 帳戶) 中建立產品組合，以便輕鬆組織產品，並將產品分發到一般使用者帳戶 (支點帳戶)。

建立產品組合

1. 在 https://console.aws.amazon.com/servicecatalog/ 開啟AWS Service Catalog主控台，然後以系統管理員身分登入。
2. 在左側導覽面板中，選擇學檔，然後選擇 [建立學檔]。
3. 輸入下列值：

   - 產品組合名 – **S3 bucket**
   - 投資組合說明-**Sample portfolio for Terraform configurations.**
   - 擁有者 — **IT (it@example.com)**

4. 選擇建立。

第 4 步：將產品添加到產品組合

建立產品組合後，您可以新增您在步驟 2 中建立的 HashiCorp Terraform 產品。

若要將產品新增至產品組合

1. 導覽至「產品清單」頁面。
2. 選取您在步驟 2 中建立的簡易 S3 儲存貯體 Terraform 產品，然後選擇 [動作]。從下拉式選單中，選擇「新增產品至產品組合」。 AWS Service Catalog顯示新增簡單 S3 儲存貯體至產品組合窗格。
3. 選取 S3 儲存貯體組合，然後關閉建立啟動限制。您將在稍後的自學課程中建立啟動約束。
4. 選擇新增產品至產品組合。

成功將產品新增至產品組合後，AWS Service Catalog會在「產品清單」頁面上顯示確認橫幅。

步驟 5：建立啟動角色

在此步驟中，您將建立 IAM 角色 (啟動角色)，指定 Terraform 佈建引擎的權限，並在使用者啟動 Terraform 產品時AWS Service Catalog可承擔的 HashiCorp 權限。

稍後指派給簡單 Amazon S3 儲存貯體 Terraform 產品做為啟動限制的 IAM 角色 (啟動角色) 必須具有下列許可：

- 存取您的 Terraform 產品的基礎AWS資源。在本教學課程中，這包括對`s3:CreateBucket*`、`s3:DeleteBucket*`s3:Get*s3:List*、和 `s3:PutBucketTagging` Amazon S3 操作的存取。
- 讀取AWS Service Catalog擁有的 Amazon S3 儲存貯體中 Amazon S3 範本的存取權
- 存取`CreateGroup`、`ListGroupResources`、`DeleteGroup`、和`Tag`資源群組作業。這些作業 AWS Service Catalog可用來管理資源群組和標記

若要在AWS Service Catalog系統管理員帳戶中建立啟動角色

1. 登入AWS Service Catalog管理員帳戶後，請遵循 IAM 使用者指南中「在 JSON」索引標籤上建立新政策的指示。
2. 為您的簡單 Amazon S3 儲存貯體 Terraform 產品建立政策。在您建立啟動角色之前，必須先建立此原則，並包含下列權限：

- `s3`— 允許AWS Service Catalog列出、讀取、寫入、佈建和標記 Amazon S3 產品的完整許可。
- `s3`— 允許存取擁有的 Amazon S3 儲存貯體AWS Service Catalog。若要部署產品，AWS Service Catalog需要存取佈建人工因素。
- `resourcegroups`— 允AWS Service Catalog許創建，列出，刪除和標記AWS Resource Groups。
- `tag`— 允許AWS Service Catalog標記權限。

> **Note**
>
> 根據您要部署的基礎資源，您可能需要修改範例 JSON 政策。

貼上下列 JSON 政策文件：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "s3:GetObject",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "s3:ExistingObjectTag/servicecatalog:provisioning": "true"
                }
            }
        },
        {
            "Action": [
                "s3:CreateBucket*",
                "s3:DeleteBucket*",
                "s3:Get*",
                "s3:List*",
                "s3:PutBucketTagging"
            ],
            "Resource": "arn:aws:s3:::*",
            "Effect": "Allow"
        },
```

```
        {
            "Action": [
                "resource-groups:CreateGroup",
                "resource-groups:ListGroupResources",
                "resource-groups:DeleteGroup",
                "resource-groups:Tag"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "tag:GetResources",
                "tag:GetTagKeys",
                "tag:GetTagValues",
                "tag:TagResources",
                "tag:UntagResources"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

3. a. 選擇下一步，標籤。
   b. 選擇下一步，檢閱。
   c. 在 [檢閱原則] 頁面中，針對 [名稱] 輸入**S3ResourceCreationAndArtifactAccessPolicy**。
   d. 選擇建立政策。
4. 在導覽窗格中，選擇 Roles (角色)，然後選擇 Create role (建立角色)。
5. 針對 [選取受信任的實體]，選擇 [自訂信任原則]，然後輸入下列 JSON 原則：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GivePermissionsToServiceCatalog",
            "Effect": "Allow",
            "Principal": {
                "Service": "servicecatalog.amazonaws.com"
            },
```

```
            "Action": "sts:AssumeRole"
        },
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::account_id:root"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringLike": {
                    "aws:PrincipalArn": [
                        "arn:aws:iam::accounti_id:role/TerraformEngine/
TerraformExecutionRole*",
                        "arn:aws:iam::accounti_id:role/TerraformEngine/
ServiceCatalogExternalParameterParserRole*",
                        "arn:aws:iam::accounti_id:role/TerraformEngine/
ServiceCatalogTerraformOSParameterParserRole*"
                    ]
                }
            }
        }
    ]
}
```

6. 選擇下一步。
7. 在「策略」清單中，選取S3ResourceCreationAndArtifactAccessPolicy您剛建立的。
8. 選擇下一步。
9. 在角色名稱中，輸入 **SCLaunch-S3product**。

> **Important**
>
> 啟動角色名稱必須以「SCLaunch」開頭，後面接著所需的角色名稱。

10. 選擇建立角色。

> **Important**
>
> 在AWS Service Catalog系統管理員帳戶中建立啟動角色之後，您也必須在使用者帳戶中建立相同的AWS Service Catalog啟動角色。一般使用者帳戶中的角色必須具有相同的名稱，並且包含與系統管理員帳戶中角色相同的策略。

在一AWS Service Catalog般使用者帳戶中建立啟動角色

1. 以系統管理員身分登入使用者帳戶，然後依照 IAM 使用者指南中的 JSON 索引標籤上建立新政策的指示進行操作。
2. 重複上述在AWS Service Catalog管理員帳戶中建立啟動角色的步驟 2-10。

> **Note**
>
> 在使用AWS Service Catalog者帳戶中建立啟動角色時，請務必在自訂信任原則**`AccountId`**中使用相同的系統管理員。

既然您已在管理員帳戶和一般使用者帳戶中建立啟動角色，您可以將啟動限制新增至產品。

步驟 6：將啟動限制新增至您的地形產品

> **Important**
>
> 您必須為 HashiCorp Terraform 產品建立啟動限制。如果沒有啟動限制，一般使用者就無法佈建產品。

在管理員帳戶中建立啟動角色後，您就可以將啟動角色與外部或 Terraform Cloud 產品的啟動限制相關聯。

此啟動限制可讓一般使用者啟動產品，並在啟動後將其作為已佈建產品進行管理。如需詳細資訊，請參閱 AWS Service Catalog 啟動限制。

使用啟動限制可讓您遵循將最終使用者 IAM 許可保持在最低限度的 IAM 最佳做法。如需詳細資訊，請參閱《IAM 使用者指南》中的授予最低權限。

若要將啟動限制指派給產品

1. 請在以下位置開啟AWS Service Catalog主控台。 https://console.aws.amazon.com/servicecatalog
2. 在左側導覽主控台中，選擇「產品組合」。
3. 選擇 S3 儲存貯體產品組合。
4. 在學檔詳細資訊頁面上，選擇「條件約束」標籤，然後選擇「建立條件約束」。

5. 對於「產品」，選擇簡單 S3 儲存貯體。 AWS Service Catalog會自動選取「啟動」約束類型。
6. 選擇 [輸入角色名稱]，然後選擇 [朗讀-S3 產品]。
7. 選擇 [建立]。

> **Note**
>
> 指定的角色名稱必須存在於建立啟動限制的帳戶，以及使用此啟動限制啟動產品的使用者帳戶中。

步驟 7：授與使用者存取權

將啟動限制套用至 HashiCorp Terraform 產品後，您就可以在支點帳戶中將存取權授予終端使用者。

在本教學課程中，您會使用主要使用者名稱共用授與存取權給使用者。主參與者名稱是群組、角色和使用者的名稱，管理員可以在學檔中指定，然後與學檔共用。當您共用學檔時，請AWS Service Catalog驗證這些主要名稱是否已存在。如果存在，則AWS Service Catalog會自動將相符的 IAM 主體與共用產品組合建立關聯，以授予最終使用者的存取權。檢閱共用學檔以取得詳細資訊。

必要條件

如果您尚未為最終使用者建立 IAM 群組，請參閱將權限授予AWS Service Catalog最終用戶。

提供存取產品組合

1. 導覽至產品組合頁面，然後選擇 S3 儲存貯體組合。
2. 選擇存取權標籤，然後選擇 [授與存取權]。
3. 在 [存取類型] 窗格中，選擇 [主體名稱]。
4. 在 [主體名稱] 窗格中，選取 [主要使用者名稱] 類型，然後在輸輻帳戶中輸入所需一般使用者的主要使用者名稱。
5. 選擇 Grant access (授與存取權)。

第 8 步：與最終用戶共享投資組合

AWS Service Catalog管理員可以使用共用或 account-to-account AWS Organizations共用來散佈具有使用者帳戶的產品組合。在本教學課程中，您將從管理員帳戶 (Hub 帳戶) (也是組織的管理帳戶) 與組織共用您的產品組合。

從管理中心帳戶共用產品組合

1. 請在以下位置開啟AWS Service Catalog主控台。 https://console.aws.amazon.com/servicecatalog/
2. 在產品組合頁面上，選取 S3 儲存貯體組合。在 [動作] 功能表中，選擇 [共用]。
3. 選擇 AWS Organizations，然後篩選至您的組織結構。
4. 在「AWS組織」窗格中，選擇一般使用者帳戶 (輪輻帳戶)。

   您也可以根據組織結構，選取根節點，與整個組織、父系組織單位 (OU) 或組織內的子 OU 共用產品組合。如需詳細資訊，請檢閱共用產品組合。
5. 在「共用設定」窗格中，選擇「主參與者共用」
6. 選擇共用。

成功與使用者共用產品組合後，下一個步驟是驗證使用者體驗並佈建 Terraform 產品。

步驟 9：測試使用者體驗

若要確認使用者能夠成功存取一般使用者主控台檢視並啟動您的**Simple S3 bucket**產品，請以使用者AWS身分登入並執行下列工作。

若要驗證最終使用者是否能存取最終使用者主控台

- 在 https://console.aws.amazon.com/servicecatalog/ 打開AWS Service Catalog控制台以查看以下內容：
  - 產品 – 使用者可以使用的產品。
  - 佈建的產品 – 使用者已啟動的佈建產品。

確認使用者是否可以啟動 Terraform 產品

1. 在主控台的「產品」區段中，選擇「簡單 S3 儲存貯體」。
2. 選擇 [啟動產品] 以啟動設定產品的精靈。
3. 在啟動簡單 S3 儲存貯體頁面上，輸入**Amazon S3 product**佈建的產品名稱。
4. 在「參數」頁面上，輸入下列項目並選擇「下一步」：
   - 名稱 — 為 Amazon S3 儲存貯體提供唯一的名稱。例如 **terraform-s3-product**。

5. 選擇「啟動產品」。主控台會顯示 Amazon S3 產品發佈的堆疊詳細資料頁面。產品的初始狀態為「變更中」。此需要幾分鐘的時間讓 AWS Service Catalog 啟動產品。若要查看目前狀態，請重新整理瀏覽器。成功推出產品後，狀態為「可用」。

   AWS Service Catalog創建一個名為的新 Amazon S3 存儲桶**`terraform-s3-product`**。

步驟 10：監視地形表單佈建作業

如果您想要監控佈建操作，可以檢閱 Amazon CloudWatch 日誌和AWS Step Functions任何佈建工作流程。

佈建工作流程有兩種狀態機器：

- `ManageProvisionedProductStateMachine`— 佈建新的 Terraform 產品時，以及更新現有 Terraform 佈建的產品時，AWS Service Catalog呼叫此狀態機器。
- `TerminateProvisionedProductStateMachine`— 終止現有 Terraform 佈建的產品時AWS Service Catalog呼叫此狀態機器。

執行監視狀態機器

1. 開啟AWS管理主控台，然後在安裝 Terraform 佈建引擎的管理中心帳戶中以系統管理員身分登入。
2. 打開 AWS Step Functions.
3. 在左側導覽面板中，選擇 [狀態機]。
4. 選擇ManageProvisionedProductStateMachine。
5. 在「執行」清單中，輸入佈建的產品 ID 以尋找您的執行項目。

   > **Note**
   >
   > AWS Service Catalog在佈建產品時建立已佈建的產品 ID。佈建的產品 ID 格式如下：**`pp-1111pwtn[ID number]`**

6. 選擇執行 ID。

在產生的「執行詳細資訊」頁面上，您可以檢視啟動設定工作流程中的所有步驟。您也可以檢閱任何失敗的步驟，以識別失敗的原因。

中的安全性 AWS Service Catalog

雲安全 AWS 是最高的優先級。身為 AWS 客戶，您可以從資料中心和網路架構中獲益，該架構專為滿足對安全性最敏感的組織的需求而打造。

安全是 AWS 與您之間共同承擔的責任。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 雲端中執行 AWS 服務的基礎架構。 AWS 還為您提供可以安全使用的服務。在 AWS 合規計劃中，第三方稽核員會定期測試並驗證我們的安全功效。

  若要深入瞭解適用於的合規方案 AWS Service Catalog，請參閱合規方案的AWS 服務範圍

- 雲端中的安全性 — 您的責任取決於您使用的 AWS 服務。您也必須對其他因素負責，包括資料的機密性、您公司的要求和適用法律和法規。

本文件可協助您瞭解如何在使用時套用共同責任模型 AWS Service Catalog。下列主題說明如何設定 AWS Service Catalog 以符合安全性與合規性目標。您還將介紹其他 AWS 服務，以幫助您監控和保護您的 AWS Service Catalog 資源。

主題

- 資料保護 AWS Service Catalog
- AWS Service Catalog中的 Identity and Access Management
- 登錄和監控 AWS Service Catalog
- 符合性驗證 AWS Service Catalog
- 韌性 AWS Service Catalog
- 基礎架構安全 AWS Service Catalog
- 安全性最佳做法 AWS Service Catalog

資料保護 AWS Service Catalog

AWS 共用責任模型適用於中的資料保護 AWS Service Catalog。如此模型中所述， AWS 負責保護執行所有 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，我們建議您使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 保護 AWS 帳戶 登入資料並設定個別使用者。如此一來，每個使用者都只會獲得授與完成其任務所必須的許可。我們也建議您採用下列方式保護資料：

- 每個帳戶均要使用多重要素驗證 (MFA)。
- 使用 SSL/TLS 與 AWS 資源進行通訊。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。
- 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。
- 如果您在透過命令列介面或 API 存取時需要經 AWS 過 FIPS 140-2 驗證的加密模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的更多相關資訊，請參閱聯邦資訊處理標準 (FIPS) 140-2 概觀。

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

使用加密來保護資料

靜態加密

AWS Service Catalog 使用 Amazon S3 儲存貯體和 Amazon DynamoDB 資料庫，這些資料庫使用亞馬遜管理的金鑰進行靜態加密。若要進一步了解，請參閱 Amazon S3 和 Amazon DynamoDB 提供的靜態加密相關資訊。

傳輸中加密

AWS Service Catalog 使用傳輸層安全性 (TLS) 和用戶端加密來電者與之間傳輸中的資訊 AWS。

您可以透過建立 VPC 端點，從 Amazon Virtual Private Cloud (Amazon VPC) 私有存取 AWS Service Catalog API。使用 VPC 端點時，VPC 和之間的路由會 AWS Service Catalog 由網路處理，而不需要 AWS 網際網路閘道、NAT 閘道或 VPN 連線。

所使用的最新一代 VPC 端點由技術提供支援 AWS PrivateLink， AWS Service Catalog 這項 AWS 技術可使用彈性網路介面與 VPC 中的私有 IP 來實現 AWS 服務之間的私有連線。

AWS Service Catalog中的 Identity and Access Management

存取需 AWS Service Catalog 要認證。這些認證必須具有存取 AWS 資源的權限，例如產品 AWS Service Catalog 組合或產品。 AWS Service Catalog 與 AWS Identity and Access Management (IAM) 整合，讓您能夠授與管理 AWS Service Catalog 員建立和管理產品所需的權限，並授與使用 AWS Service Catalog 者啟動產品和管理已佈建產品所需的權限。這些策略由系統管理員和一般使用者建立和管理， AWS 或是個別建立和管理。若要控制存取權，請將這些原則附加至搭配使用的使用者、群組和角色 AWS Service Catalog。

物件

您擁有的權限 AWS Identity and Access Management (IAM) 可能取決於您扮演的角色 AWS Service Catalog。

您透過 AWS Identity and Access Management (IAM) 擁有的許可也取決於您扮演的角色 AWS Service Catalog。

管理員-身為管理 AWS Service Catalog 員，您需要擁有管理員主控台和 IAM 許可的完整存取權，以便執行諸如建立和管理產品組合和產品、管理限制以及授予使用者存取權限等工作。

一般使用者-您必須先授與使用者存取使用者主控台的權限，才能讓使用 AWS Service Catalog 者使用您的產品。他們也可以擁有啟動產品與管理佈建產品的許可。

IAM 管理員-如果您是 IAM 管理員，您可能想要瞭解如何撰寫政策來管理存取權限的詳細資訊 AWS Service Catalog。若要檢視可在 IAM 中使用的 AWS Service Catalog 基於身分的政策範例，請參閱。the section called “AWS 受管理政策”

以身分識別為基礎的原則範例 AWS Service Catalog

主題

終端使用者的主控台存取

`AWSServiceCatalogEndUserFullAccess` 和 **`AWSServiceCatalogEndUserReadOnlyAccess`** 政策會將存取權授予 AWS Service Catalog 最終使用者主控台檢視。當具有這些策略之一的使用者

AWS Service Catalog 在中選擇時 AWS Management Console，一般使用者主控台檢視會顯示他們有權啟動的產品。

最終使用者可以成功啟動您授予存取權的產品之前，您必須提供其他 IAM 許可，以允許他們使用產品 AWS CloudFormation 範本中的每個基礎 AWS 資源。 AWS Service Catalog 例如，如果產品範本包含 Amazon Relational Database Service (Amazon RDS)，您必須授與使用者 Amazon RDS 啟動產品的許可。

若要瞭解如何讓使用者啟動產品，同時強制 AWS 資源的最低存取權限，請參閱。the section called “使用限制”

若您套用 **AWSServiceCatalogEndUserReadOnlyAccess** 政策，使用者有權存取最終使用者主控台，但他們沒有啟動產品與管理佈建產品所需的權限。您可以使用 IAM 將這些許可直接授與最終使用者，但如果您想限制最終使用者對 AWS 資源的存取權限，則應將該政策附加到啟動角色。然後，您可 AWS Service Catalog 以使用將啟動角色套用至產品的啟動條件約束。如需套用啟動角色、啟動角色限制和範例啟動角色的更多資訊，請參閱 AWS Service Catalog 啟動限制條件。

> **Note**
>
> 如果您授與使用者管理 AWS Service Catalog 員的 IAM 權限，則會改為顯示管理員主控台檢視。請勿授予最終使用者這些權限，除非您希望他們擁有管理員主控台檢視的存取權。

終端使用者的產品存取

最終使用者可以使用您授予存取權的產品之前，您必須提供其他 IAM 許可，以允許他們使用產品 AWS CloudFormation 範本中的每個基礎 AWS 資源。例如，如果產品範本包含 Amazon Relational Database Service (Amazon RDS)，您必須授與使用者 Amazon RDS 啟動產品的許可。

若您套用 **AWSServiceCatalogEndUserReadOnlyAccess** 政策，使用者有權存取最終使用者主控台檢視，但他們沒有啟動產品與管理佈建產品所需的權限。您可以將這些權限直接授與 IAM 中的一般使用者，但如果您想要限制最終使用者對 AWS 資源的存取權限，則應將該政策附加到啟動角色。然後，您可 AWS Service Catalog 以使用將啟動角色套用至產品的啟動條件約束。如需套用啟動角色、啟動角色限制和範例啟動角色的更多資訊，請參閱 AWS Service Catalog 啟動限制條件。

管理已佈建產品的範例原則

您可以建立自訂政策以協助符合組織的安全性要求。下列範例說明如何使用使用者、角色和帳戶層級的支援為每個動作自訂存取層級。您可以授予使用者檢視、更新、終止與管理佈建產品的存取權，該佈建產品的建立對象僅為該使用者或由在其角色下的其他人或他人登入的帳戶所建立。此存取權是階層式的

— 授與帳戶層級存取權限也會授予角色層級存取權限和使用者層級存取權，而新增角色層級存取權限也會授予使用者層級存取權，但不會授予 您可以使用 Condition 區塊在 policy JSON 指定這些做為 accountLevel、roleLevel 或 userLevel。

這些範例也適用於 AWS Service Catalog API 寫入作業的存取層級：UpdateProvisionedProduct和TerminateProvisionedProduct、和讀取作業：DescribeRecordScanProvisionedProducts、和ListRecordHistory。ScanProvisionedProducts 和 ListRecordHistory API 操作使用 AccessLevelFilterKey 做為輸入，且該金鑰值與在此討論的 Condition 區塊層級相對應 (accountLevel 等於「帳戶」的 AccessLevelFilterKey 值，roleLevel 對「角色」和 userLevel 對「使用者」)。如需詳細資訊，請參閱 Service Catalog 開發人員指南。

範例

- 佈建產品的完整管理員存取權
- 使用者存取已佈建產品
- 佈建產品的部分管理員存取權

佈建產品的完整管理員存取權

下列政策允取對在帳戶層級之目錄中佈建產品和報告的完整讀取和寫入存取權。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "servicecatalog:*"
         ],
         "Resource":"*",
         "Condition": {
            "StringEquals": {
               "servicecatalog:accountLevel": "self"
            }
         }
      }
   ]
}
```

此政策的功能與下列政策相等：

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "servicecatalog:*"
         ],
         "Resource":"*"
      }
   ]
}
```

未在的任何原則中指定Condition區塊會 AWS Service Catalog 被視為與指定"servicecatalog:accountLevel"存取權相同。請注意，accountLevel 存取包含 roleLevel 和 userLevel 存取。

使用者存取已佈建產品

下列政策會將讀取和寫入操作的存取權限制在只有目前使用者已建立的佈建產品和相關報告。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "servicecatalog:DescribeProduct",
                "servicecatalog:DescribeProductView",
                "servicecatalog:DescribeProvisioningParameters",
                "servicecatalog:DescribeRecord",
                "servicecatalog:ListLaunchPaths",
                "servicecatalog:ListRecordHistory",
                "servicecatalog:ProvisionProduct",
                "servicecatalog:ScanProvisionedProducts",
                "servicecatalog:SearchProducts",
                "servicecatalog:TerminateProvisionedProduct",
                "servicecatalog:UpdateProvisionedProduct"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "servicecatalog:userLevel": "self"
```

```
                }
            }
        }
    ]
}
```

佈建產品的部分管理員存取權

以下兩個政策 (若同時適用於相同使用者) 透過提供完整唯讀存取與限制寫入存取來允許一種被稱為「部分管理存取」的存取權。此表示使用者可以看到目錄帳戶中的任何佈建產品或相關報告，但無法對非該使用者擁有的任何佈建產品或報告執行任何動作。

第一個政策允許使用者對目前使用者建立的佈建產品進行寫入操作，但不得對其他人建立的佈建產品進行相同操作。第二個政策會新增對所有 (使用者、角色或帳戶) 建立之佈建產品的讀取操作存取權。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "servicecatalog:DescribeProduct",
                "servicecatalog:DescribeProductView",
                "servicecatalog:DescribeProvisioningParameters",
                "servicecatalog:ListLaunchPaths",
                "servicecatalog:ProvisionProduct",
                "servicecatalog:SearchProducts",
                "servicecatalog:TerminateProvisionedProduct",
                "servicecatalog:UpdateProvisionedProduct"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "servicecatalog:userLevel": "self"
                }
            }
        }
    ]
}
```

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "servicecatalog:DescribeRecord",
                "servicecatalog:ListRecordHistory",
                "servicecatalog:ScanProvisionedProducts"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "servicecatalog:accountLevel": "self"
                }
            }
        }
    ]
}
```

AWS 受管理的政策 AWS Service Catalog AppRegistry

AWS 受管理的策略：**AWSServiceCatalogAdminFullAccess**

您可以附加AWSServiceCatalogAdminFullAccess到 IAM 實體。 AppRegistry 也會將此原則附加至允許代表您執 AppRegistry 行動作的服務角色。

此原則會授與#理權限，這些權限允許完整存取管理員主控台檢視，並授與建立和管理產品和產品組合的權限。

許可詳細資訊

此政策包含以下許可。

- servicecatalog— 允許主參與者擁有管理員主控台檢視的完整權限，以及建立和管理產品組合與產品、管理條件約束、授與存取權給使用者，以及在中 AWS Service Catalog執行其他管理工作。
- cloudformation— 允許 AWS Service Catalog 列出，讀取，寫入和標記 AWS CloudFormation 堆棧的完整權限。
- config— 允許透過以下方式對產品組合、產品和佈建產品的 AWS Service Catalog 有限權限 AWS Config。
- iam— 允許主參與者完整權限來檢視及建立建立及管理產品及產品組合所需的服務使用者、群組或角色。

- ssm-允許 AWS Service Catalog 使用列 AWS Systems Manager 出和讀取當前 AWS 帳戶和 AWS 區域中的 Systems Manager 文檔。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStackEvents",
                "cloudformation:DescribeStacks",
                "cloudformation:SetStackPolicy",
                "cloudformation:UpdateStack",
                "cloudformation:CreateChangeSet",
                "cloudformation:DescribeChangeSet",
                "cloudformation:ExecuteChangeSet",
                "cloudformation:ListChangeSets",
                "cloudformation:DeleteChangeSet",
                "cloudformation:ListStackResources",
                "cloudformation:TagResource",
                "cloudformation:CreateStackSet",
                "cloudformation:CreateStackInstances",
                "cloudformation:UpdateStackSet",
                "cloudformation:UpdateStackInstances",
                "cloudformation:DeleteStackSet",
                "cloudformation:DeleteStackInstances",
                "cloudformation:DescribeStackSet",
                "cloudformation:DescribeStackInstance",
                "cloudformation:DescribeStackSetOperation",
                "cloudformation:ListStackInstances",
                "cloudformation:ListStackSetOperations",
                "cloudformation:ListStackSetOperationResults"
            ],
            "Resource": [
                "arn:aws:cloudformation:*:*:stack/SC-*",
                "arn:aws:cloudformation:*:*:stack/StackSet-SC-*",
                "arn:aws:cloudformation:*:*:changeSet/SC-*",
                "arn:aws:cloudformation:*:*:stackset/SC-*"
            ]
        },
```

```
        {
            "Effect": "Allow",
            "Action": [
                "cloudformation:CreateUploadBucket",
                "cloudformation:GetTemplateSummary",
                "cloudformation:ValidateTemplate",
                "iam:GetGroup",
                "iam:GetRole",
                "iam:GetUser",
                "iam:ListGroups",
                "iam:ListRoles",
                "iam:ListUsers",
                "servicecatalog:Get*",
                "servicecatalog:Scan*",
                "servicecatalog:Search*",
                "servicecatalog:List*",
                "servicecatalog:TagResource",
                "servicecatalog:UntagResource",
                "servicecatalog:SyncResource",
                "ssm:DescribeDocument",
                "ssm:GetAutomationExecution",
                "ssm:ListDocuments",
                "ssm:ListDocumentVersions",
                "config:DescribeConfigurationRecorders",
                "config:DescribeConfigurationRecorderStatus"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "servicecatalog:Accept*",
                "servicecatalog:Associate*",
                "servicecatalog:Batch*",
                "servicecatalog:Copy*",
                "servicecatalog:Create*",
                "servicecatalog:Delete*",
                "servicecatalog:Describe*",
                "servicecatalog:Disable*",
                "servicecatalog:Disassociate*",
                "servicecatalog:Enable*",
                "servicecatalog:Execute*",
                "servicecatalog:Import*",
                "servicecatalog:Provision*",
```

```
                "servicecatalog:Put*",
                "servicecatalog:Reject*",
                "servicecatalog:Terminate*",
                "servicecatalog:Update*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "servicecatalog.amazonaws.com"
                }
            }
        },
     {
    "Effect": "Allow",
    "Action": "iam:CreateServiceLinkedRole",
    "Resource": "arn:aws:iam::*:role/aws-service-role/
orgsdatasync.servicecatalog.amazonaws.com/AWSServiceRoleForServiceCatalogOrgsDataSync",
    "Condition": {
    "StringEquals": {
     "iam:AWSServiceName": "orgsdatasync.servicecatalog.amazonaws.com"
           }
        }
    }
```

AWS 受管理的策略：**AWSServiceCatalogAdminReadOnlyAccess**

您可以附加AWSServiceCatalogAdminReadOnlyAccess到 IAM 實體。 AppRegistry 也會將此原則附加至允許代表您執 AppRegistry 行動作的服務角色。

此原則會授與##權限，允許對系統管理員主控台檢視進行完整存取。此原則不會授予建立或管理產品和產品組合的存取權。

許可詳細資訊

此政策包含以下許可。

- servicecatalog— 允許主參與者對管理員主控台檢視的唯讀權限。

- `cloudformation`— 允許 AWS Service Catalog 有限的權限列出和讀取 AWS CloudFormation 堆棧.
- `config`— 允許透過以下方式對產品組合、產品和佈建產品的 AWS Service Catalog 有限權限 AWS Config。
- `iam`— 可讓主參與者有限權限檢視建立及管理產品及產品組合所需的服務使用者、群組或角色。
- `ssm`-允許 AWS Service Catalog 使用列 AWS Systems Manager 出和讀取當前 AWS 帳戶和 AWS 區域中的 Systems Manager 文檔。

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "cloudformation:DescribeStackEvents",
    "cloudformation:DescribeStacks",
    "cloudformation:DescribeChangeSet",
    "cloudformation:ListChangeSets",
    "cloudformation:ListStackResources",
    "cloudformation:DescribeStackSet",
    "cloudformation:DescribeStackInstance",
    "cloudformation:DescribeStackSetOperation",
    "cloudformation:ListStackInstances",
    "cloudformation:ListStackSetOperations",
    "cloudformation:ListStackSetOperationResults"
   ],
   "Resource": [
    "arn:aws:cloudformation:*:*:stack/SC-*",
    "arn:aws:cloudformation:*:*:stack/StackSet-SC-*",
    "arn:aws:cloudformation:*:*:changeSet/SC-*",
    "arn:aws:cloudformation:*:*:stackset/SC-*"
   ]
  },
  {
   "Effect": "Allow",
   "Action": [
    "cloudformation:GetTemplateSummary",
    "iam:GetGroup",
    "iam:GetRole",
    "iam:GetUser",
    "iam:ListGroups",
```

```
    "iam:ListRoles",
    "iam:ListUsers",
    "servicecatalog:Get*",
    "servicecatalog:List*",
    "servicecatalog:Describe*",
    "servicecatalog:ScanProvisionedProducts",
    "servicecatalog:Search*",
    "ssm:DescribeDocument",
    "ssm:GetAutomationExecution",
    "ssm:ListDocuments",
    "ssm:ListDocumentVersions",
    "config:DescribeConfigurationRecorders",
    "config:DescribeConfigurationRecorderStatus"
   ],
   "Resource": "*"
  }
 ]
}
```

AWS 受管理的策略：**AWSServiceCatalogEndUserFullAccess**

您可以附加AWSServiceCatalogEndUserFullAccess到 IAM 實體。 AppRegistry 也會將此原則附加至允許代表您執 AppRegistry 行動作的服務角色。

此原則會授與參與#權限，這些權限允許使用者主控台檢視的完整存取權，並授與啟動產品和管理已佈建產品的權限。

許可詳細資訊

此政策包含以下許可。

- servicecatalog— 允許主參與者擁有一般使用者主控台檢視的完整權限，以及啟動產品和管理已佈建產品的能力。
- cloudformation— 允許 AWS Service Catalog 列出，讀取，寫入和標記 AWS CloudFormation 堆棧的完整權限。
- config— 允許 AWS Service Catalog 有限的權限列出和閱讀有關產品組合、產品和佈建產品的詳細資訊 AWS Config。
- ssm-允許 AWS Service Catalog 使用讀 AWS Systems Manager 取當前 AWS 帳戶和 AWS 區域中的 Systems Manager 文檔。

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "cloudformation:CreateStack",
    "cloudformation:DeleteStack",
    "cloudformation:DescribeStackEvents",
    "cloudformation:DescribeStacks",
    "cloudformation:SetStackPolicy",
    "cloudformation:ValidateTemplate",
    "cloudformation:UpdateStack",
    "cloudformation:CreateChangeSet",
    "cloudformation:DescribeChangeSet",
    "cloudformation:ExecuteChangeSet",
    "cloudformation:ListChangeSets",
    "cloudformation:DeleteChangeSet",
    "cloudformation:TagResource",
    "cloudformation:CreateStackSet",
    "cloudformation:CreateStackInstances",
    "cloudformation:UpdateStackSet",
    "cloudformation:UpdateStackInstances",
    "cloudformation:DeleteStackSet",
    "cloudformation:DeleteStackInstances",
    "cloudformation:DescribeStackSet",
    "cloudformation:DescribeStackInstance",
    "cloudformation:DescribeStackSetOperation",
    "cloudformation:ListStackInstances",
    "cloudformation:ListStackResources",
    "cloudformation:ListStackSetOperations",
    "cloudformation:ListStackSetOperationResults"
   ],
   "Resource": [
    "arn:aws:cloudformation:*:*:stack/SC-*",
    "arn:aws:cloudformation:*:*:stack/StackSet-SC-*",
    "arn:aws:cloudformation:*:*:changeSet/SC-*",
    "arn:aws:cloudformation:*:*:stackset/SC-*"
   ]
  },
  {
   "Effect": "Allow",
   "Action": [
```

```
    "cloudformation:GetTemplateSummary",
    "servicecatalog:DescribeProduct",
    "servicecatalog:DescribeProductView",
    "servicecatalog:DescribeProvisioningParameters",
    "servicecatalog:ListLaunchPaths",
    "servicecatalog:ProvisionProduct",
    "servicecatalog:SearchProducts",
    "ssm:DescribeDocument",
    "ssm:GetAutomationExecution",
    "config:DescribeConfigurationRecorders",
    "config:DescribeConfigurationRecorderStatus"
   ],
   "Resource": "*"
  },
  {
   "Effect": "Allow",
   "Action": [
    "servicecatalog:DescribeProvisionedProduct",
    "servicecatalog:DescribeRecord",
    "servicecatalog:ListRecordHistory",
    "servicecatalog:ListStackInstancesForProvisionedProduct",
    "servicecatalog:ScanProvisionedProducts",
    "servicecatalog:TerminateProvisionedProduct",
    "servicecatalog:UpdateProvisionedProduct",
    "servicecatalog:SearchProvisionedProducts",
    "servicecatalog:CreateProvisionedProductPlan",
    "servicecatalog:DescribeProvisionedProductPlan",
    "servicecatalog:ExecuteProvisionedProductPlan",
    "servicecatalog:DeleteProvisionedProductPlan",
    "servicecatalog:ListProvisionedProductPlans",
    "servicecatalog:ListServiceActionsForProvisioningArtifact",
    "servicecatalog:ExecuteProvisionedProductServiceAction",
    "servicecatalog:DescribeServiceActionExecutionParameters"
   ],
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "servicecatalog:userLevel": "self"
    }
   }
  }
 ]
}
```

AWS 受管理的策略：**AWSServiceCatalogEndUserReadOnlyAccess**

您可以附加AWSServiceCatalogEndUserReadOnlyAccess到 IAM 實體。 AppRegistry 也會將此原則附加至允許代表您執 AppRegistry 行動作的服務角色。

此原則會授與##權限，允許使用者主控台檢視的唯讀存取權。此原則不會授與啟動產品或管理已佈建產品的權限。

許可詳細資訊

此政策包含以下許可。

- servicecatalog— 允許主參與者存取一般使用者主控台檢視的唯讀權限。
- cloudformation— 允許 AWS Service Catalog 有限的權限列出和讀取 AWS CloudFormation 堆棧.
- config— 允許 AWS Service Catalog 有限的權限列出和閱讀有關產品組合、產品和佈建產品的詳細資訊 AWS Config。
- ssm-允許 AWS Service Catalog 使用讀 AWS Systems Manager 取當前 AWS 帳戶和 AWS 區域中的 Systems Manager 文檔。

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "cloudformation:DescribeStackEvents",
    "cloudformation:DescribeStacks",
    "cloudformation:DescribeChangeSet",
    "cloudformation:ListChangeSets",
    "cloudformation:DescribeStackSet",
    "cloudformation:DescribeStackInstance",
    "cloudformation:DescribeStackSetOperation",
    "cloudformation:ListStackInstances",
    "cloudformation:ListStackResources",
    "cloudformation:ListStackSetOperations",
    "cloudformation:ListStackSetOperationResults"
   ],
   "Resource": [
    "arn:aws:cloudformation:*:*:stack/SC-*",
    "arn:aws:cloudformation:*:*:stack/StackSet-SC-*",
```

```
    "arn:aws:cloudformation:*:*:changeSet/SC-*",
    "arn:aws:cloudformation:*:*:stackset/SC-*"
   ]
  },
  {
   "Effect": "Allow",
   "Action": [
    "cloudformation:GetTemplateSummary",
    "servicecatalog:DescribeProduct",
    "servicecatalog:DescribeProductView",
    "servicecatalog:DescribeProvisioningParameters",
    "servicecatalog:ListLaunchPaths",
    "servicecatalog:SearchProducts",
    "ssm:DescribeDocument",
    "ssm:GetAutomationExecution",
    "config:DescribeConfigurationRecorders",
    "config:DescribeConfigurationRecorderStatus"
   ],
   "Resource": "*"
  },
  {
   "Effect": "Allow",
   "Action": [
    "servicecatalog:DescribeProvisionedProduct",
    "servicecatalog:DescribeRecord",
    "servicecatalog:ListRecordHistory",
    "servicecatalog:ListStackInstancesForProvisionedProduct",
    "servicecatalog:ScanProvisionedProducts",
    "servicecatalog:SearchProvisionedProducts",
    "servicecatalog:DescribeProvisionedProductPlan",
    "servicecatalog:ListProvisionedProductPlans",
    "servicecatalog:ListServiceActionsForProvisioningArtifact",
    "servicecatalog:DescribeServiceActionExecutionParameters"
   ],
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "servicecatalog:userLevel": "self"
    }
   }
  }
 ]
}
```

AWS 受管理的策略：**AWSServiceCatalogSyncServiceRolePolicy**

AWS Service Catalog 將此原則附加至AWSServiceRoleForServiceCatalogSync服務連結角色 (SLR)， AWS Service Catalog 以便將外部儲存庫中的範本同步至 AWS Service Catalog 產品。

此原則會授與權限，允許有限存取 AWS Service Catalog 動作 (例如 API 呼叫)，以及其他相 AWS Service Catalog 依 AWS 服務動作的權限。

此政策包含以下許可。

- servicecatalog— 允許成 AWS Service Catalog 品同步角色對 AWS Service Catalog 公用 API 的有限存取。
- codestar-connections— 允許成 AWS Service Catalog 品同步角色對CodeConnections 公用 API 的有限存取。
- cloudformation— 允許成 AWS Service Catalog 品同步角色對 AWS CloudFormation 公用 API 的有限存取。

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "ArtifactSynctoServiceCatalog",
   "Effect": "Allow",
   "Action": [
    "servicecatalog:ListProvisioningArtifacts",
    "servicecatalog:DescribeProductAsAdmin",
    "servicecatalog:DeleteProvisioningArtifact",
    "servicecatalog:ListServiceActionsForProvisioningArtifact",
    "servicecatalog:CreateProvisioningArtifact",
    "servicecatalog:UpdateProvisioningArtifact"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AccessArtifactRepositories",
   "Effect": "Allow",
   "Action": [
    "codestar-connections:UseConnection"
   ],
   "Resource": "arn:aws:codestar-connections:*:*:connection/*"
```

```
  },
  {
   "Sid": "ValidateTemplate",
   "Effect": "Allow",
   "Action": [
    "cloudformation:ValidateTemplate"
   ],
   "Resource": "*"
  }
 ]
}
```

AWS Service Catalog 針對使用者建立或更新使用的 AWS Service Catalog 產品時所建立的AWSServiceRoleForServiceCatalogSync服務連結角色，使用 CodeConnections上述權限詳細資料。您可以使用 AWS CLI、 AWS API 或透過 AWS Service Catalog 主控台修改此原則。如需如何建立、編輯及刪除服務連結角色的詳細資訊，請參閱〈使用服務連結角色 (SLR)〉。 AWS Service Catalog

AWSServiceRoleForServiceCatalogSync服務連結角色中包含的權限可 AWS Service Catalog 代表客戶執行下列動作。

- servicecatalog:ListProvisioningArtifacts— 允許人工因 AWS Service Catalog 素同步角色列出已同步至存放庫中範本檔案之指定 AWS Service Catalog 產品的佈建人工因素。
- servicecatalog:DescribeProductAsAdmin— 允許成 AWS Service Catalog 品同步角色使用 DescribeProductAsAdmin API 取得 AWS Service Catalog 產品的詳細資訊，以及與存放庫中範本檔案同步的產品及其關聯的已佈建成品。人工因素同步角色會使用此呼叫的輸出來驗證產品佈建人工因素的服務配額限制。
- servicecatalog:DeleteProvisioningArtifact— 允許成 AWS Service Catalog 品同步角色刪除已佈建的成品。
- servicecatalog:ListServiceActionsForProvisioningArtifact— 可讓 AWS Service Catalog 人工因素同步角色判斷「服務動作」是否與佈建人工因素相關聯，並確保在關聯「服務動作」時不會刪除佈建人工因素。
- servicecatalog:DescribeProvisioningArtifact— 允許成 AWS Service Catalog 品同步角色從 DescribeProvisioningArtifact API 擷取詳細資訊，包括SourceRevisionInfo輸出中提供的提交 ID。
- servicecatalog:CreateProvisioningArtifact— 如果對外部存放庫中的來源範本檔案偵測到變更 (例如，git-push 已提交)，則允許成 AWS Service Catalog 品同步角色建立新的佈建成品。

- `servicecatalog:UpdateProvisioningArtifact`— 允許 AWS Service Catalog 人工因素同步角色更新已連線或同步產品的已佈建成品。
- `codestar-connections:UseConnection`— 允許 AWS Service Catalog 成品同步角色使用現有連線來更新和同步產品。
- `cloudformation:ValidateTemplate`-允許 AWS Service Catalog 人工因素同步角色受限存 AWS CloudFormation 取權，以驗證外部存放庫中使用之範本的範本格式，並確認是否 AWS CloudFormation 可以支援範本。

AWS 受管理的策略：**AWSServiceCatalogOrgsDataSyncServiceRolePolicy**

AWS Service Catalog 將此原則附加至`AWSServiceRoleForServiceCatalogOrgsDataSync`服務連結角色 (SLR)， AWS Service Catalog 以允許同步處理。 AWS Organizations

此原則會授與權限，允許有限存取 AWS Service Catalog 動作 (例如 API 呼叫)，以及其他相 AWS Service Catalog 依 AWS 服務動作的權限。

此政策包含以下許可。

- `organizations`— 允許資 AWS Service Catalog 料同步角色對 AWS Organizations 公用 API 的有限存取。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "OrganizationsDataSyncToServiceCatalog",
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "organizations:ListAccounts",
                "organizations:ListChildren",
                "organizations:ListParents",
                "organizations:ListAWSServiceAccessForOrganization"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS Service Catalog 在使用者啟用共用學檔存取權或建立學檔 AWS Organizations 共用時所建立的AWSServiceRoleForServiceCatalogOrgsDataSync服務連結角色，使用上述權限詳細資料。您可以使用 AWS CLI、 AWS API 或透過 AWS Service Catalog 主控台修改此原則。如需如何建立、編輯及刪除服務連結角色的詳細資訊，請參閱〈使用服務連結角色 (SLR)〉。 AWS Service Catalog

AWSServiceRoleForServiceCatalogOrgsDataSync服務連結角色中包含的權限可 AWS Service Catalog 代表客戶執行下列動作。

- organizations:DescribeAccount— 允許「Organ AWS Service Catalog izations 資料同步」角色擷取有 AWS Organizations關指定帳戶的相關資訊。
- organizations:DescribeOrganization— 允許「組 Organ AWS Service Catalog izations 資料同步」角色擷取使用者帳戶所屬組織的相關資訊。
- organizations:ListAccounts— 允許「組 Organ AWS Service Catalog izations 資料同步」角色列出使用者組織中的帳號。
- organizations:ListChildren— 允許「組 Organ AWS Service Catalog izations 資料同步」角色列出指定父 OU 或根目錄中包含的所有組織單位 (UO) 或帳號。
- organizations:ListParents— 允許「Organ AWS Service Catalog izations 資料同步」角色列出作為指定子 OU 或帳戶之直接父系的根或 OU。
- organizations:ListAWSServiceAccessForOrganization— 允許「組 Organ AWS Service Catalog izations 資料同步」角色擷取使用者啟用以與其組織整合的 AWS 服務清單。

已取代政策

下列管理的政策已作廢。

- ServiceCatalogAdminFullAccess— 請AWSServiceCatalogAdminFullAccess改用。
- ServiceCatalogAdminReadOnlyAccess— 請AWSServiceCatalogAdminReadOnlyAccess改用。
- ServiceCatalogEndUserFullAccess— 請AWSServiceCatalogEndUserFullAccess改用。
- ServiceCatalogEndUserAccess— 請AWSServiceCatalogEndUserReadOnlyAccess改用。

使用下列程序以使用目前的政策確保系統管理員和最終使用者獲授予權限。

若要從已取代的政策遷移至目前政策，請參閱AWS Identity and Access Management 使用指南中的新增和移除 IAM 身分許可。

AppRegistry AWS 受管理策略的更新

檢視 AppRegistry 自此服務開始追蹤這些變更以來的 AWS 受管理策略更新詳細資料。如需有關此頁面變更的自動警示，請訂閱「 AppRegistry 文件歷史記錄」頁面上的 RSS 摘要。

變更	描述	日期
AWSServiceCatalogAdminFullAccess— 更新受管理策略	AWS Service Catalog 已更新`AWSServiceCatalogAdminFullAccess` 策略，以納入 AWS Service Catalog 管理員在其帳戶中建立`AWSServiceRoleForServiceCatalogOrgsDataSync` 服務連結角色 (SLR) 所需的權限。	2023 年 4 月 14 日
AWSServiceCatalogOrgsDataSyncServiceRolePolicy— 新的受管理策略	AWS Service Catalog 添加了`AWSServiceCatalogOrgsDataSyncServiceRolePolicy` ，它附加到`AWSServiceRoleForServiceCatalogOrgsDataSync` 服務鏈接角色（SLR），允許 AWS Service Catalog 與同步。 AWS Organizations此原則允許有限存取 AWS Service Catalog 動作 (例如 API 呼叫)，以及其他 AWS Service Catalog 依賴的 AWS 服務動作。	2023 年 4 月 14 日
AWSServiceCatalogAdminFullAccess— 更新受管理策略	AWS Service Catalog 已更新`AWSServiceCatalogAdminFullAccess` 原則以包含 AWS Service Catalog 管理	2023 年 1 月 12 日

變更	描述	日期
	員的所有權限，並建立與的相容性 AppRegistry。	
AWSServiceCatalogSyncServiceRolePolicy— 新的受管理策略	AWS Service Catalog 已新增附加至`AWSServiceRoleForServiceCatalogSync` 服務連結角色 (SLR) 的`AWSServiceCatalogSyncServiceRolePolicy` 原則。此原則允許 AWS Service Catalog 將外部儲存庫中的範本同步至 AWS Service Catalog 產品。	2022 年 11 月 18 日
AWSServiceRoleForServiceCatalogSync— 新的服務連結角色	AWS Service Catalog 已新增`AWSServiceRoleForServiceCatalogSync` 服務連結角色 (SLR)。 AWS Service Catalog 若要使用 CodeConnections 和建立、更新和描述產品的 AWS Service Catalog 佈建人工因素，需要此角色。	2022 年 11 月 18 日

變更	描述	日期
AWSServiceCatalogAdminFullAccess-更新了管理策略	AWS Service Catalog 更新`AWSServiceCatalogAdminFullAccess` 策略以包含 AWS Service Catalog 管理員所需的所有權限。此原則可識別管理員可對所有 AWS Service Catalog 資源執行的特定動作，例如建立、描述、刪除等。此外，原則已變更為支援最近啟動的功能，屬性型存取控制 (ABAC)。 AWS Service Catalog ABAC 可讓您使用`AWSServiceCatalogAdminFullAccess` 原則做為範本，以允許或拒絕以標籤為基礎的 AWS Service Catalog 資源動作。如需 ABAC 的詳細資訊，請參閱中的 ABAC 是什麼。 AWSAWS Identity and Access Management	2022 年 9 月 30 日
AppRegistry 開始追蹤變更	AppRegistry 開始追蹤其 AWS 受管理策略的變更。	2022 年 9 月 15 日

使用 AWS Service Catalog的服務連結角色

AWS Service Catalog 使用 AWS Identity and Access Management (IAM) 服務連結角色。服務連結角色是直接連結到 AWS Service Catalog的唯一 IAM 角色類型。服務連結角色由預先定義， AWS Service Catalog 並包含服務代表您呼叫其他服 AWS 務所需的所有權限。

服務連結角色可讓您 AWS Service Catalog 更輕鬆地設定，因為您不需要手動新增必要的權限。 AWS Service Catalog 定義其服務連結角色的權限，除非另有定義，否則只 AWS Service Catalog 能擔任其角色。定義的許可包括信任政策和許可政策，且該許可政策無法附加至其他 IAM 實體。

您必須先刪除服務連結角色的相關資源，才能將其刪除。這樣可以保護您的 AWS Service Catalog 資源，因為您無法不小心移除存取資源的權限。

如需支援服務連結角色之其他服務的相關資訊，請參閱可搭配 IAM 運作的AWS 服務，並尋找 Service-linked roles (服務連結角色) 資料行中顯示為 Yes (是) 的服務。選擇具有連結的是，以檢視該服務的服務連結角色文件。

AWSServiceRoleForServiceCatalogSync 的服務連結角色許可

AWS Service Catalog 可以使用名為的服務連結角色 **AWSServiceRoleForServiceCatalogSync**— 需要此服務連結角色， AWS Service Catalog 才能使用 CodeConnections 和建立、更新和描述產品的 AWS Service Catalog 佈建人工因素。

AWSServiceRoleForServiceCatalogSync 服務連結角色信任下列服務以擔任角色：

- sync.servicecatalog.amazonaws.com

名為的角色權限原則AWSServiceCatalogSyncServiceRolePolicy AWS Service Catalog 允許對指定的資源完成下列動作：

- 動作：CodeConnections 上的 Connection
- 動作：ProvisioningArtifact針Create, Update, and Describe對 AWS Service Catalog 產品開啟

您必須設定許可，IAM 實體 (如使用者、群組或角色) 才可建立、編輯或刪除服務連結角色。如需詳細資訊，請參閱 IAM 使用者指南中的服務連結角色許可。

建立 AWSServiceRoleForServiceCatalogSync 服務連結角色

您不需要手動建立AWSServiceRoleForServiceCatalogSync服務連結角色。 AWS Service Catalog 當您 CodeConnections 在 AWS Management Console、或 AWS API 中建立時，會自動為您建立服務連結角色。 AWS CLI

> **Important**
>
> 此服務連結角色可以顯示在您的帳戶，如果您於其他服務中完成一項動作時，可以使用支援此角色的功能。此外，如果您在 2022 年 11 月 18 日之前使用該 AWS Service Catalog 服務，則該服務開始支援服務連結角色時，請在您的帳戶中 AWS Service Catalog 建立

該AWSServiceRoleForServiceCatalogSync角色。若要進一步了解，請參閱我的 IAM 帳戶中出現的新角色。

若您刪除此服務連結角色，之後需要再次建立，您可以在帳戶中使用相同程序重新建立角色。當您建立時 CodeConnections， AWS Service Catalog 會再次為您建立服務連結角色。

您也可以使用 IAM 主控台，透過同步的 AWS Service Catalog 產品使用案例建立服務連結角色。在 AWS CLI 或 AWS API 中，使用sync.servicecatalog.amazonaws.com服務名稱建立服務連結角色。如需詳細資訊，請參閱《IAM 使用者指南》中的「建立服務連結角色」。如果您刪除此服務連結角色，您可以使用此相同的程序以再次建立該角色。

AWSServiceRoleForServiceCatalogOrgsDataSync 的服務連結角色許可

AWS Service Catalog 可以使用名為的服務連結角色 **AWSServiceRoleForServiceCatalogOrgsDataSync**— AWS Service Catalog 組織必須使用此服務連結角色才能與之保持同步。 AWS Organizations

AWSServiceRoleForServiceCatalogOrgsDataSync 服務連結角色信任下列服務以擔任角色：

- orgsdatasync.servicecatalog.amazonaws.com

除了AWSServiceCatalogOrgsDataSyncServiceRolePolicy受管理的策略之外，AWSServiceRoleForServiceCatalogOrgsDataSync服務連結角色還要求您使用下列信任策略：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "orgsdatasync.servicecatalog.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

名為的角色權限原則AWSServiceCatalogOrgsDataSyncServiceRolePolicy AWS Service Catalog 允許對指定的資源完成下列動作：

- 動作：DescribeAccountDescribeOrganization、和ListAWSServiceAccessForOrganization開啟 Organizations accounts
- 動作：ListAccountsListChildren、和ListParent開啟 Organizations accounts

您必須設定許可，IAM 實體 (如使用者、群組或角色) 才可建立、編輯或刪除服務連結角色。如需詳細資訊，請參閱 IAM 使用者指南中的服務連結角色許可。

建立 **AWSServiceRoleForServiceCatalogOrgsDataSync** 服務連結角色

您不需要手動建立AWSServiceRoleForServiceCatalogOrgsDataSync服務連結角色。 AWS Service Catalog 將您的行動視為啟用以 AWS Organizations 共用或作共用產品組合為代表您在背景建立單鏡反光相機的權限。 AWS Service Catalog

AWS Service Catalog 當您要求EnableAWSOrganizationsAccess或CreatePortfolioShare在 AWS Management Console、或 AWS API 中，自動為您建立服務連結角色。 AWS CLI

> **Important**
>
> 此服務連結角色可以顯示在您的帳戶，如果您於其他服務中完成一項動作時，可以使用支援此角色的功能。若要進一步了解，請參閱我的 IAM 帳戶中出現的新角色。

若您刪除此服務連結角色，之後需要再次建立，您可以在帳戶中使用相同程序重新建立角色。當您要求EnableAWSOrganizationsAccess或時CreatePortfolioShare， AWS Service Catalog 會再次為您建立服務連結角色。

為 AWS Service Catalog編輯服務連結角色

AWS Service Catalog 不允許您編輯AWSServiceRoleForServiceCatalogSync或AWSServiceRoleForServiceCatalogOrgsDataSyn務連結角色。因為有各種實體可能會參考服務連結角色，所以您無法在建立角色之後變更角色名稱。然而，您可使用 IAM 來編輯角色描述。如需詳細資訊，請參閱《IAM 使用者指南》中的編輯服務連結角色。

為 AWS Service Catalog刪除服務連結角色

您可以使用 IAM 主控台、 AWS CLI 或 AWS API 手動刪除AWSServiceRoleForServiceCatalogSync或AWSServiceRoleForServiceCatalogOrgsDataSyn反相機。若要這麼做，您必須先手動移除所有使用服務連結角色的資源 (例如，同步至外部存放庫的任何 AWS Service Catalog 產品)，然後再手動刪除服務連結角色。

AWS Service Catalog 服務連結角色的支援區域

AWS Service Catalog 支援在所有提供服務的區域中使用服務連結角色。如需詳細資訊，請參閱 AWS 區域與端點。

區域名稱	區域身分	中的 Support AWS Service Catalog
美國東部 (維吉尼亞北部)	us-east-1	是
美國東部 (俄亥俄)	us-east-2	是
美國西部 (加利佛尼亞北部)	us-west-1	是
美國西部 (奧勒岡)	us-west-2	是
非洲 (開普敦)	af-south-1	是
亞太區域 (香港)	ap-east-1	是
亞太區域 (雅加達)	ap-southeast-3	是
亞太區域 (孟買)	ap-south-1	是
亞太區域 (大阪)	ap-northeast-3	是
亞太區域 (首爾)	ap-northeast-2	是
亞太區域 (新加坡)	ap-southeast-1	是
亞太區域 (雪梨)	ap-southeast-2	是
亞太區域 (東京)	ap-northeast-1	是

區域名稱	區域身分	中的 Support AWS Service Catalog
加拿大 (中部)	ca-central-1	是
歐洲 (法蘭克福)	eu-central-1	是
歐洲 (愛爾蘭)	eu-west-1	是
歐洲 (倫敦)	eu-west-2	是
歐洲 (米蘭)	eu-south-1	是
歐洲 (巴黎)	eu-west-3	是
歐洲 (斯德哥爾摩)	eu-north-1	是
中東 (巴林)	me-south-1	是
南美洲 (聖保羅)	sa-east-1	是
AWS GovCloud (美國東部)	us-gov-east-1	否
AWS GovCloud (美國西部)	us-gov-west-1	否

疑難排解 AWS Service Catalog 身分和存取

使用下列資訊可協助您診斷和修正使用和 IAM 時可能遇到的 AWS Service Catalog 常見問題。

主題

我沒有執行操作的授權 AWS Service Catalog

如果 AWS Management Console 告訴您您沒有執行動作的授權，則您必須聯絡管理員以尋求協助。您的管理員是為您提供簽署憑證的人員。當 mateojackson 使用者嘗試使用主控台來檢視虛構 my-example-widget資源的詳細資料，但沒有虛構的權限時，就會發生下列範例錯誤。`aws:GetWidget`

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 aws:GetWidget on resource: my-example-widget
```

在此情況下，Mateo 會請求管理員更新他的政策，允許他使用 `my-example-widget` 動作存取 `aws:GetWidget` 資源。

我未獲得執行 **iam:PassRole** 的授權

若您收到錯誤，告知您並未獲得執行 `iam:PassRole` 動作的授權，您必須聯絡您的管理員以取得協助。您的管理員是提供您使用者名稱和密碼的人員。要求該人員更新您的政策，允許您將角色傳遞給 AWS Service Catalog。

某些 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 marymajor 的使用者嘗試使用主控台來執行中的動作時，就會發生下列範例錯誤。 AWS Service Catalog但是，動作要求服務具備服務角色授予的許可。Mary 沒有將角色傳遞至該服務的許可。

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

在此情況下，Mary 會要求管理員更新政策，以允許她執行 iam: PassRole 動作。

我想允許 AWS 帳戶以外的人員存取我的 AWS Service Catalog 資源

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

如需進一步了解，請參閱以下內容：

- 若要瞭解是否 AWS Service Catalog 支援這些功能，請參閱《AWS Service Catalog 管理員指南》AWS Identity and Access Management AWS Service Catalog中的〈〉。
- 若要了解如何跨您擁有的 AWS 帳戶提供資源的存取權，請參閱《IAM 使用者指南》中的另一個 AWS 帳戶提供存取權給 IAM 使用者。
- 若要了解如何為第三方 AWS 帳戶提供對資源的存取權，請參閱《IAM 使用者指南》中的提供第三方擁有 AWS 帳戶的存取權。

- 若要了解如何透過聯合身分提供存取權，請參閱 IAM 使用者指南中的將存取權提供給在外部進行身分驗證的使用者 (聯合身分)。
- 若要了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱 IAM 使用者指南中的 IAM 角色與資源型政策的差異。

控制存取

AWS Service Catalog 產品組合可為您的管理員提供一定程度的一般使用者群組存取控制。當您將使用者新增到產品組合時，這些使用者可以瀏覽並啟動產品組合中的任何產品。如需詳細資訊，請參閱 the section called “管理產品組合”。

限制

限制條件控制最終使用者自特定產品組合啟動產品時要套用哪些規則。您會使用它們來套用限制到產品以便監管或控制成本。如需限制條件的詳細資訊，請參閱 the section called “使用限制”。

AWS Service Catalog 啟動條件約束可讓您更好地控制使用者所需的權限。當管理員為產品組合中的一項產品建立啟動限制條件時，啟動限制條件便會關聯至當最終使用者從該產品組合啟動該產品時所使用的角色 ARN。使用此模式，您可以控制對 AWS 資源建立的存取。如需詳細資訊，請參閱 the section called “啟動限制條件”。

登錄和監控 AWS Service Catalog

AWS Service Catalog 與整合的服務可擷取所有 AWS Service Catalog API 呼叫 AWS CloudTrail，並將日誌檔傳送到您指定的 Amazon S3 儲存貯體。如需詳細資訊，請 AWS Service Catalog 參閱使用 CloudTrail.

您也可以使用通知限制來設定有關堆疊事件的 Amazon SNS 通知。如需詳細資訊，請參閱 the section called “通知限制條件”。

符合性驗證 AWS Service Catalog

協力廠商稽核人員會評估多項合規計畫 AWS Service Catalog 的安全性與 AWS 合規性，包括下列各項：

- 系統和組織控制 (SOC)
- 支付卡產業資料安全標準 (PCI DSS)

- 聯邦風險與授權管理計劃 (FedRAMP)
- 美國健康保險流通與責任法案 (HIPAA)

如需特定合規計劃範圍內的 AWS 服務清單，請參閱合規計劃的 AWS 服務範圍。 有關一般資訊，請參閱AWS 合規計劃AWS。

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

您在使用時的合規責任 AWS Service Catalog 取決於資料的敏感性、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：

- 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，並提供在上部署以安全性和法規遵循為重點的基準環境的步驟。 AWS
- 建構 HIPAA 安全性與合規性白皮書 — 本白皮書說明公司如何使用建立符合 HIPAA 標準的應用 AWS 程式。
- AWS 合規資源 — 此工作簿和指南集合可適用於您的產業和所在地。
- AWS Config— 此 AWS 服務評估您的資源配置是否符合內部實踐，行業準則和法規。
- AWS Security Hub— 此 AWS 服務提供安全狀態的全面檢視，協助您檢查您 AWS 是否符合安全性產業標準和最佳做法。

韌性 AWS Service Catalog

AWS 全球基礎架構是圍繞區 AWS 域和可用區域建立的。 AWS 區域提供多個實體分離和隔離的可用區域，這些區域透過低延遲、高輸送量和高度備援的網路連線。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。

如需區域和可用區域的相關 AWS 資訊，請參閱AWS 全域基礎結構。

除了 AWS 全球基礎架構外，還 AWS Service Catalog 提供 AWS Service Catalog 自助服務操作。有了自助式動作，客戶可以減少管理維護和最終使用者訓練，同時遵守合規和安全措施。身為管理員的您可借助自助式動作讓最終使用者執行如備份和還原等操作式任務、排除問題、執行核准的命令，以及在AWS Service Catalog中請求許可。如需進一步了解，請參閱the section called “使用服務動作”。

基礎架構安全 AWS Service Catalog

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

您可以使用 AWS 已發佈的 API 呼叫透 AWS Service Catalog 過網路進行存取。使用者端必須支援下列專案：

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

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

使用 AWS Service Catalog，您可以控制儲存資料的區域。產品組合和產品只能在您有提供它們的區域推出。您可以使用 `CopyProduct` API 來將產品複製到其他區域。

安全性最佳做法 AWS Service Catalog

AWS Service Catalog 在您開發和實作自己的安全性原則時，提供許多安全性功能供您考量。以下最佳實務為一般準則，並不代表完整的安全解決方案。這些最佳實務可能不適用或無法滿足您的環境需求，因此請將其視為實用建議就好，而不要當作是指示。

您可以定義規則，限制使用者在啟動產品時輸入的參數值。這些規則稱為範本限制，因為它們限制了產品的 AWS CloudFormation 範本的部署方式。您可以使用簡單的編輯器建立範本限制，然後將其套用到個別產品。

AWS Service Catalog 在佈建新產品或更新已在使用中的產品時套用限制。在套用到產品組合和產品的所有限制中，永遠會套用最嚴格的限制。例如，假設產品允許啟動所有 Amazon EC2 執行個體，且產品組合有兩個限制：一個允許啟動所有非 GPU 類型 EC2 執行個體，另一個僅允許啟動 t1.micro 和 m1.small EC2 執行個體。在此範例中， AWS Service Catalog 套用第二個限制較嚴格的約束 (t1.micro 和 m1.small)。

將 IAM 政策附加到啟動角色時，您可以限制最終使用者對 AWS 資源的存取權限。然後，您可 AWS Service Catalog 以使用建立啟動條件約束，以在啟動產品時使用該角色。

若要深入了解的受管理原則 AWS Service Catalog，請參閱的AWS 受管政策 AWS Service Catalog。

管理目錄

AWS Service Catalog 提供介面以便從管理員主控台管理產品組合、產品及限制條件。

> **Note**
>
> 若要執行本節的任何任務，您必須具有 AWS Service Catalog 的管理員權限。如需詳細資訊，請參閱 AWS Service Catalog中的 Identity and Access Management。

任務

- 管理產品組合
- 管理產品
- 使用 AWS Service Catalog 限制
- AWS Service Catalog 服務動作
- 將 AWS Marketplace 產品新增至產品組合
- 使用 AWS CloudFormation StackSets
- 管理預算

管理產品組合

您可以在AWS Service Catalog管理員主控台的學檔頁面上建立、檢視及更新學檔。

任務

- 建立、檢視和刪除產品組合
- 檢視產品組合詳細資訊
- 建立和刪除產品組合
- 新增產品
- 新增限制條件
- 授予存取權限給使用者
- 共用產品組合

- 共用和匯入投資組合

建立、檢視和刪除產品組合

「學檔」頁面會顯示您在目前區域中建立的學檔清單。使用此頁面來建立新產品組合、檢視產品組合詳細資訊或從帳戶中刪除產品組合。

若要檢視學檔頁面

1. 在 https://console.aws.amazon.com/servicecatalog/ 開啟 Service Catalog 主控台。
2. 必要時選取不同的區域。
3. 如果您是 AWS Service Catalog 的新使用者，就會看見 AWS Service Catalog 開始頁面。選擇 [入門] 以建立產品組合。依照指示建立您的第一個學檔，然後前往學檔頁面。

使用時AWS Service Catalog，您可以隨時返回「學檔」頁面；在導覽列中選擇「Service Catalog」，然後選擇「學檔」。

檢視產品組合詳細資訊

在 AWS Service Catalog 管理員主控台中，Portfolio details (產品組合詳細資訊) 頁面會列出產品組合的設定。您可以在此頁面管理產品組合中的產品、授與使用者產品存取權，以及套用 TagOptions 和限制條件。

檢視 Portfolio details (產品組合詳細資訊) 頁面

1. 在 https://console.aws.amazon.com/servicecatalog/ 開啟 Service Catalog 主控台。
2. 選擇您要管理的產品組合。

建立和刪除產品組合

使用學檔頁面來建立和刪除學檔。

新建產品組合

1. 在左側導覽選單中，選擇學檔。
2. 選擇 [建立組合]。
3. 在「建立學檔」頁面上，輸入要求的資訊。

4. 選擇建立。AWS Service Catalog 會建立產品組合，並顯示產品組合的詳細資訊。

刪除產品組合

> **Note**
>
> 您只能刪除本地學檔。您可以移除匯入的 (共用) 學檔，但無法刪除匯入的學檔。

刪除學檔之前，您必須先移除學檔的所有產品、條件約束、群組、角色、使用者、共用和 TagOptions。為此，請打開一個投資組合以顯示投資組合的詳細信息。然後選擇一個選項卡以將其刪除。

> **Note**
>
> 若要避免錯誤，請先移除產品組合中的限制，然後再移除任何產品。

1. 在左側導覽選單中，選擇學檔。
2. 選取您要刪除的學檔。
3. 選擇刪除。您只能刪除本地學檔。如果您嘗試刪除匯入的 (共用) 學檔，則無法使用 「動作」功能表。
4. 在確認視窗中，選擇 Delete (刪除)。

新增產品

您可以將產品直接上傳至現有產品組合，或將目錄中的現有產品與產品組合相關聯，將產品新增至產品組合。

> **Note**
>
> 建立AWS Service Catalog產品時，您可以上傳AWS CloudFormation範本或 Terraform 設定檔。該AWS CloudFormation模板存儲在 Amazon Simple Storage Service (Amazon S3) 存儲桶中，存儲桶名稱以「CF-模板-」開頭。佈建產品時，您也必須擁有從其他值區擷取物件的權限。如需詳細資訊，請參閱建立產品。

添加新產品

您可以直接從投資組合詳細信息頁面添加新產品。當您從此頁面建立產品，AWS Service Catalog 會將其新增到目前所選的產品組合。

若要新增一個新產品

1. 導覽至「學檔」頁面，然後選擇您要新增產品的學檔名稱。
2. 在產品組合詳細資料頁面上，展開「產品」區段，然後選擇「上傳新產品」。
3. 請於 Enter product details (輸入產品詳細資訊) 輸入以下資訊：
   - Product name (產品名稱) – 即產品名稱。
   - 產品說明 (選擇性) — 產品說明。此說明會顯示在產品清單中，以協助您選擇正確的產品。
   - 「描述」— 完整描述。此說明會顯示在產品清單中，以協助您選擇正確的產品。
   - 「所有者」或「經銷商」— 所有者的姓名或電子郵件地址。代理商的聯繫信息是可選的。
   - 廠商 (選用) — 應用程式發行者的名稱。此欄位可讓您對產品清單進行排序，以便更輕鬆地尋找產品。
4. 在 Version details (版本詳細資訊) 頁面上，輸入以下資訊：
   - 選擇範本 — 對於AWS CloudFormation產品，請選擇您自己的AWS CloudFormation範本檔案、本機磁碟機中的範本或指向 Amazon S3 中存放範本的 URL、現有的 AWS CloudFormation Stack ARN 範本或存放在外部存放庫中的範本檔案。

     對於 Teradata 產品，請選擇您自己的範本檔案、從本機磁碟機中選擇 tar.gz 組態檔或指向 Amazon S3 中存放之範本的 URL，或是存放在外部儲存庫中的 tar.gz 組態檔。
   - 版本名稱 (選用) — 產品版本的名稱 (例如，「v1"、「v2beta」)。不可使用空格。
   - Description (描述) (可選) – 產品版本的描述，包括此版本與先前版本的差異。
5. 請於 Enter support details (輸入支援詳細資訊) 輸入以下資訊：
   - Email contact (電子郵件聯絡人 [選擇性]) – 回報產品問題的電子郵件地址。
   - Sup@@ port 連結 (選用) — 網站的 URL，使用者可以在其中尋找支援資訊或檔案票證。URL 必須以 `http://`或 `https://` 開頭。管理員必須負責維護支援資訊的準確性與存取權。
   - Sup@@ port 說明 (選擇性) — 您應如何使用電子郵件連絡人與 Sup port 連結的說明。
6. 選擇「建立產品」。

新增現有產品

您可以從三個位置將現有產品新增至產品組合：產品組合清單、產品組合詳細資料頁面或產品清單頁面。

若要新增現有產品到產品組合中

1. 導覽至「學檔」頁面。
2. 選擇一個投資組合。然後選擇 [動作]-將產品新增至產品組合
3. 選擇產品，然後選擇「新增產品至產品組合」。

從產品組合中移除產品

如果您不想再使用某項產品，請將其從產品組合中移除。該產品仍然可以從「產品」頁面在您的目錄中找到，您仍然可以將其添加到其他產品組合中。您可以一次從產品組合移除多個產品。

若要從產品組合中移除產品

1. 導覽至「學檔」頁面，然後選擇包含該產品的學檔。學檔詳細資訊頁面隨即開啟。
2. 展開「產品」區段。
3. 選擇一或多個產品，然後選擇「移除」。
4. 確認您的選擇。

新增限制條件

您應該新增限制，以控制使用者與產品互動的方式。關於 AWS Service Catalog 所支援的限制條件類型，詳細資訊請參閱使用 AWS Service Catalog 限制。

您會在產品置入產品組合之後，對產品新增限制條件。

若要新增產品的限制條件

1. 在 https://console.aws.amazon.com/servicecatalog/ 開啟 Service Catalog 主控台。
2. 選擇投資組合並選擇投資組合。
3. 在學檔詳細資訊頁面中，展開「建立限制條件」區段，然後選擇「新增限制
4. 對於「產品」，選取要套用限制的產品。

5. 針對「限制」類型，選擇下列其中一個選項：

   啟動 — 可讓您將 IAM 角色指派給用於佈建AWS資源的產品。如需詳細資訊，請參閱 AWS Service Catalog 啟動限制條件。

   通知 — 可讓您將產品通知串流至 Amazon SNS 主題。如需詳細資訊，請參閱 AWS Service Catalog 通知限制條件。

   範本 — 可讓您限制終端使用者啟動產品時可用的選項。範本由包含一或多個規則的 JSON 格式文字檔組成。規則會加進產品所使用的 AWS CloudFormation 範本。如需詳細資訊，請參閱 範本限制規則。

   堆疊集 — 可讓您使用 AWS CloudFormation StackSets. 如需詳細資訊，請參閱 AWS Service Catalog 堆疊集限制。

   標籤更新 — 可讓您在佈建產品後更新標籤。若要取得更多資訊，請參閱AWS Service Catalog標籤更新約束。
6. 選擇「繼續」，然後輸入必要資訊。

若要編輯限制條件

1. 登入AWS Management Console並開啟AWS Service Catalog管理員主控台，網址為 https://console.aws.amazon.com/catalog/。
2. 選擇投資組合並選擇投資組合。
3. 在學檔詳細資訊頁面中，展開「建立條件約束」區段，然後選取要編輯的條件約束。
4. 選擇 「編輯限制」。
5. 視需要編輯限制，然後選擇「儲存」。

授予存取權限給使用者

讓使用者透過群組或角色存取學檔。為許多使用者提供產品組合存取權限的最佳方式是將使用者置於 IAM 群組中，並授予該群組的存取權。如此，您只要將使用者新增到群組或從群組中移除，就能管理對產品組合的存取。如需詳細資訊，請參閱 IAM 使用者指南中的 IAM 使用者和群組。

除了存取產品組合之外，使用者還必須擁有使用AWS Service Catalog者主控台的存取權。您可以透過在 IAM 中套用許可來授與主控台的存取權。如需詳細資訊，請參閱 AWS Service Catalog中的 Identity and Access Management。

如果您想要與其他帳戶共用學檔及其主參與者，您可以將主參與者名稱 (群組、角色或使用者) 與學檔產生關聯。主參與者名稱會與學檔共用，並在收件者帳戶中使用，以授與使用者存取權。

若要授予產品組合的存取權限給使用者或群組

1. 在 https://console.aws.amazon.com/servicecatalog/ 開啟 Service Catalog 主控台。
2. 從導覽窗格中選擇「管理」，然後選擇「學檔」。
3. 選擇您要授與群組、角色或使用者存取權的學檔。 AWS Service Catalog指向投資組合的詳細信息頁面。
4. 在學檔詳細資料頁面上，選擇存取權標籤。
5. 在「產品組合存取權限」下，選擇「授
6. 在「類型」中，選擇「主要使用者名稱」，然後選取群組/、角色/或使用者/、類型。您最多可以新增 9 個主要名稱。
7. 選擇授與存取權，將主參與者與目前的學檔產生關聯。

若要移除對產品組合的存取權限

1. 在學檔詳細資訊頁面上，選擇群組、角色或使用者名稱。
2. 選擇移除存取權限。

共用產品組合

若要讓其他AWS帳戶的AWS Service Catalog管理員能夠將您的產品發佈給使用者，請使用共用或與他們 account-to-account 共用您的產品AWS Service Catalog組合AWS Organizations。

當您使用「 account-to-account 共用」或「組 Organizations」共用學檔時，您正在分享該學檔的參考資料。在匯入的產品組合中的產品和限制條件，會與您對共用產品組合 (您所共用的原始產品組合) 所做的變更同步。

收件者無法變更產品或條件約束，但可以新增使用者的AWS Identity and Access Management存取權。

> **Note**
>
> 您無法共用共用資源。這包括包含已共用產品的產品組合。

一個ccount-to-account 分享

若要完成這些步驟，您必須取得目標帳戶的AWS帳號 ID。您可以在目標帳戶的「我AWS Management Console的帳戶」頁面上找到 ID。

與AWS帳戶分享投資組合

1. 在 https://console.aws.amazon.com/servicecatalog/ 開啟 Service Catalog 主控台。
2. 在左側導覽選單中，選擇學檔，然後選取您要分享的投資組合。在 [動作] 功能表中，選取 [共用]。
3. 在 [輸入帳戶 ID] 中，輸入您要共用之AWS帳戶的帳戶 ID。(選擇性) 選取 [TagOption 共用]。然後，選擇「分享到」。
4. 將該 URL 傳送給目標帳戶的 AWS Service Catalog 管理員。此 URL 會開啟「匯入學檔」頁面，並自動提供共用學檔的 ARN。

匯入一個產品組合

如果其他AWS帳戶的AWS Service Catalog管理員與您共用產品組合，請將該產品組合匯入您的帳戶，以便將其產品散佈給最終使用者。

如果投資組合是透過共用，則不需要匯入學檔AWS Organizations。

若要匯入學檔，您必須向管理員取得學檔 ID。

若要檢視所有匯入的學檔，請在 https://console.aws.amazon.com/servicecatalog/ 開啟AWS Service Catalog主控台。在「學檔」頁面上，選取「已匯入」標籤。檢閱「匯入的學檔」表。

以 AWS Organizations 共用

您可以使用 AWS Organizations 來共用 AWS Service Catalog 產品組合。

首先，您必須決定是從管理帳戶還是委派的系統管理員帳戶共用。如果您不想從管理帳戶共用，請註冊可用於共用的委派管理員帳戶。如需詳細資訊，請參閱《AWS CloudFormation 使用者指南》中的註冊委派管理員。

接下來，您必須決定要共用的對象。您可以共用至下列實體：

- 組織帳戶。
- 組織單位 (OU)。
- 組織本身。(這樣會與組織中的每個帳戶共用。)

從管理帳戶共用

當您使用組織結構或輸入組織節點的 ID 時，您可以與組織共用學檔。

使用組織結構與組織共用學檔

1. 開啟主AWS Service Catalog控台，網址為 https://console.aws.amazon.com/servicecatalog/。
2. 在學檔頁面上，選取您要分享的學檔。在 [動作] 功能表中，選取 [共用]。
3. 選取AWS Organizations並篩選至您的組織結構。

   您可以選取「根」節點，與整個組織、父系組織單位 (OU)、子 OU 或組織內的AWS帳戶共用產品組合。

   共用至父 OU 會將投資組合共用至該父 OU 內的所有帳戶和子系 OU。

   您可以選取 [僅檢視AWS帳戶] 以查看組織中所有AWS帳戶的清單。

若要透過輸入組織節點的 ID 與組織共用學檔

1. 開啟主AWS Service Catalog控台，網址為 https://console.aws.amazon.com/servicecatalog/。
2. 在學檔頁面上，選取您要分享的學檔。在 [動作] 功能表中，選取 [共用]。
3. 選取「組織節點」。

   選取要與整個組織共用、組織內的AWS帳戶或 OU 共用。

   輸入您所選組織節點的 ID，您可以在AWS Organizations主控台中找到此 ID，網址為 https://console.aws.amazon.com/organizations/。

從委派的管理員帳戶共用

組織的管理帳戶可以將其他帳戶註冊並取消註冊為組織的委派系統管理員。

委派的管理員可以像管理帳戶一樣，在其組織中共用AWS Service Catalog資源。他們被授權創建，刪除和共享投資組合。

若要註冊或取消註冊委派的系統管理員，您必須使用管理帳戶中的 API 或 CLI。如需詳細資訊，請參閱RegisterDelegatedAdministrator和 AWS Organizations API 參考中的DeregisterDelegatedAdministrator。

> **Note**
>
> 管理員必須先致電，才能指定代理人`EnableAWSOrganizationsAccess`。

從委派的系統管理員帳戶共用產品組合的程序與從管理帳戶共用產品組合的程序相同，如上所示the section called “從管理帳戶共用”。

如果成員已取消註冊為委派管理員，則會發生下列情況：

- 從該帳戶建立的產品組合共用會被移除。
- 他們不能再建立新的產品組合共用。

> **Note**
>
> 如果委派管理員取消註冊後，未移除委派管理員建立的學檔和共用，請再次註冊並取消註冊委派管理員。此動作會移除該帳戶建立的投資組合和股份。

在組織內移動帳戶

如果您在組織內移動帳戶，與該帳戶共用的AWS Service Catalog產品組合可能會變更。

帳戶只能存取與其目的地組織或組織單位共用的學檔。

共享 TagOptions 時的投資組合

身為管理員，您可以建立要包含的共用 TagOptions。 TagOptions 是可讓管理員執行下列作業的索引鍵值組：

- 定義並強制執行標籤的分類法。
- 定義標籤選項，並將其與產品和產品組合相關聯。
- 與其他帳戶的產品組合和產品相關聯的分享標籤選項。

當您在主帳戶中新增或移除標籤選項時，變更會自動顯示在收件者帳戶中。在收件者帳戶中，當使用者佈建產品時 TagOptions，他們必須為成為已佈建產品標籤的標籤選擇值。

在收件者帳戶中，管理員可以將其他本 TagOptions 機與其匯入的產品組合相關聯，以強制執行該帳戶專屬的標記規則。

> **Note**
>
> 要共享投資組合，您需要消費者的AWS帳戶 ID。在主機的「我的AWS帳戶」中找到帳戶 ID。

> **Note**
>
> 如果 TagOption 具有單一值，則會在佈建程序期間AWS自動強制執行該值。

分享投資組合 TagOptions 時

1. 在左側導覽選單中，選擇學檔。
2. 在本地投資組合中，選擇並打開一個投資組合。
3. 選擇分享到從上面的列表中，然後選擇分享到按鈕。
4. 選擇與其他AWS帳戶或組織共用。
5. 輸入 12 位數的帳戶 ID 號碼，選取 [啟用]，然後選擇 [共用]。

   您共用的帳戶會顯示在「共用對象」區段中。它指示是否 TagOptions 已啟用。

您也可以更新投資組合份額以包含在內 TagOptions。現在 TagOptions ，所有屬於投資組合和產品的內容都分享到此帳戶。

若要更新投資組合份額以包含 TagOptions

1. 在左側導覽選單中，選擇學檔。
2. 在本地投資組合中，選擇並打開一個投資組合。
3. 選擇分享到從上面的列表中。
4. 在共用對象的帳戶中，選擇帳戶 ID，然後選擇 [動作]。
5. 選取 [更新取消共用] 或 [取消共用]

   當您選取 [更新取消共用] 時，請選擇 [啟用] 以啟動共 TagOptions用。您共用的帳戶會顯示在「共用對象」區段中。

   當您選取 [取消共用] 時，請確認您不想再共用該帳戶。

分享投資組合時共享主要姓名

身為管理員，您可以建立包含主參與者名稱的學檔共用。主參與者名稱是群組、角色和使用者的名稱，管理員可以在學檔中指定，然後與學檔共用。當您共用學檔時，請AWS Service Catalog驗證這些主要名稱是否已存在。如果存在，則AWS Service Catalog會自動將相符的 IAM 主體與共用產品組合建立關聯，以授予使用者存取權。

> **Note**
>
> 當您將主體與產品組合建立關聯時，若該產品組合之後與其他帳戶共用，可能會出現潛在的權限提升途徑。對於收件者帳戶中不是AWS Service Catalog管理員，但仍然可以建立主體 (使用者/角色) 的使用者，該使用者可以建立與產品組合的主要名稱關聯相符的 IAM 主體。雖然此使用者可能無法透過 AWS Service Catalog 知道與哪些主體名稱相關聯，但他們可能會猜到使用者。如果對這種潛在的提升途徑有所顧慮，那麼 AWS Service Catalog 建議使用 `PrincipalType` 作為 `IAM`。使用此組態時，收件者帳戶中必須已存在 `PrincipalARN`，才能建立關聯。

當您在主帳戶中新增或移除主要帳戶中的主要帳戶時，AWS Service Catalog會自動在收件者帳戶中套用這些變更。接著，收件者帳戶中的使用者可以根據其角色執行工作：

- 最終用戶可以佈建，更新和終止產品組合的產品。
- 管理員可以將其他 IAM 主體與其匯入的產品組合建立關聯，以授與該帳戶專屬的終端使用者存取權。

> **Note**
>
> 主參與者名稱共用僅適用於AWS Organizations。

分享投資組合時共用主要名稱

1. 在左側導覽選單中，選擇學檔。
2. 在本地投資組合中，選擇您要分享的投資組合。
3. 在 [動作] 功能表中，選擇 [共用]。
4. 在中選取一個組織AWS Organizations。

5. 選取整個組織根目錄、組織單位 (OU) 或組織成員。
6. 在共用設定中，啟用主參與者共用選項。

您也可以更新投資組合共用以包含「主要使用者名稱」共用。這會與收款人帳戶共用屬於該投資組合的所有主要名稱。

若要更新學檔共用以啟用或停用主參與者名稱

1. 在左側導覽選單中，選擇學檔。
2. 在本地投資組合中，選擇要更新的投資組合。
3. 選擇 [共用] 索引標籤。
4. 選取您要更新的共用，然後選擇 [共用]。
5. 選擇 [更新共用]，然後選擇 [啟用] 以啟動主參與者共用。 AWS Service Catalog然後在收件者帳戶中共用主要名稱。

如果您想要停止與收件者帳戶共用主參與者名稱，請停用主參與者共用。

共用主要名稱時使用萬用字元

AWS Service Catalog支援使用萬用字元 (例如 '*' 或 '?') 授與 IAM 主體 (使用者、群組或角色) 名稱的產品組合存取權。使用萬用字元模式可讓您一次涵蓋多個 IAM 主體名稱。ARN 路徑和主要名稱允許無限制的萬用字元。

可接受的萬用字元 ARN 範例：

- **`arn:aws:iam:::role/ResourceName_*`**
- **`arn:aws:iam:::role/*/ResourceName_?`**

不可接受的萬用字元 ARN 範例：

- **`arn:aws:iam:::*/ResourceName`**

在 IAM 主要 ARN 格式 (**`arn:partition:iam:::resource-type/resource-path/resource-name`**) 中，有效值包括使用者/、群組/或角色/。該「？」 和「*」僅在資源 ID 段中的資源類型之後被允許。您可以在資源 ID 中的任何位置使用特殊字符。

「*」字符也匹配「/」字符，允許在資源 ID 中形成路徑。例如：

arn:aws:iam:::role/*/ResourceName_?匹配arn:aws:iam:::role/pathA/pathB/ResourceName_1和arn:aws:iam:::role/pathA/ResourceName_1。

共用和匯入投資組合

若要讓不屬於您的使用者 (例如屬於其他組織或組織中其他組織的使用者) 使用您AWS 帳戶的AWS Service Catalog產品，您可以與他們共用您的產品組合。AWS 帳戶您可以透過多種方式共用，包括 account-to-account 共用、組織共用和使用堆疊集部署目錄。

在與其他帳戶共用產品和產品組合之前，您必須決定是要共用目錄的參考，還是要將目錄複本部署到每個收件人帳戶。請注意，如果您部署複本，則如果有您要傳播到收件人帳戶的更新，就必須重新部署。

您可以使用堆疊集，同時將目錄部署至多個帳戶。如果您想要分享參考文獻 (作品集的匯入版本與原始檔案保持同步)，您可以使用分 account-to-account 享或使用分享AWS Organizations。

若要使用堆疊集部署目錄副本，請參閱如何設定公司標準AWS Service Catalog產品的多地區、多帳戶目錄。

當您使用 account-to-account 共用或分享產品組合時AWS Organizations，您可以允許其他AWS帳戶的AWS Service Catalog管理員將您的產品組合匯入他們的帳戶，並將產品分發給該帳戶中的終端使用者。

這個匯入的產品組合並非單獨的副本。在匯入的產品組合中的產品和限制條件，會與您對共用產品組合 (您所共用的原始產品組合) 所做的變更同步。收件者管理員 (與您共用產品組合的管理員) 無法變更產品或限制，但可以為最終使用者新增 AWS Identity and Access Management (IAM) 存取權。如需詳細資訊，請參閱 授予存取權限給使用者。

收件者管理員可以透過下列方式將產品散發給屬於其AWS帳戶的使用者：

- 將使用者、群組和角色新增至匯入的學檔。
- 透過將匯入產品組合中的產品新增至本機產品組合，收件者管理員會建立並屬於其AWS帳戶的個別產品組合。接著，收件者管理員會將使用者、群組和角色新增至該本機產品組合。原本套用至共用產品組合中產品的任何限制也會出現在本地產品組合中。本機學檔收件者管理員可以新增其他條件約束，但無法移除最初從共用學檔匯入的條件約束。

當您將產品或限制條件新增到共用的產品組合，或從中移除產品或限制條件時，變更會傳播到該產品組合所有匯入的執行個體。例如，如果您從共用產品組合移除產品時，該產品也會從匯入的產品組合中移除。該產品也會從匯入的產品加進的所有本機產品組合中移除。如果最終使用者在您移除之前啟動了產品，最終使用者已佈建的產品會繼續執行，但未來則無法再啟動和使用該產品。

如果您對共用產品組合中的產品，套用了啟動的限制條件，則此限制會傳播到該產品所有匯入的執行個體。若要覆寫此項啟動限制，收件人管理員可將產品新增到本機產品組合，然後對其套用不同的啟動限制條件。生效中的啟動限制條件，會設定產品的啟動角色。

啟動角色是一種 IAM 角色，AWS Service Catalog用於在最終使用者啟動產品時佈建AWS資源 (例如 Amazon EC2 執行個體或 Amazon RDS 資料庫)。身為管理員，您可以選擇指定特定的啟動角色 ARN 或區域角色名稱。如果您使用角色 ARN，即使一般使用者所屬的帳戶與擁有啟動角色的AWS帳戶不同，仍會使用該角色。如果您使用本機角色名稱，則會使用終端使用者帳戶中具有該名稱的 IAM 角色。

關於啟動限制條件和啟動角色的詳細資訊，請參閱 AWS Service Catalog 啟動限制條件。擁有啟動角色的 AWS 帳戶，會佈建 AWS 資源，而此帳戶會針對這些資源的使用產生費用。如需詳細資訊，請參閱 AWS Service Catalog 定價。

此影片說明如何在中跨帳戶共用投資組合AWS Service Catalog。

在中共用 (https://www.youtube.com/embed/BVSohYOppjk%22%3EShare) 跨帳戶的AWS Service Catalog投資組合

> **Note**
>
> 對於已匯入或共用的產品組合，您不能再共用其中的產品。

> **Note**
>
> 投資組合匯入必須在管理帳戶與相依帳戶之間的相同區域進行。

共用的和匯入的產品組合之間的關係

此表格總結匯入的學檔與共用學檔之間的關係，以及匯入學檔的管理員可以且無法使用該產品組合及其中產品的動作。

共用產品組合的項目	用來匯入產品組合的關係	收件人管理員可以	收件人管理員不能
產品和產品版本	繼承。	將匯入的產品新增到本機產品組合。產品	將產品上傳或新增到匯入的產品組合，或是從中移除產品。

共用產品組合的項目	用來匯入產品組合的關係	收件人管理員可以	收件人管理員不能
	如果產品組合的建立者將產品新增到共用的產品組合，或從中移除產品，則變更會傳播到匯入的產品組合。	會與共用的產品組合保持同步。	
啟動限制條件	繼承。 如果產品組合建立者將啟動限制新增至共用產品，或從共用產品中移除啟動限制，則變更會傳播至產品的所有匯入實例。 如果收件者管理員將匯入的產品新增至其本機產品組合，則匯入的啟動條件約束不會結轉至共用產品組合。	在本機產品組合中，管理員可以套用會影響產品本機啟動的啟動條件約束。	將啟動限制條件新增到匯入的產品組合，或從中移除啟動限制。

共用產品組合的項目	用來匯入產品組合的關係	收件人管理員可以	收件人管理員不能
範本限制條件	繼承。 如果產品組合的建立者將範本限制條件新增到共用的產品，或從中移除範本限制，則變更會傳播到產品所有匯入的執行個體。 如果收件者管理員將匯入的產品新增至本機產品組合，則匯入的範本條件約束不會結轉至本機產品組合。	在本端產品組合中，管理員可以加入限制本端產品的範本約束。	移除已匯入的範本限制條件。
使用者、群組和角色	未繼承。	新增管理員AWS帳戶中的使用者、群組和角色。	不適用。

管理產品

您可以建立產品、根據更新的範本建立新版本來更新產品，以及將產品群組到產品組合中，以便將產品分發給使用者。

產品新版本已傳播給有權透過產品組合存取產品的所有使用者。當您發佈更新時，使用者可以更新現有的已佈建產品。

任務

- 檢視產品頁面
- 建立產品
- 新增產品至產品組合
- 更新產品

- 將產品同步到來自 GitHub GitHub 企業或 Bitbucket 的範本檔案
- 刪除產品
- 管理版本

檢視產品頁面

您可以從管理AWS Service Catalog員主控台的「產品清單」頁面管理產品。

若要檢視產品清單頁面

1. 在 https://console.aws.amazon.com/servicecatalog/ 開啟 Service Catalog 主控台。
2. 選擇 [產品清單]。

建立產品

您可以從AWS Service Catalog管理員主控台的「產品」頁面建立產品。

> **Note**
>
> 建立 Terraform 產品需要額外的設定，包括 Terraform 佈建引擎和啟動角色。如需詳細資訊，請檢閱開始使用地形產品。

建立新的 AWS Service Catalog 產品

1. 導覽至「產品清單」頁面。
2. 選擇「建立產品」，然後選擇「建立產品」。
3. 產品詳細資訊 — 可讓您選擇要建立的產品類型。 AWS Service Catalog支持AWS CloudFormation，地形雲和外部（支持地形社區版）產品類型。產品詳細資訊也包含當您在清單或詳細資訊頁面中搜尋和檢視產品時所顯示的中繼資料。輸入下列資料：
   - Product name (產品名稱) – 即產品名稱。
   - 產品說明 — 產品說明會顯示在產品清單中，以協助您選擇正確的產品。
   - 「所有者」— 發行此產品的人員或組織。擁有者可以是您的 IT 組織或管理員的名稱。
   - 散發者 (選用) — 應用程式發行者的名稱。此欄位可讓您對產品清單進行排序，以便更輕鬆地尋找產品。

4. 版本詳細資料可讓您新增範本檔案並建立產品。輸入下列資料：

   - 選擇方法-有四種方法可以添加模板文件。
     - 使用本地模板文件-從本地驅動器上傳AWS CloudFormation模板或地形 tar.gz 配置文件。
     - 使用 Amazon S3 網址-指定一個指向存放在 Amazon S3 中的AWS CloudFormation範本或地形 tar.gz 組態檔案的網址。如果您指定一個 Amazon S3 URL，它必須以開頭`https://`。
     - 使用外部存儲庫-指定您的 GitHub， GitHub 企業或 Bitbucket 代碼存儲庫。 AWS Service Catalog可讓您將產品同步至範本檔案。對於 Terraform 產品，範本檔案格式必須是以 Tar 封存並以 Gzip 壓縮的單一檔案。
     - 使用現有 CloudFormation 堆疊-輸入現有 CloudFormation 堆疊的 ARN。此方法不支援地形雲端或外部產品。
   - 版本名稱 (選用) — 產品版本的名稱 (例如，「v1"、「v2beta」)。不可使用空格。
   - 說明 (選用) — 產品版本的說明，包括此版本與其他版本有何不同。
   - 指引 — 在「產品」詳細資訊頁面的「版本」索引標籤中管理。建立產品版本時 (在建立產品工作流程期間)，該版本的指引會設定為預設值。若要深入了解指引，請參閱管理版本。

5. Sup@@ port 詳細資料可識別您公司內的組織，並提供支援的聯絡窗口。輸入下列資料：

   - Email contact (電子郵件聯絡人 [選擇性]) – 回報產品問題的電子郵件地址。
   - Sup@@ port 連結 (選用) — 網站的 URL，使用者可以在其中尋找支援資訊或檔案票證。URL 必須以 `http://`或 `https://` 開頭。管理員必須負責維護支援資訊的準確性與存取權。
   - Sup@@ port 說明 (選用) — 您應如何使用電子郵件連絡人和 Sup port 連結的說明。

6. 管理標籤 (選用) — 除了使用標籤對資源進行分類之外，您還可以使用它們來驗證建立此資源的權限。

7. 建立產品 — 完成表單後，請選取 [建立產品]。幾秒鐘後，產品會顯示在「產品清單」頁面上。可能需要重新整理瀏覽器才能看到產品。

您也可以使用 CodePipeline 建立和設定管道，將產品範本部署到來源儲存庫中，AWS Service Catalog並傳遞您在來源儲存庫中所做的變更。如需詳細資訊，請參閱教學課程：建立部署到 AWS Service Catalog 的管道。

您可以在AWS CloudFormation或 Terraform 範本中定義參數屬性，並在佈建期間強制執行這些規則。這些屬性可以定義最小和最大長度、最小值和最大值、允許的值，以及值的規則運算式。 AWS Service Catalog如果提供的值不符合參數屬性，則在佈建期間發出警告。若要進一步瞭解參數性質，請參閱《AWS CloudFormation使用指南》中的〈參數〉。

故障診斷

您必須擁有從 Amazon S3 儲存貯體擷取物件的權限。否則，啟動或更新產品時，您可能會遇到下列錯誤。

```
Error: failed to process product version s3 access denied exception
```

如果您遇到此訊息，請確定擁有從下列值區擷取物件的權限：

- 儲存佈建成品範本的值區。
- 以 "cf-templates-*" 開頭的值區，以及AWS Service Catalog儲存佈建成品範本的位置。
- 以 "sc-*" 開頭且儲存中繼資料的內部AWS Service Catalog儲存貯體。您將無法從您的帳戶中看到此值區。

下列範例原則顯示從先前提到的值區擷取物件所需的最低權限。

```
{
          "Sid": "VisualEditor1",
          "Effect": "Allow",
          "Action": "s3:GetObject*",
          "Resource": [
              "arn:aws:s3:::YOUR_TEMPLATE_BUCKET",
              "arn:aws:s3:::YOUR_TEMPLATE_BUCKET/*",
              "arn:aws:s3:::cf-templates-*",
              "arn:aws:s3:::cf-templates-*/*",
              "arn:aws:s3:::sc-*",
              "arn:aws:s3:::sc-*/*"
          ]
      }
```

新增產品至產品組合

您可以將產品添加到任意數量的投資組合。更新產品時，包含該產品的所有產品組合 (包括共用產品組合) 都會自動接收新版本。

將產品從您的目錄新增到產品組合中

1. 導覽至「產品清單」頁面。
2. 選取產品，然後選擇「動作」。從下拉式選單中，選擇「新增產品至產品組合」。您將被定向到添加***name-of-product***到投資組合頁面。

3. 選擇產品組合，然後選擇「新增產品至產品組合」。

將 Terraform 產品新增至產品組合時，該產品需要啟動限制。您必須從帳戶中選取 IAM 角色、輸入 IAM 角色 ARN，或輸入角色名稱。如果您指定角色名稱，並且帳戶使用啟動限制，則該帳戶會使用該名稱作為 IAM 角色。這可讓啟動角色限制與帳戶無關，確保您可以為每個共用帳戶建立更少的資源。有關詳細信息和說明，請查看 步驟 6：將啟動限制新增至您的地形產品

一個組合可以包含大量的產品，是混合AWS CloudFormation和 Terraform 產品類型。

更新產品

當您更新產品的範本時，您會建立產品的新版本。新產品版本會自動提供給所有可存取包含產品組合的使用者使用。

> **Note**
>
> 更新現有產品時，您無法變更產品類型 (AWS CloudFormation或 Terform)。例如，如果您更新AWS CloudFormation產品，則無法使用 Terraform tar.gz 組態檔案取代現有的範AWS CloudFormation本。您必須使用新AWS CloudFormation樣板檔來更新既有的AWS CloudFormation樣板檔。

目前執行先前產品版本之已佈建產品的使用者可以將其佈建的產品更新為新版本。當產品有新版本可用時，使用者可以在已佈建的產品清單或已佈建的產品詳細資訊頁面上使用更新佈建的產品命令。

建立產品的新版本之前，建AWS Service Catalog議您在 Terraform 引擎中AWS CloudFormation或在 Terraform 引擎中測試產品更新，以確保它們正常運作。

建立新的產品版本

1. 導覽至「產品清單」頁面。
2. 選擇您要更新的產品。系統會將您導向至「產品詳細資料」頁面。
3. 在 [產品詳細資料] 頁面上，展開 [版本] 索引標籤，然後選擇 [建立新版本]。
4. 在 [版本詳細資料] 下，執行下列動作

   - 選擇範本-新增範本檔案的方式有四種。

     使用本地模板文件-從本地驅動器上傳AWS CloudFormation模板或地形 tar.gz 配置文件。

使用 Amazon S3 網址-指定一個指向存放在 Amazon S3 中的AWS CloudFormation範本或地形 tar.gz 組態檔案的網址。如果您指定一個 Amazon S3 網址，它必須以 https://開頭。

使用外部存儲庫-指定您的 GitHub， GitHub 企業或 Bitbucket 代碼存儲庫。 AWS Service Catalog可讓您將產品同步至範本檔案。對於 Terraform 產品，範本檔案格式必須是以 Tar 封存並以 Gzip 壓縮的單一檔案。

使用現有 CloudFormation 堆疊-輸入現有 CloudFormation 堆疊的 ARN。此方法不支援地形雲端或外部產品。

- 版本標題 — 產品版本的名稱 (例如，「v1"、「v2beta」)。不可使用空格。
- 說明 (選用) — 產品版本的說明，包括此版本與先前版本的不同之處。

5. 選擇 [建立產品版本]。

您也可以使用 CodePipeline 建立和設定管道，以將產品範本部署至來源儲存庫AWS Service Catalog，並將變更傳送至來源儲存庫。如需詳細資訊，請參閱教學課程：建立部署到 AWS Service Catalog 的管道。

將產品同步到來自 GitHub GitHub 企業或 Bitbucket 的範本檔案

AWS Service Catalog 可讓您將產品同步至透過外部存放庫提供者管理的範本檔案。 AWS Service Catalog 將具有此類範本連線的產品稱為 GIT 同步產品。儲存庫選項包括 GitHub「 GitHub 企業」或「比特桶」。 AWS 帳戶 使用外部存放庫帳戶授權後，您可以建立新 AWS Service Catalog 產品或更新現有產品，以同步至儲存庫中的範本檔案。對範本檔案進行變更並在儲存庫中提交 (例如，使用 git-push) 時， AWS Service Catalog 會自動偵測變更並建立新的產品版本 (成品)。

主題

- 將產品同步至外部範本檔案所需的權限
- 建立帳戶連線
- 查看與 GIT 同步的產品連接
- 更新 GIT 同步的產品連接
- 刪除與 GIT 同步的產品連線
- 將地形產品同步到來自 GitHub GitHub 企業或 Bitbucket 的範本檔案
- AWS 區域 支援與 GIT 同步的產品

將產品同步至外部範本檔案所需的權限

您可以使用下列 AWS Identity and Access Management (IAM) 政策做為範本，讓 AWS Service Catalog 管理員能夠將產品同步到外部存放庫中的範本檔案。此原則包含 CodeConnections 和所需的權限 AWS Service Catalog。 AWS Service Catalog 建議您複製下列範本原則，並在啟用儲存庫同步產品時使用 AWS Service Catalog `AWSServiceCatalogAdminFullAccess`受管理的策略。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CodeStarAccess",
            "Effect": "Allow",
            "Action": [
            "codestar-connections:UseConnection",
            "codestar-connections:PassConnection",
            "codestar-connections:CreateConnection",
            "codestar-connections:DeleteConnection",
            "codestar-connections:GetConnection",
            "codestar-connections:ListConnections",
            "codestar-connections:ListInstallationTargets",
            "codestar-connections:GetInstallationUrl",
            "codestar-connections:StartOAuthHandshake",
            "codestar-connections:UpdateConnectionInstallation",
            "codestar-connections:GetIndividualAccessToken"
            ],
            "Resource": "arn:aws:codestar-connections:*:*:connection/*"
        },
        {
        "Sid": "CreateSLR",
        "Effect": "Allow",
        "Action": "iam:CreateServiceLinkedRole",
        "Resource": "arn:aws:iam::*:role/aws-service-role/
sync.servicecatalog.amazonaws.com/AWSServiceRoleForServiceCatalogArtifactSync",
        "Condition": {
        "StringLike": {
        "iam:AWSServiceName": "sync.servicecatalog.amazonaws.com"
                }
            }
        }
    ]
}
```

建立帳戶連線

將範本檔案同步至 AWS Service Catalog 產品之前，您必須先建立並授權一次性 account-to-account 連線。您可以使用此連線來指定包含所需範本檔案的存放庫詳細資訊。您可以使用 AWS Service Catalog 主控台、主控 CodeConnections 台 AWS Command Line Interface (CLI) 或 CodeConnections API 建立連線。

建立連線後，您可以使用 AWS Service Catalog 主控台、 AWS Service Catalog API 或 CLI 建立同步的 AWS Service Catalog 產品。 AWS Service Catalog 管理員可以根據存放庫和分支中的範本檔案來建立新 AWS Service Catalog 產品或更新現有產品。如果存放庫中已提交變更，則 AWS Service Catalog 會自動偵測變更並建立新的產品版本。先前的產品版本會維持在規定的版本限制內，並指派已取代狀態。

此外，在建立連線之後， AWS Service Catalog 會自動建立服務連結角色 (SLR)。此 SLR 允許檢測提交 AWS Service Catalog 到存儲庫的任何模板文件更改。SLR 還允許自動 AWS Service Catalog 為同步產品創建新的產品版本。如需 SLR 權限和功能的詳細資訊，請參閱的服務連結角色。 AWS Service Catalog

若要建立新的 GIT 同步產品

1. 在左側導覽面板中，選擇 [產品清單]，然後選擇 [建立產品]。
2. 輸入產品詳細資訊。
3. 在 [版本詳細資料] 中，選擇 [使用 AWS CodeStar 提供者指定您的程式碼儲存庫]，然後選擇 [建立新的 AWS CodeStar 連線] 連結。
4. 建立連線之後，請重新整理連線清單，然後選取新的連線。指定存放庫詳細資訊，包括存放庫、分支和範本檔案路徑。

   如需有關使用 Terraform 組態檔案的資訊，請參閱。將地形產品同步到來自 GitHub GitHub 企業或 Bitbucket 的範本檔案

   a. (建立新 AWS Service Catalog 產品資源時選用) 在「Sup port 詳細資料」區段中，新增產品的中繼資料。

   b. (建立新 AWS Service Catalog 產品資源時選擇性) 在「標籤」區段中，選擇「新增標籤」，然後輸入「金鑰」和「值」配對。
5. 選擇 [建立新產品]。

若要建立多個 GIT 同步產品

1. 在 AWS Service Catalog 主控台左側導覽面板中，選擇 [產品清單]，然後選擇 [建立多個由 Git 管理的產品]。
2. 輸入「一般產品」詳細資訊。
3. 在外部存放庫詳細資訊中，選取AWS CodeStar 連線，然後指定存放庫和分支。
4. 在「新增產品」窗格中，輸入「範本檔案路徑」和「產品名稱」。選擇 [新增項目]，然後視需要繼續新增產品。
5. 新增所有需要的產品後，選擇「大量建立產品」。

若要將現有 AWS Service Catalog 產品連線至外部存放庫

1. 在 AWS Service Catalog 主控台左側導覽面板中，選擇 [產品清單]，然後選擇 [將產品 Connect 至外部存放庫]。
2. 在 [選取產品] 頁面上，選取您要連線至外部儲存庫的產品，然後選擇 [下一步]。
3. 在 [指定來源詳細資訊] 頁面上，選取現有的 AWS CodeStar 連線，然後指定存放庫、分支和範本檔案路徑。
4. 選擇下一步。
5. 在「檢閱並提交」頁面上，確認連線詳細資訊，然後選擇「將產品連線至外部儲存庫」。

查看與 GIT 同步的產品連接

您可以使用主 AWS Service Catalog 控台、API 或 AWS CLI 檢視存放庫連線詳細資料。對於連結至範本檔案的產 AWS Service Catalog 品，您可以從「上次同步狀態」擷取有關儲存庫連線以及範本上次與產品同步的時間資訊。

> **Note**
>
> 您可以在產品層級檢視儲存庫資訊和上次同步狀態。使用者必須在 CodeConnections API 中擁有 IAM 許可，才能檢視儲存庫詳細資料。如需有關這些 IAM 許可所需政策的詳細資訊，請參閱將 AWS Service Catalog 產品同步到範本檔案的所需權限。

若要檢視連線和儲存庫詳細資訊， AWS Management Console

1. 在左側導覽面板中，選擇 [產品清單]。

2. 從清單中選取產品。
3. 在「產品」頁面上，瀏覽至「產品來源詳細資料」區段。
4. 若要檢視產品版本的來源修訂 ID，請選擇「上次建立版本」連結。「版本詳細資訊」區段會顯示來源修訂 ID。

若要檢視連線和儲存庫詳細資訊， AWS CLI

從中 AWS CLI，執行下列命令：

```
$ aws servicecatalog describe-product-as-admin
```

```
$ aws servicecatalog describe-provisioning-artifact
```

```
$ aws servicecatalog search-product-as-admin
```

```
$ aws servicecatalog list-provisioning-artifacts
```

更新 GIT 同步的產品連接

您可以使用 AWS Service Catalog 主控台、 AWS Service Catalog API 或更新現有帳戶連線和 GIT 同步產品。 AWS CLI

要了解如何將現有 AWS Service Catalog 產品連接到模板文件，請參閱創建新的 GIT 同步產品連接。

將現有產品更新為 GIT 同步產品

1. 在左側導覽面板中，選擇 [產品清單]，然後選擇下列其中一個選項：
   - 若要更新單一產品，請選取該產品，瀏覽至「產品來源詳細資料」區段，然後選擇「編輯詳細資料」。
   - 若要更新多個產品，請選擇「將產品連線至外部儲存庫」，最多選取十個產品，然後選擇「下一步」。
2. 在「產品來源詳細資料」區段中，執行下列更新：
   - 指定連接。
   - 指定存放庫。
   - 指定分支。
   - 命名範本檔案。
3. 選擇儲存變更。

> **Note**
>
> 對於尚未連 Connect 至外部存放庫的產品，您可以在選取產品後，使用產品資訊頁面頂端警示中顯示的「連線至外部存放庫」選項。

您也可以使用 AWS Service Catalog 控制台或 AWS CLI

- 將現有 AWS Service Catalog 產品 Connect 至外部存放庫中的範本檔案
- 更新產品中繼資料，包括產品名稱、說明和標籤。
- 為先前連線的 AWS Service Catalog 產品重新設定 (更新同步以使用不同的存放庫來源) 連線。

使用 AWS Service Catalog 控制台更新連接和存儲庫詳細信息

1. 在 AWS Service Catalog 主控台左側導覽面板中，選擇 [產品清單]，然後選取目前連線至外部存放庫的產品。
2. 在「產品來源詳細資料」區段中選擇 「編輯產品來源」。
3. 在「產品來源詳細資料」區段中，指定新的所需儲存庫。
4. 選擇儲存變更。

若要更新連線和儲存庫詳細資訊， AWS CLI

從運 AWS CLI 行`$ aws servicecatalog update-product`和`$ aws servicecatalog update-provisioning-artifact`命令。

刪除與 GIT 同步的產品連線

您可以使用 AWS Service Catalog 主控台、 CodeConnections API 或刪除 AWS Service Catalog 產品與範本檔案之間的連線 AWS CLI。當您中斷產品與範本檔案的連線時，同步的 AWS Service Catalog 產品會切換至定期受管理的產品。中斷產品連線後，如果範本檔案在先前連線的儲存庫中發生變更並認可，變更不會反映出來。若要將 AWS Service Catalog 產品重新連線至外部儲存庫中的範本檔案，請參閱更新連線和同步的產 AWS Service Catalog 品。

使用控制台中斷與 GIT 同步的產品的連接 AWS Service Catalog

1. 在中 AWS Management Console，從左側導覽面板中選擇「產品清單」。
2. 從清單中選取產品。

3. 在「產品」頁面上，瀏覽至「產品來源詳細資料」區段。
4. 選擇中斷連線。
5. 確認動作，然後選擇 [中斷連線]。

若要使用中斷與 GIT 同步的產品連線 AWS CLI

從中 AWS CLI，執行命`$ aws servicecatalog update-product`令。
在`ConnectionParameters`輸入中，刪除指定的連接。

若要使用 CodeConnections API 刪除連線，或 AWS CLI

在 CodeConnections API 中 AWS CLI，或執行命`$ aws codestar-connections delete-connection`令。

將地形產品同步到來自 GitHub GitHub 企業或 Bitbucket 的範本檔案

使用 Terraform 設定檔建立 GIT 同步產品時，檔案路徑僅接受 tar.gz 格式。檔案路徑中不接受 Terraform 資料夾格式。

AWS 區域 支援與 GIT 同步的產品

AWS Service Catalog 支援中的 GIT 同步產品， AWS 區域 如下表所示。

AWS 區域 名稱	AWS 區域 身份	Support 與 GIT 同步的產品
美國東部 (維吉尼亞北部)	us-east-1	是
美國東部 (俄亥俄)	us-east-2	是
美國西部 (加利佛尼亞北部)	us-west-1	是
美國西部 (奧勒岡)	us-west-2	是
非洲 (開普敦)	af-south-1	否
亞太區域 (香港)	ap-east-1	否
亞太區域 (雅加達)	ap-southeast-3	否

AWS 區域 名稱	AWS 區域 身份	Support 與 GIT 同步的產品
亞太區域 (孟買)	ap-south-1	是
亞太區域 (大阪)	ap-northeast-3	否
亞太區域 (首爾)	ap-northeast-2	是
亞太區域 (新加坡)	ap-southeast-1	是
亞太區域 (雪梨)	ap-southeast-2	是
亞太區域 (東京)	ap-northeast-1	是
加拿大 (中部)	ca-central-1	是
歐洲 (法蘭克福)	eu-central-1	是
歐洲 (愛爾蘭)	eu-west-1	是
歐洲 (倫敦)	eu-west-2	是
歐洲 (米蘭)	eu-south-1	否
歐洲 (巴黎)	eu-west-3	是
歐洲 (斯德哥爾摩)	eu-north-1	是
中東 (巴林)	me-south-1	否
南美洲 (聖保羅)	sa-east-1	是
AWS GovCloud (美國東部)	us-gov-east-1	否
AWS GovCloud (美國西部)	us-gov-west-1	否

刪除產品

刪除產品時，AWS Service Catalog會從包含該產品的每個產品組合中移除所有產品版本。

AWS Service Catalog可讓您使用AWS Service Catalog主控台或刪除產品AWS CLI。若要成功刪除產品，您必須先取消與該產品相關聯的所有資源的關聯。產品資源關聯的範例包括產品組合關聯TagOptions、預算及服務動作。

> **Important**
>
> 刪除產品後，您無法復原該產品。

使用AWS Service Catalog主控台刪除產品

1. 導覽至「學檔」頁面，然後選取包含您要刪除之產品的學檔。
2. 選取您要刪除的產品，然後選擇產品窗格右上角的 [刪除]。
3. 對於沒有關聯資源的產品，請在文字方塊中輸入 delete 來確認您要刪除的產品，然後選擇「刪除」。

   對於具有相關資源的產品，請繼續執行步驟 4。
4. 在「刪除產品」視窗中，複查顯示所有產品相關資源的「關聯」表格。 AWS Service Catalog刪除產品時，會嘗試取消這些資源的關聯。
5. 在文字方塊中輸入 delete，確認您要刪除該產品並移除其所有關聯的資源。
6. 選擇「取消關聯並刪除」。

如果AWS Service Catalog無法取消產品所有資源的關聯，則不會刪除該產品。「刪除產品」視窗會顯示失敗的取消關聯數目，以及每個失敗的說明。如需有關解決刪除產品時失敗資源中斷關聯的詳細資訊，請參閱下方刪除產品時解決失敗的資源中斷關聯。

主題

使用刪除產品 AWS CLI

AWS Service Catalog可讓您使用 AWS Command Line Interface(AWS CLI) 從您的產品組合中刪除產品。AWS CLI 是開放原始碼工具，可讓您在命令列 shell 中使用命令來與 AWS 服務互動。AWS Service Catalog強制刪除函數需要AWS CLI別名，這是您可以在中建立的捷徑，以縮短您經常AWS CLI使用的指令或指令碼。

必要條件

- 安裝及設定 AWS CLI。如需詳細資訊，請參閱安裝或更新最新版本的AWS CLI和組態基本知識。使用 AWS CLI 最低版本 1.11.24 或 2.0.0。
- 刪除產品 CLI 別名需要與 Bash 相容的終端機和 JQ 命令列 JSON 處理器。如需有關安裝命令列 JSON 處理器的詳細資訊，請參閱下載 jq。
- 建立AWS CLI別名以批次處理 `Disassociation` API 呼叫，讓您在單一命令中刪除產品。

若要成功刪除產品，您必須先取消與該產品相關聯的所有資源的關聯。產品資源關聯的範例包括產品組合關聯、預算、標籤選項及服務動作。使用 CLI 刪除產品時，CLI `force-delete-product` 別名可讓您呼叫 `Disassociate` API 以取消任何可能阻止 `DeleteProduct` API 的資源的關聯。這樣可以避免單獨呼籲個人分離。

> **Note**
>
> 下列程序中顯示的檔案路徑可能會因您用來執行這些動作的作業系統而有所不同。

建立AWS CLI別名以刪除AWS Service Catalog產品

使用刪除AWS Service Catalog產品時，CLI `force-delete-product` 別名可讓您呼叫 `Disassociate` API 以取消任何可能阻止呼`DeleteProduct`叫的資源的關聯。AWS CLI

在您的AWS CLI組態資料夾中建立**`alias`**檔案

1. 在AWS CLI主控台中，瀏覽至設定資料夾。根據預設，設定資料夾路徑是`~/.aws/`在 Linux 和 macOS 上，或`%USERPROFILE%\.aws\`在視窗上。
2. `cli`使用檔案導覽或在偏好的終端機中輸入以下指令，建立名為的子資料夾：

   ```
   $ mkdir -p ~/.aws/cli
   ```

   產生的`cli`資料夾預設路徑是`~/.aws/cli/`在 Linux 和 MacOS 上，或`%USERPROFILE%\.aws\cli`在視窗上。
3. 在新資`cli`料夾中，建立名為不`alias`含副檔名的文字檔案。您可以使用`alias`檔案導覽或在偏好的終端機中輸入以下指令來建立檔案：

```
$ touch ~/.aws/cli/alias
```

4. [toplevel]在第一行輸入。
5. 儲存檔案。

接下來，您可以手動將 force-delete-product 別名指令碼貼到alias檔案中，或使用終端機視窗中的指令，將別名新增至檔案。

手動將 force-delete-product 別名新增至檔**alias**案

1. 在AWS CLI主控台中，瀏覽至您的AWS CLI設定資料夾並開啟alias檔案。
2. 在該[toplevel]行下方的檔案中輸入下列程式碼別名：

```
 [command servicecatalog]
force-delete-product =
  !f() {
    if [ "$#" -ne 1 ]; then
        echo "Illegal number of parameters"
        exit 1
    fi

    if [[ "$1" != prod-* ]]; then
       echo "Please provide a valid product id."
       exit 1
    fi

    productId=$1
    describeProductAsAdminResponse=$(aws servicecatalog describe-
product-as-admin --id $productId)
    listPortfoliosForProductResponse=$(aws servicecatalog list-
portfolios-for-product --product-id $productId)

    tagOptions=$(echo "$describeProductAsAdminResponse" | jq -r
 '.TagOptions[].Id')
    budgetName=$(echo "$describeProductAsAdminResponse" | jq -r
 '.Budgets[].BudgetName')
    portfolios=$(echo "$listPortfoliosForProductResponse" | jq -r
 '.PortfolioDetails[].Id')
```

```
                provisioningArtifacts=$(echo "$describeProductAsAdminResponse" | jq
 -r '.ProvisioningArtifactSummaries[].Id')
                provisioningArtifactServiceActionAssociations=()

                for provisioningArtifactId in $provisioningArtifacts; do
                  listServiceActionsForProvisioningArtifactResponse=$(aws
 servicecatalog list-service-actions-for-provisioning-artifact --product-id
 $productId --provisioning-artifact-id $provisioningArtifactId)
                  serviceActions=$(echo
 "$listServiceActionsForProvisioningArtifactResponse" | jq -r
 '[.ServiceActionSummaries[].Id] | join(",")')
                  if [[ -n "$serviceActions" ]]; then
                    provisioningArtifactServiceActionAssociations
+=("${provisioningArtifactId}:${serviceActions}")
                  fi
                done

                echo "Before deleting a product, the following associated resources
 must be disassociated. These resources will not be deleted. This action may take
 some time, depending on the number of resources being disassociated."

                echo "Portfolios:"
                for portfolioId in $portfolios; do
                  echo "\t${portfolioId}"
                done

                echo "Budgets:"
                if [[ -n "$budgetName" ]]; then
                  echo "\t${budgetName}"
                fi

                echo "Tag Options:"
                for tagOptionId in $tagOptions; do
                  echo "\t${tagOptionId}"
                done

                echo "Service Actions on Provisioning Artifact:"
                for association in
 "${provisioningArtifactServiceActionAssociations[@]}"; do
                  echo "\t${association}"
                done

                read -p "Are you sure you want to delete ${productId}? y,n "
                if [[ ! $REPLY =~ ^[Yy]$ ]]; then
```

```
                   exit
                fi

                for portfolioId in $portfolios; do
                  echo "Disassociating ${portfolioId}"
                  aws servicecatalog disassociate-product-from-portfolio --product-
id $productId --portfolio-id $portfolioId
                done

                if [[ -n "$budgetName" ]]; then
                  echo "Disassociating ${budgetName}"
                  aws servicecatalog disassociate-budget-from-resource --budget-
name "$budgetName" --resource-id $productId
                fi

                for tagOptionId in $tagOptions; do
                  echo "Disassociating ${tagOptionId}"
                  aws servicecatalog disassociate-tag-option-from-resource --tag-
option-id $tagOptionId --resource-id $productId
                done

                for association in
 "${provisioningArtifactServiceActionAssociations[@]}"; do
                  associationPair=(${association//:/ })
                  provisioningArtifactId=${associationPair[0]}
                  serviceActionsList=${associationPair[1]}
                  serviceActionIds=${serviceActionsList//,/ }
                  for serviceActionId in $serviceActionIds; do
                    echo "Disassociating ${serviceActionId} from
 ${provisioningArtifactId}"
                    aws servicecatalog disassociate-service-action-from-
provisioning-artifact --product-id $productId --provisioning-artifact-id
 $provisioningArtifactId --service-action-id $serviceActionId
                  done
                done

                echo "Deleting product ${productId}"
                aws servicecatalog delete-product --id $productId

              }; f
```

3. 儲存檔案。

使用終端機視窗將 force-delete-product 別名新增至**alias**檔案

1. 打開終端窗口並運行以下命令

   ```
   $ cat >> ~/.aws/cli/alias
   ```

2. 將別名指令碼貼到終端機視窗中，然後按 CTRL+D 結束指cat令。

呼叫別 force-delete-product 名

1. 在終端機視窗中，執行下列命令以呼叫刪除產品別名

   ```
   $ aws servicecatalog force-delete-product {product-id}
   ```

   下面的例子顯示了 force-delete-product alias 命令及其產生的響應

   ```
   $ aws servicecatalog force-delete-product prod-123
   ```

   ```
   Before deleting a product, the following associated resources must
   be disassociated. These resources will not be deleted. This action may take some
   time, depending on the number of resources being disassociated.
   Portfolios:
     port-123
   Budgets:
       budgetName
   Tag Options:
       tag-123
   Service Actions on Provisioning Artifact:
       pa-123:act-123
   Are you sure you want to delete prod-123? y,n
   ```

2. 輸入y以確認您要刪除產品。

成功刪除產品後，終端機窗口顯示以下結果

```
        Disassociating port-123
        Disassociating budgetName
```

```
        Disassociating tag-123
        Disassociating act-123 from pa-123
        Deleting product prod-123
```

其他資源

如需有關AWS CLI使用別名和刪除AWS Service Catalog產品的詳細資訊，請檢閱下列資源：

- 在 AWS Command Line Interface(CLI) 使用者指南中建立和使用AWS CLI別名。
- AWS CLI別名倉庫 git 存儲庫。
- 刪除AWS Service Catalog產品。
- AWS回復：發明 2016 年：有效AWS CLI的用戶。YouTube

解決刪除產品時失敗的資源中斷關聯

如果您先前嘗試刪除產品因資源取消關聯例外而失敗，請檢閱下方的例外清單及其解決方案。

> **Note**
>
> 如果您在收到失敗的資源解除關聯訊息之前關閉了「刪除產品」視窗，您可以依照「刪除產品」區段中的步驟 1 到 3，再次開啟視窗。

解決失敗的資源中斷關聯

在「刪除產品」視窗中，複查「關聯」表「狀態」欄。識別失敗的資源解除關聯例外狀況及建議的解決方案：

狀態例外類型	原因	解析度
產品證明 ****	AWS Service Catalog 無法刪除產品，因為產品仍有相關聯的預算 TagOptions、至少一個ProvisioningArtifact 具有	嘗試再次刪除產品。

狀態例外類型	原因	解析度
	相關動作、產品仍指派給「產品組合」、產品有使用者或產品有限制。	
使用者：username未授權執行下列動作：	嘗試刪除產品的使用者沒有取消產品資源關聯的必要權限。	AWS Service Catalog 建議您聯絡您的帳戶管理員，以取消目前沒有取消關聯之產品資源關聯的詳細資訊。

管理版本

您可以在建立產品時指派產品版本，而且可以隨時更新產品版本。

版本具有 AWS CloudFormation 範本、標題、描述、狀態和指導。

版本狀態

版本可具有下列三種狀態的其中一種：

- Active (作用中) - 版本清單中會顯示作用中版本，且可讓使用者啟動。
- Inactive (非作用中) - 版本清單中會隱藏非作用中版本。從此版本啟動的現有佈建產品不會受到影響。
- 已刪除-刪除的版本會從版本清單中移除。刪除版本無法復原。

版本指導

您可以設定版本指導，將產品版本相關資訊提供給最終使用者。版本指導只會影響作用中產品版本。

版本指導有下列兩種選項：

- 無-依預設，產品版本沒有任何指引。使用者可以使用該版本來更新和啟動已佈建的產品。
- 已取代-使用者無法使用已取代的產品版本啟動新的佈建產品。如果先前啟動的 p 佈建產品使用現已取代的版本，則使用者只能使用現有版本或新版本來更新已佈建的產品。

更新版本

您可以在建立產品時指派產品版本，而且也可以隨時更新版本。如需有關建立產品的詳細資訊，請參閱建立產品。

更新產品版本

1. 在 AWS Service Catalog 主控台中，選擇 Products (產品)。
2. 從產品清單中選擇您要更新版本的產品。
3. 在 Product details (產品詳細資料) 頁面上，選擇 Versions (版本) 標籤，然後選擇您要更新的版本。
4. 在 Version details (版本詳細資料) 頁面上，編輯產品版本，然後選擇 Save changes (儲存變更)。

使用 AWS Service Catalog 限制

您可以套用限制來控制在最終使用者啟動特定產品組合中要套用至產品的規則。當最終使用者啟動產品時，他們會看到您使用限制所套用的規則。您可以在產品放入產品組合後，隨即將限制套用至產品。當您建立限制時，限制便會處於主動狀態，並套用至所有尚未啟動之產品的目前版本。

限制

- AWS Service Catalog 啟動限制條件
- AWS Service Catalog 通知限制條件
- AWS Service Catalog 標籤更新限制
- AWS Service Catalog 堆疊集限制
- AWS Service Catalog 範本限制條件

AWS Service Catalog 啟動限制條件

啟動限制會指定使用者啟動、更新或終止產品時AWS Service Catalog假設的 AWS Identity and Access Management (IAM) 角色。IAM 角色是使用者或AWS服務可暫時假設使用AWS服務的許可集合。有關介紹性示例，請參閱：

- AWS CloudFormation產品類型:步驟 6：新增啟動限制以指派 IAM 角色
- 地形開源或地形雲產品類型：步驟 5：建立啟動角色

啟動限制適用於產品組合中的產品 (產品組合關聯)。啟動限制不適用於投資組合層級，也不適用於所有產品組合的產品。若要將啟動限制與產品組合中的產品建立關聯，您必須將啟動限制個別套用至每個產品。

如果沒有啟動限制，最終使用者必須使用自己的 IAM 登入資料啟動和管理產品。若要這麼做，他們必須擁有產品所使用之AWS服務和的權限AWS Service Catalog。AWS CloudFormation透過使用啟動角色，您可以將使用者的權限限制在他們對該產品所需的最低限度。如需有關最終使用者權限的詳細資訊，請參閱 AWS Service Catalog中的 Identity and Access Management。

若要建立和指派 IAM 角色，您必須具有下列 IAM 管理許可：

- `iam:CreateRole`
- `iam:PutRolePolicy`
- `iam:PassRole`
- `iam:Get*`
- `iam:List*`

設定啟動角色

您指派給產品做為啟動限制的 IAM 角色必須具有使用下列項目的權限：

適用於雲形產品

- `arn:aws:iam::aws:policy/AWSCloudFormationFullAccess`AWS CloudFormation受管理的策略
- 產品AWS CloudFormation範本中的服務
- 讀取服務擁有的 Amazon S3 儲存貯體中AWS CloudFormation範本的存取權限。

對於地形產品

- 產品的 Amazon S3 模板中的服務
- 讀取服務擁有的 Amazon S3 儲存貯體中 Amazon S3 範本的存取權限。
- `resource-groups:Tag`用於在 Amazon EC2 執行個體中進行標記 (執行佈建操作時由 Terraform 佈建引擎假設)
- `resource-groups:CreateGroup`用於資源群組標記 (假設AWS Service Catalog建立資源群組並指派標籤)

IAM 角色的信任政策必須允AWS Service Catalog許擔任該角色。在下列程序中，當您選取AWS Service Catalog作為角色類型時，會自動設定信任原則。如果您未使用主控台，請參閱如何將信任政策與 IAM 角色搭配使用中的角色，為擔任角色的AWS服務建立信任政策一節。

> **Note**
>
> `servicecatalog:ProvisionProduct`、`servicecatalog:TerminateProvisionedProduct` 及 `servicecatalog:UpdateProvisionedProduct` 權限無法以啟動角色指派。您必須使用 IAM 角色，如授與使用者權限一節中的內嵌政策步驟所示。AWS Service Catalog

> **Note**
>
> 若要在AWS Service Catalog主控台中檢視佈建的 Cloudformation 產品和資源，最終使用者需要AWS CloudFormation讀取存取權。在主控台中檢視佈建的產品和資源不會使用啟動角色。

建立啟動角色

1. 開啟位於 https://console.aws.amazon.com/iam/ 的 IAM 主控台。

   Terraform 產品需要額外的啟動角色設定。如需詳細資訊，請檢閱 Terraform 開放原始碼產品入門中的步驟 5：建立啟動角色。
2. 選擇角色。
3. 選擇 Create New Role (建立新角色)。
4. 輸入角色名稱，然後選擇 Next Step (下一步)。
5. 在旁邊的AWS服務角色下 AWS Service Catalog，選擇選取。
6. 在 Attach Policy (連接政策) 頁面上，選擇 Next Step (下一步)。
7. 若要建立角色，請選擇 Create Role (建立角色)。

將政策連接到新的角色

1. 選取您建立的角色以檢視該角色的詳細資訊頁面。
2. 選擇 Permissions (許可) 索引標籤，然後展開 Inline Policies (內嵌政策) 區段。然後，選擇 click here (按一下這裡)。
3. 選擇 Custom Policy (自訂政策)，然後選擇 Select (選取)。

4. 輸入原則的名稱，然後將以下內容貼到 Policy Document (政策文件) 編輯器：

```
          "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "s3:GetObject"
         ],
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "s3:ExistingObjectTag/servicecatalog:provisioning":"true"
            }
         }
   ]
}
```

> **Note**
>
> 為啟動條件約束設定啟動角色時，必須使用以下字串：`"s3:ExistingObjectTag/servicecatalog:provisioning":"true"`。

5. 為產品使用的每個其他服務新增一行至原則。例如，若要新增 Amazon 關聯式資料庫服務 (Amazon RDS) 的權限，請在清單最後一行的末尾輸入逗號，然後新增下`Action`列行：

```
"rds:*"
```

6. 選擇 Apply Policy (套用政策)

套用啟動限制

配置啟動角色之後，請將角色指派給產品做為啟動限制。此動作會告知AWS Service Catalog使用者在啟動產品時擔任該角色。

將角色指派至產品

1. 在 https://console.aws.amazon.com/servicecatalog/ 開啟 Service Catalog 主控台。
2. 選擇包含該產品的產品組合。

3. 選擇 Constraints (限制) 索引標籤，並選擇 Create constraint (建立限制)。
4. 從產品中選擇產品，然後在「限制類型」下選擇「啟動」 選擇 繼續。
5. 在「啟動限制」區段中，您可以從帳戶中選取 IAM 角色，然後輸入 IAM 角色 ARN，或輸入角色名稱。

   如果您指定角色名稱，並且帳戶使用啟動限制，則該帳戶將使用該名稱作為 IAM 角色。此方法允許啟動角色限制與帳戶無關，因此您可以為每個共用帳戶建立更少的資源。

   > **Note**
   >
   > 指定的角色名稱必須存在於建立啟動限制的帳戶，以及使用此啟動限制啟動產品的使用者帳戶中。

6. 指定 IAM 角色後，選擇 Create (建立)。

將混淆的代理添加到啟動約束

AWS Service Catalog支援與假設角色要求一起執行的 API 的混淆副保護。新增啟動限制時，您可以使用啟動角色信任原則中的`sourceAccount`和`sourceArn`條件來限制啟動角色存取。它可確保啟動角色是由受信任的來源呼叫。

在下列範例中，一AWS Service Catalog般使用者屬於帳戶 1111111111。當AWS Service Catalog系統管理員`LaunchConstraint`為產品建立時，終端使用者可以在啟動角色信任原則中指定下列條件，將假設角色限制為帳號 1111111111。

```
"Condition":{
   "ArnLike":{
      "aws:SourceArn":"arn:aws:servicecatalog:us-east-1:111111111111:*"
   },
   "StringEquals":{
      "aws:SourceAccount":"111111111111"
   }

}
```

佈建具有產品的使用者`LaunchConstraint`必須具有相同的 `AccountId` (111111111111)。如果沒有，則作業會失敗並顯示錯`AccessDenied`誤，進而防止啟動角色濫用。

以下 AWS Service Catalog API 是保護混淆的副手保護：

- `LaunchConstraint`
- `ProvisionProduct`
- `UpdateProvisionedProduct`
- `TerminateProvisionedProduct`
- `ExecuteProvisionedProductServiceAction`
- `CreateProvisionedProductPlan`
- `ExecuteProvisionedProductPlan`

的`sourceArn` 保護AWS Service Catalog僅支援範本化 ARN，例如 "`arn:<aws-partition>:servicecatalog:<region>:<accountId>:`" 它不支援特定的資源 ARN。

驗證啟動限制

若要驗證AWS Service Catalog使用角色啟動產品並成功佈建產品，請從AWS Service Catalog主控台啟動產品。若要在發佈至使用者之前測試限制，請建立包含相同產品的測試產品組合，然後以該產品組合測試限制。

啟動產品

1. 在AWS Service Catalog主控台的功能表中，選擇 Service Catalog > 一般使用者。
2. 選擇產品以開啟「產品詳細資訊」頁面。在啟動選項表格中，確認角色的 Amazon 資源名稱 (ARN) 出現。
3. 選擇「啟動產品」。
4. 繼續啟動步驟，填寫任何必要的資訊。
5. 確認產品已成功啟動。

AWS Service Catalog 通知限制條件

> **Note**
>
> AWS Service Catalog不支援地形開放原始碼或 Terraform 雲端產品的通知限制。

通知限制可指定 Amazon SNS 主題以接收有關堆疊事件的通知。

使用下列程序以建立一個 SNS 主題並訂閱。

建立 SNS 主題與訂閱。

1. 在 https://console.aws.amazon.com/sns/v3/home 開啟 Amazon SNS 主控台。
2. 請選擇 建立主題。
3. 輸入主題名稱，然後選擇 Create topic (建立主題)。
4. 選擇建立訂閱。
5. 關於通訊協定，請選擇電子郵件。關於 Endpoint(端點)，輸入可用於接收通知的電子郵件地址。選擇 Create subscription (建立訂閱)。
6. 您將收到一封具有主旨行的確認電子郵件 `AWS Notification - Subscription Confirmation`。開啟電子郵件並遵循指示完成訂閱。

透過您用之前程序建立的 SNS 主題來使用下列程序以套用通知條件限制。

套用通知限制條件至產品

1. 在 https://console.aws.amazon.com/servicecatalog/ 開啟 Service Catalog 主控台。
2. 選擇包含該產品的產品組合。
3. 展開 Constraints (限制)，然後選擇 Add constraints (加入限制)。
4. 從「產品」中選擇產品，並將「限制類型」設為「通知」 選擇 繼續。
5. 選擇 Choose a topic from your account(從帳戶選擇一個主題)，然後選取您從 Topic Name (主題名稱) 建立的 SNS 主題。
6. 選擇提交。

AWS Service Catalog 標籤更新限制

> **Note**
>
> AWS Service Catalog不支援 Terraform 開放原始碼產品的標籤更新限制。

透過標籤更新限制，AWS Service Catalog管理員可以允許或禁止最終使用者更新與已佈建產品相關聯之資源的標籤。如果允許標籤更新，則與產品或產品組合相關聯的新標籤會在佈建的產品更新期間套用至已佈建的資源。

啟用產品的標籤更新

1. 在 https://console.aws.amazon.com/servicecatalog/ 開啟 Service Catalog 主控台。
2. 選擇包含您要更新之產品的產品組合。
3. 選擇「限制」頁標，並選擇「新增限制」。
4. 在 Constraint type (限制類型) 下，選擇 Tag Update (標籤更新)。
5. 從 Product (產品) 中選擇產品，然後選擇 Continue (繼續)。
6. 在 Tag Updates (標籤更新) 頁面 上，選取 Enable Tag Updates (啟用標籤更新)。
7. 選擇提交。

AWS Service Catalog 堆疊集限制

> **Note**
>
> - AWS Service Catalog不支援 Terraform 開放原始碼產品的堆疊集合限制。
> - AutoTags 目前不支援AWS CloudFormation StackSets。

堆疊集合限制可讓您使用來設定產品部署選項AWS CloudFormation StackSets。您可以指定多個帳戶和區域的產品啟動。使用者可以管理這些帳戶，並決定產品的部署位置和部署順序。

套用堆疊集限制至產品

1. 在 https://console.aws.amazon.com/servicecatalog/ 開啟 Service Catalog 主控台。
2. 選擇您想要的產品組合。
3. 選擇「限制」頁標，然後選擇「建立限制」。
4. 在「產品」中，選擇產品。在「限制」類型中，選擇「堆疊集」。
5. 設定堆疊集限制的帳戶、地區和權限。
   - 在帳戶設定中，識別您要在其中建立產品的帳戶。
   - 在「地區」設定中，選擇要部署產品的地理區域，以及您希望這些產品在這些區域中部署的順序。
   - 在許可中，選擇 IAM 管理 StackSet員角色來管理您的目標帳戶。如果您不選擇角色，請StackSets使用預設的 ARN。進一步了解如何設定堆疊集許可。

6. 選擇建立。

AWS Service Catalog 範本限制條件

> **Note**
>
> AWS Service Catalog不支援地形開放原始碼或地形雲端產品的範本限制。

若要限制最終使用者啟動產品的選項，您可以套用範本限制條件。套用範本限制條件以確保最終使用者可以使用產品，而不會違反您組織的合規要求。您可以將範本限制套用至學檔中的產AWS Service Catalog品。產品組合必須包含一或多個產品，然後您才可以定義範本限制條件。

範本限制條件包含一或多項規則，以縮小允許的參數值範圍，這些參數定義於產品底層的 AWS CloudFormation 範本中。AWS CloudFormation 範本中的參數定義一組值，使用者可在建立堆疊時指定這些值。例如，參數可定義各種執行個體類型，讓使用者可在啟動堆疊時選擇，其中包含 EC2 執行個體。

如果範本中的一組參數值對於您的產品組合的目標對象而言太寬廣，您可以定義範本限制條件，以限制使用者在啟動產品時可選擇的值。例如，如果範本參數包含的 EC2 執行個體類型，對於只應使用小型執行個體類型 (例如，`t2.micro` 或 `t2.small`) 的使用者而言過大，則您可以新增範本限制條件，以限制最終使用者可選擇的執行個體類型。如需有關 AWS CloudFormation 範本參數的詳細資訊，請參閱 https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/parameters-section-structure.html 使用者指南中的AWS CloudFormation參數相關文章。

範本限制條件會綁定在產品組合中。如果您將範本限制條件套用至一個產品組合，然後將該產品包含至另一個產品組合，則該限制將不會套用到第二個產品組合中的該產品。

如果您將範本限制條件套用至已與使用者共用的產品，則這些限制立即生效的範圍包括所有後續的產品啟動，以及產品組合中的所有產品版本。

您可以使用規則編輯器或在 AWS Service Catalog 管理員主控台以 JSON 文字編寫規則，以定義範本限制條件規則。如需有關規則的詳細資訊，包括語法和範例，請參閱 範本限制規則。

若要在發佈至使用者之前測試限制，請建立包含相同產品的測試產品組合，然後以該產品組合測試限制。

將範本限制條件套用至產品

1. 在 https://console.aws.amazon.com/servicecatalog/ 開啟 Service Catalog 主控台。

2. 在「學檔」頁面上，選擇包含您要套用範本限制之產品的學檔。
3. 展開「約束」區段，然後選擇「加入約束」
4. 在「選取產品與型態」視窗中，針對「產品」選擇您要定義範本限制的產品。然後，針對「條件約束」類型選擇「範本」 選擇 繼續。
5. 在 [範本條件約束產生器] 頁面上，使用 JSON 編輯器或規則產生器介面編輯條件約束規則。

   - 若要編輯規則的 JSON 代碼，請選擇「條件約束文字編輯器」索引標籤。此索引標籤提供數個範例以協助您開始使用。

     若要使用規則產生器介面來建置規則，請選擇「規則產生器」標籤。在此索引標籤上，您可以選擇產品的範本中指定的任何參數，而且您可為該參數指定允許的值。根據參數的類型，您指定允許值的方式包括選擇檢查清單中的項目、直接指定數值，或在以逗號分隔的清單中指定一組值。

     完成建立規則後，請選擇 [新增規則]。規則會顯示在「規則產生器」標籤的表格中。若要檢閱和編輯 JSON 輸出，請選擇「條件約束文字編輯器」索引標籤。
6. 編輯完條件約束的規則後，請選擇「提交」(Submit)。若要查看限制條件，請前往組合詳細資訊頁面，然後展開 [條件約束]

範本限制規則

在產品AWS Service Catalog組合中定義範本條件約束的規則說明一般使用者何時可以使用範本，以及他們可以為範AWS CloudFormation本中宣告的參數指定哪些值，這些參數用於建立他們嘗試使用的產品。規則有助於防止最終使用者在無意間指定了錯誤的值。例如，您可以新增規則以確認是否在特定 VPC 指定有效的子網路，或使用指定測試環境的 `m1.small` 執行個體類型。AWS CloudFormation 使用規則來驗證參數值，然後再建立產品的資源。

每個規則包含兩種屬性：規則條件 (選用) 和宣告 (必要)。規則條件決定規則是否生效。宣告說明了使用者可針對特定參數指定的值。如果您未定義規則條件，則該規則的宣告一律生效。若要定義規則條件，您可以使用規則特定的內部函數，這些函式只能在範本的 `Rules` 區塊中使用。您可以建立巢狀函式，但規則條件或宣告的最終結果必須為 true 或 false。

舉例來說，假設您在 `Parameters` 區塊中宣告了 VPC 和子網路參數。您可以建立一個規則，用來驗證特定的子網路是否在特定的 VPC 中。因此，當使用者指定 VPC，AWS CloudFormation 會在建立或更新堆疊之前評估宣告，來檢查子網路的參數值是否在該 VPC 中。如果參數值為無效，AWS CloudFormation 會立即無法建立或更新堆疊。如果使用者未指定 VPC，則 AWS CloudFormation 不會檢查子網路的參數值。

語法

範本的 Rules 區塊包含了金鑰名稱 Rules，後面接著單一冒號。所有的規則宣告皆會以括弧括起。如果宣告多項規則，這些規則會以逗號分隔。對於每項規則，您會在引號中宣告其邏輯名稱，後面依序接著冒號和括號，括號之中是規則條件與宣告。

規則可包含 RuleCondition 屬性，而且必須包含 Assertions 屬性。針對每項規則，您只能定義一個規則條件；您可以在 Assertions 屬性中定義一個或多個宣告。您可以使用規則特定的內部函數，來定義規則條件和宣告，如下列的虛擬範本所示：

```
"Rules":{
   "Rule01":{
      "RuleCondition":{
         "Rule-specific intrinsic function"
      },
      "Assertions":[
         {
            "Assert":{
               "Rule-specific intrinsic function"
            },
            "AssertDescription":"Information about this assert"
         },
         {
            "Assert":{
               "Rule-specific intrinsic function"
            },
            "AssertDescription":"Information about this assert"
         }
      ]
   },
   "Rule02":{
      "Assertions":[
         {
            "Assert":{
               "Rule-specific intrinsic function"
            },
            "AssertDescription":"Information about this assert"
         }
      ]
   }
}
```

虛擬範本顯示包含兩個名為 Rule01 和 Rule02 規則的 Rules 區段。Rule01 包含規則條件和兩個聲明。如果規則條件中的函式計算結果為 true，則會評估和套用每個宣告中的兩種函式。如果規則條件為 false，該規則不會生效。Rule02 始終生效，因為它沒有規則條件，這表示一律評估和套用一個宣告。

如需有關定義規則條件和宣告的特定規則內建函數的資訊，請參閱《使用指南》中的AWS規則函數。AWS CloudFormation

範例：有條件地驗證參數值

下列兩項規則會檢查 InstanceType 參數的值。視環境參數 (test 或 prod) 的值而定，使用者必須針對 m1.small 參數指定 m1.large 或 InstanceType。InstanceType 與 Environment 參數必須在同一個範本的 Parameters 區塊中宣告。

```
"Rules" : {
  "testInstanceType" : {
    "RuleCondition" : {"Fn::Equals":[{"Ref":"Environment"}, "test"]},
    "Assertions" : [
      {
        "Assert" :  { "Fn::Contains" : [ ["m1.small"], {"Ref" : "InstanceType"} ] },
        "AssertDescription" : "For the test environment, the instance type must be
 m1.small"
      }
    ]
  },
  "prodInstanceType" : {
    "RuleCondition" : {"Fn::Equals":[{"Ref":"Environment"}, "prod"]},
    "Assertions" : [
      {
        "Assert" :  { "Fn::Contains" : [ ["m1.large"], {"Ref" : "InstanceType"} ] },
        "AssertDescription" : "For the prod environment, the instance type must be
 m1.large"
      }
    ]
  }
}
```

AWS Service Catalog 服務動作

> **Note**
>
> AWS Service Catalog不支援地形開放原始碼或地形雲端產品的服務動作。

AWS Service Catalog 可讓您減少管理維護和最終使用者訓練，同時遵守合規和安全措施。身為管理員的您可借助服務動作讓最終使用者執行操作式任務、排除問題、執行核准的命令，或在 AWS Service Catalog 中請求許可。您可以使用 AWS Systems Manager 文件 定義服務動作。這些AWS Systems Manager文件可讓您存取實作AWS最佳實務的預先定義動作，例如 Amazon EC2 停止和重新開機，您也可以定義自訂動作。

在本教學中，您可以為最終使用者提供重新啟動 Amazon EC2 執行個體的功能。您新增必要的許可、定義服務動作、為服務動作與產品建立關聯，以及透過佈建的產品，利用動作來測試最終使用者體驗。

必要條件

此教學課程假設您具有完整的 AWS 管理員權限，您已熟悉 AWS Service Catalog，而且您已有一組基本產品、產品組合及使用者。如果您不熟悉 AWS Service Catalog，請先完成設定和開始任務，再使用此教學課程。

主題

- 步驟 1：設定最終使用者許可
- 步驟 2：建立服務動作
- 步驟 3：將服務動作與產品版本建立關聯
- 步驟 4：測試最終使用者體驗
- 步驟 5：管理服務動作 AWS CloudFormation
- 步驟 6：疑難排解

步驟 1：設定最終使用者許可

使用者必須具備檢視及執行特定服務動作的必要權限。在此範例中，最終使用者需要許可才能存取AWS Service Catalog服務動作功能和執行 Amazon EC2 重新啟動。

更新權限

1. 開啟 AWS Identity and Access Management (IAM) 主控台，網址為 https://console.aws.amazon.com/iam/。
2. 從功能表中找出使用者群組。
3. 選擇最終使用者將用來存取AWS Service Catalog資源的群組。在這個範例中，我們選擇最終使用者群組。在您自己的實作中，選擇相關的最終使用者所使用的群組。

4. 在群組的詳細資訊頁面的 Permissions (許可) 標籤上，可以建立新政策，或編輯現有的政策。在這個範例中，我們透過選取為群組的 AWS Service Catalog 佈建和終止許可而建立的自訂政策，將許可權加入到現有政策。
5. 在 Policy (政策) 頁面上，選擇 Edit Policy (編輯政策) 以新增必要的許可。您可以使用視覺化編輯器或 JSON 編輯器來編輯政策。在這個範例中，我們使用 JSON 編輯器來新增權限。對於此教學課程，將下列政策加入到許可中：

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "Stmt1536341175150",
   "Action": [
    "servicecatalog:ListServiceActionsForProvisioningArtifact",
    "servicecatalog:ExecuteprovisionedProductServiceAction",
    "ssm:DescribeDocument",
    "ssm:GetAutomationExecution",
    "ssm:StartAutomationExecution",
    "ssm:StopAutomationExecution",
    "cloudformation:ListStackResources",
    "ec2:DescribeInstanceStatus",
    "ec2:StartInstances",
    "ec2:StopInstances"
   ],
   "Effect": "Allow",
   "Resource": "*"
  }
 ]
}
```

6. 在編輯政策後，審核及核准政策的變更。最終使用者群組中的使用者現在具有在中執行 Amazon EC2 重新啟動動作的必要許可AWS Service Catalog。

步驟 2：建立服務動作

接下來，建立服務動作以重新啟動 Amazon EC2 執行個體。

1. 開啟主AWS Service Catalog控台，網址為 https://console.aws.amazon.com/sc/。
2. 從功能表中選擇 Service actions (服務動作)。

3. 在 [服務動作] 頁面上，選擇 [建立動作]。
4. 在 Create action (建立動作) 頁面中，選擇 AWS Systems Manager 文件來定義服務動作。Amazon EC2 執行個體重新啟動動作由AWS Systems Manager文件定義，因此我們將預設選項保留在 Amazon 文件下拉式功能表上。
5. 搜尋並選擇-重新啟動 C2 執AWS行個體動作。
6. 提供符合您環境和團隊動作的名稱和描述。最終使用者將會看到此描述，因此選擇可協助他們了解動作的選項。
7. 在「參數和目標組態」下，選擇將成為動作目標的 SSM 文件參數 (例如，執行個體 ID)，然後選擇參數的目標。選擇 Add parameter (新增參數) 以新增其他參數。
8. 在 Permissions (許可) 下，選擇角色。我們為此範例使用預設的許可。此頁面可設定及定義其他許可組態。
9. 檢閱組態之後，可選擇 Create action (建立動作)。
10. 到了下一頁，當建立好動作並準備好開始使用時，出現確認訊息。

步驟 3：將服務動作與產品版本建立關聯

在您定義動作後，您必須為產品與該動作建立關聯。

1. 在 [服務動作] 頁面上，選擇 AWS-重新啟動 C2 執行個體，然後選擇 [關聯動作]。
2. 在 Associate action (關聯動作) 頁面，選擇您希望您的最終使用者採取服務動作的產品。在這個範例中，我們選擇 Linux Desktop (Linux 桌面)。
3. 選擇產品版本。請注意，您可以使用最上面的核取方塊來選取所有的版本。
4. 選擇 Associate action (建立關聯)。
5. 在下一頁出現確認訊息。

現在您已經在 AWS Service Catalog 建立服務動作。此教學課程的下一步是以最終使用者身分使用服務動作。

步驟 4：測試最終使用者體驗

最終使用者可以在佈建的產品上執行服務動作。基於此教學課程的目的，最終使用者必須至少有一項佈建的產品。已佈建產品應該從您在之前步驟與服務動作關聯之產品版本啟動。

以最終使用者身分存取服務動作

1. 以最終使用者身分登入 AWS Service Catalog主控台。
2. 在導覽窗格的 AWS Service Catalog 儀表板上，選擇 Provisioned products list (佈建產品清單)。此清單會顯示為最終使用者帳戶佈建的產品。
3. 在 Provisioned products list (佈建產品清單) 頁面上，選擇已佈建的執行個體。
4. 在 [佈建的產品詳細資訊] 頁面上，選擇右上角的 [動作]，然後選擇 AWS-Restar teC2 執行個體動作。
5. 確認您要執行自訂動作。您收到確認表示動作已傳送。

步驟 5：管理服務動作 AWS CloudFormation

您可以建立服務動作及其與AWS CloudFormation資源的關聯。如需詳細資訊，請參閱《AWS CloudFormation 使用者指南》 中的下列主題：

- AWS::ServiceCatalog::CloudFormation产品 ProvisioningArtifactProperties
- AWS::ServiceCatalog::ServiceAction協會

> **Note**
>
> 如果您管理與AWS CloudFormation資源的服務動作關聯，請勿透過或新增或移除服務動作 AWS Management Console。AWS Command Line Interface當您執行堆疊更新時，會取代在以外對服務動作所做的AWS CloudFormation任何變更。

步驟 6：疑難排解

如果您的服務動作執行失敗，您可以在「已佈建的產品」頁面上服務動作執行事件的「輸出」區段中找到錯誤訊息。您可以在下方看到常見錯誤訊息的說明。

> **Note**
>
> 錯誤消息的確切文本可能會改變，因此您應該避免在任何類型的自動化過程中使用這些文本。

內部錯誤

AWS Service Catalog 發生內部錯誤。請稍後再試。如果問題持續發生，請聯絡客戶支援。

調用 StartAutomationExecution 操作時ThrottlingException發生錯誤（ ）

後端服務 (例如 SSM) 限制了服務動作執行。

假設角色時拒絕存取

AWS Service Catalog 無法承擔服務動作定義中指定的角色。請確定服務主體或區域主體，例如服務卡塔洛 .US 東部 -1.amazonaws.com，允許列在角色的信任原則中。

呼叫 StartAutomationExecution 作業時發生錯誤 (AccessDeniedException)：使用者未授權在資源 StartAutomationExecution 上執行:ssm:。

在服務動作定義中指定的角色沒有叫用 ssm: StartAutomationExecution 的權限。請確定角色具有適當的 SSM 權限。

TargetType在已佈建產品中找不到任何具有類型的資源

佈建的產品不包含符合 SSM 文件中指定之目標類型的任何資源，例如:: EC2:AWS: 執行個體。請檢查佈建的產品是否有這些資源，或確認文件是否正確。

具有該名稱的文件不存在

服務動作定義中指定的文件不存在。

無法描述 SSM 自動化文件

AWS Service Catalog嘗試描述指定的文件時，發生來自 SSM 的未知例外狀況。

無法擷取角色的認證

假設指定的角色時 AWS Service Catalog 遇到未知的錯誤。

參數的值 "***InvalidValue***" 在 ***{ValidValue1} #####{ValidValue2}***

傳遞給 SSM 的參數值不在文件的允許值清單中。確認提供的參數有效，然後再試一次。

參數類型錯誤。提供的值不***ParameterName***是有效的字串。

傳遞給 SSM 的參數值不適用於文件上的類型。

未在服務動作定義中定義參數

參數傳遞給未在服務動作定義中定義的 AWS Service Catalog。您只能使用在服務動作定義中定義的參數。

步驟在執行/取消動作時失敗。*#####*請參閱自動化服務疑難排解指南以取得更多診斷詳情。

SSM 自動化文件中的步驟失敗。請參閱訊息中的錯誤，以進一步疑難排解。

不允許使用下列參數值，因為它們不在佈建的產品中：*InvalidResourceId*

使用者要求對不在佈建產品中的資源執行動作。

TargetType 未針對 SSM 自動化文件定義

服務動作需要有 TargetType 定義的 SSM 自動化文件。檢查您的 SSM 自動化文件。

將 AWS Marketplace 產品新增至產品組合

您可以將 AWS Marketplace 產品新增至產品組合，以讓那些產品可供 AWS Service Catalog 最終使用者使用。

AWS Marketplace 是您可在其中尋找、訂閱，與使用大量軟體與服務選項而啟動的線上商店。AWS Marketplace 中的產品類型包含資料庫、應用程式伺服器、測試工具、監控工具、內容管理工具和商業智慧軟體。AWS Marketplace 可用於 https://aws.amazon.com/marketplace。請注意，您無法將軟體即服務 (SaaS) 產品從新增AWS Marketplace至AWS Service Catalog。

您可以將AWS Marketplace產品與AWS CloudFormation範本複製到，然後將產品新增至產品組合AWS Service Catalog，藉此將產品散佈給AWS Service Catalog最終使用者。

> **Note**
>
> AWS Service Catalog不支援使用 Terraform 開放原始碼或 Terraform 雲AWS Service Catalog端AWS Marketplace產品範本將產品散發給終端使用者。

AWS Marketplace 直接支援 AWS Service Catalog 或使用手動選項訂閱和新增產品。我們建議使用為 AWS Service Catalog 特別設計的功能來新增產品。

使用 AWS Service Catalog 管理 AWS Marketplace 產品

您可以使用自訂介面直接將訂閱的 AWS Marketplace 產品新增至 AWS Service Catalog。在 AWS Marketplace 中，選擇 Service Catalog (服務目錄)。如需詳細資訊，請參閱「AWS Marketplace說明和常見問題集」AWS Service Catalog 中的「將產品複製到

手動管理與新增 AWS Marketplace 產品

完成下列步驟即可訂閱AWS Marketplace產品、在AWS CloudFormation範本中定義該產品，並將範本新增至學AWS Service Catalog檔。

訂閱 AWS Marketplace 產品

1. 在 AWS Marketplace 前往 https://aws.amazon.com/marketplace。
2. 瀏覽該產品或搜尋以尋找您要新增至 AWS Service Catalog 產品組合的產品。選擇產品以檢視產品詳細資訊頁面。
3. 選擇「繼續」以檢視出貨頁面，然後選擇「手動啟動」頁標。

   履行頁面上的資訊包括支援的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體類型AWS區域、支援的執行個體類型，以及產品在每個AWS區域使用的 Amazon 機器映像 (AMI) ID。請注意，部分選擇將會影響成本。您將使用此資訊以在稍後步驟自訂 AWS CloudFormation 範本。
4. 選擇 [接受條款] 以訂閱該產品。

   在訂閱產品後，您可以選擇 [AWS Marketplace您的軟體]，然後選擇該產品以隨時存取在 中產品履行頁面上的資訊。

在 AWS CloudFormation 範本中定義 AWS Marketplace 產品

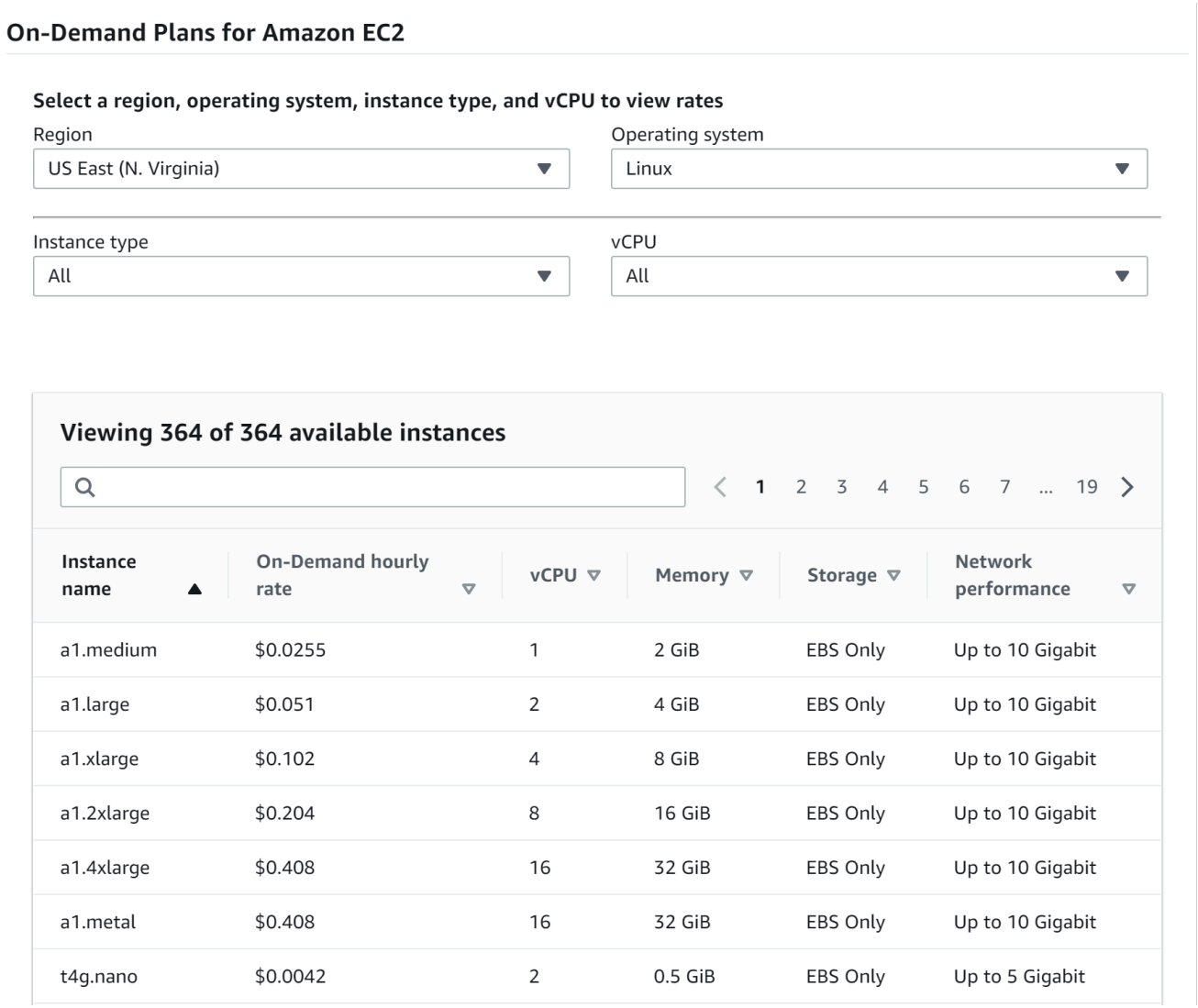
若要完成以下步驟，您將使用其中一個 AWS CloudFormation 範例範本做為開始點，然後您將自訂範本，讓其呈現 AWS Marketplace 產品。若要存取範例範本，請參閱 https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cfn-sample-templates.html 使用者指南中的AWS CloudFormation範例範本。

1. 在「AWS CloudFormation使用者指南」的「範例範本」頁面上，選擇產品的「AWS地區」。您的AWS Marketplace產品必須支援該AWS地區。您可以在 AWS Marketplace 的產品履行頁面上檢視受支援的區域。
2. 若要檢視適用於「區域」的服務範例範本清單，請選擇「服務」連結。
3. 您可以使用任何適合您需求的範本做為開始點。在此程序中的步驟使用安全群組中的 Amazon EC2 執行個體範本。若要檢視範例範本，請選擇 [檢視]，然後將範本副本儲存在本機，如此您就可以進行編輯。您的本機檔案必須擁有 `.template` 延伸模組。
4. 在文字編輯器中開啟範本檔案。
5. 在範本頂部自訂說明。您的說明看起來可能會與以下範例類似：

```
"Description": "Launches a LAMP stack from AWS Marketplace",
```

6. 自訂 InstanceType 參數，讓其僅包含受您產品支援的 EC2 執行個體類型。若您的範本包含未受支援的 EC2 執行個體類型，產品將會無法為最終使用者啟動。

   a. 在的產品履行頁面上AWS Marketplace，在「定價詳細資訊」區段中檢視支援的 EC2 執行個體類型。



On-Demand Plans for Amazon EC2

Select a region, operating system, instance type, and vCPU to view rates

Region: US East (N. Virginia) | Operating system: Linux

Instance type: All | vCPU: All

Viewing 364 of 364 available instances

1 2 3 4 5 6 7 ... 19

Instance name	On-Demand hourly rate	vCPU	Memory	Storage	Network performance
a1.medium	$0.0255	1	2 GiB	EBS Only	Up to 10 Gigabit
a1.large	$0.051	2	4 GiB	EBS Only	Up to 10 Gigabit
a1.xlarge	$0.102	4	8 GiB	EBS Only	Up to 10 Gigabit
a1.2xlarge	$0.204	8	16 GiB	EBS Only	Up to 10 Gigabit
a1.4xlarge	$0.408	16	32 GiB	EBS Only	Up to 10 Gigabit
a1.metal	$0.408	16	32 GiB	EBS Only	Up to 10 Gigabit
t4g.nano	$0.0042	2	0.5 GiB	EBS Only	Up to 5 Gigabit

   b. 在您的範本中，將預設執行個體類型變更為您選擇的受支援 EC2 執行個體類型。

   c. 編輯 AllowedValues 清單，讓其僅包含受您產品支援的 EC2 執行個體類型。

   d. 移除任何您不希望最終使用者在從 AllowedValues 清單中啟動產品時使用的 EC2 執行個體類型。

   在編輯 InstanceType 參數時，其看起來可能會與以下範例類似：

```
    "InstanceType" : {
      "Description" : "EC2 instance type",
      "Type" : "String",
      "Default" : "m1.small",
      "AllowedValues" : [ "t1.micro", "m1.small", "m1.medium", "m1.large",
"m1.xlarge", "m2.xlarge", "m2.2xlarge", "m2.4xlarge", "c1.medium", "c1.xlarge",
"c3.large", "c3.large", "c3.xlarge", "c3.xlarge", "c3.4xlarge", "c3.8xlarge" ],
      "ConstraintDescription" : "Must be a valid EC2 instance type."
    },
```

7. 在範本的 Mappings 區段中，編輯 AWSInstanceType2Arch 對應，如此僅包含受支援的 EC2 執行個體類型與基礎結構。

   a. 透過移除 AllowedValues 參數 InstanceType 清單中不包含的所有 EC2 執行個體類型，編輯對應清單。

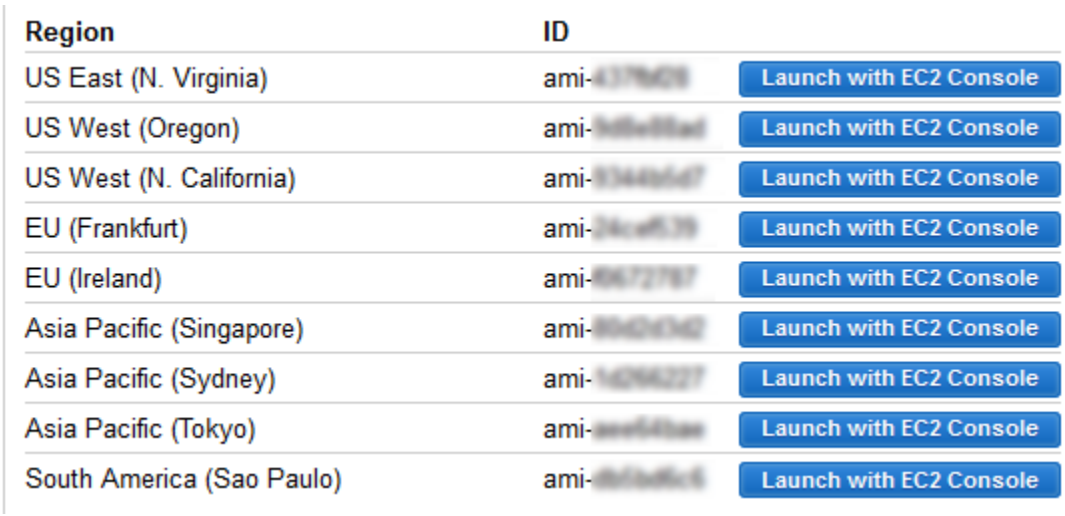
   b. 為每個要成為基礎結構類型的 EC2 執行個體類型編輯 Arch 值，該基礎結構類型會受您產品的支援。有效值為 PV64、HVM64 和 HVMG2。若要了解您產品支援哪些基礎結構，請參閱 AWS Marketplace 中的產品詳細資訊。若要了解 EC2 執行個體系列支援哪些基礎結構，請參閱 Amazon Linux AMI 執行個體類型矩陣。

   在您完成編輯 AWSInstanceType2Arch 對應時，其看起來可能會與以下範例類似：

```
    "AWSInstanceType2Arch" : {
      "t1.micro"    : { "Arch" : "PV64"  },
      "m1.small"    : { "Arch" : "PV64"  },
      "m1.medium"   : { "Arch" : "PV64"  },
      "m1.large"    : { "Arch" : "PV64"  },
      "m1.xlarge"   : { "Arch" : "PV64"  },
      "m2.xlarge"   : { "Arch" : "PV64"  },
      "m2.2xlarge"  : { "Arch" : "PV64"  },
      "m2.4xlarge"  : { "Arch" : "PV64"  },
      "c1.medium"   : { "Arch" : "PV64"  },
      "c1.xlarge"   : { "Arch" : "PV64"  },
      "c3.large"    : { "Arch" : "PV64"  },
      "c3.xlarge"   : { "Arch" : "PV64"  },
      "c3.2xlarge"  : { "Arch" : "PV64"  },
      "c3.4xlarge"  : { "Arch" : "PV64"  },
      "c3.8xlarge"  : { "Arch" : "PV64"  }
    }
,
```

8. 在範本區Mappings段中，編輯AWSRegionArch2AMI對應，將每個AWS區域與產品的對應架構和 AMI ID 建立關聯。

   a. 在中的產品出貨頁面上AWS Marketplace，檢視產品在每個AWS區域使用的 AMI ID，如下列範例所示：



Region	ID	
US East (N. Virginia)	ami-	Launch with EC2 Console
US West (Oregon)	ami-	Launch with EC2 Console
US West (N. California)	ami-	Launch with EC2 Console
EU (Frankfurt)	ami-	Launch with EC2 Console
EU (Ireland)	ami-	Launch with EC2 Console
Asia Pacific (Singapore)	ami-	Launch with EC2 Console
Asia Pacific (Sydney)	ami-	Launch with EC2 Console
Asia Pacific (Tokyo)	ami-	Launch with EC2 Console
South America (Sao Paulo)	ami-	Launch with EC2 Console

   b. 在範本中，移除您不支援的任何AWS區域的對應。

   c. 為每個區域編輯對應以移除未受支援的基礎結構 (PV64、HVM64 或 HVMG2) 和其關聯的 AMI ID。

   d. 對於每個剩餘的AWS區域和架構對應，請從中的產品詳細資訊頁面指定對應的 AMI ID AWS Marketplace。

當您完成編輯 AWSRegionArch2AMI 對應時，您的程式碼看起來可能與以下範例類似：

```
"AWSRegionArch2AMI" : {
  "us-east-1"        : {"PV64" : "ami-nnnnnnnn"},
  "us-west-2"        : {"PV64" : "ami-nnnnnnnn"},
  "us-west-1"        : {"PV64" : "ami-nnnnnnnn"},
  "eu-west-1"        : {"PV64" : "ami-nnnnnnnn"},
  "eu-central-1"     : {"PV64" : "ami-nnnnnnnn"},
  "ap-northeast-1"   : {"PV64" : "ami-nnnnnnnn"},
  "ap-southeast-1"   : {"PV64" : "ami-nnnnnnnn"},
  "ap-southeast-2"   : {"PV64" : "ami-nnnnnnnn"},
  "sa-east-1"        : {"PV64" : "ami-nnnnnnnn"}
}
```

您現在可以使用範本將產品新增至產品AWS Service Catalog組合。如果您希望進行其他變更，請參閱使用 AWS CloudFormation 範本以進一步了解範本的詳細資訊。

若要將您的AWS Marketplace產品新增至產品AWS Service Catalog組合

1. 登入AWS Management Console並瀏覽至AWS Service Catalog管理員主控台，網址為 https://console.aws.amazon.com/servicecatalog/。
2. 在「產品組合」頁面上，選擇您要新增AWS Marketplace產品的產品組合。
3. 在產品組合詳細資料頁面上，選擇 [上傳新產品]。
4. 輸入要求的產品與支援的詳細資訊。
5. 在 [版本詳細資訊] 頁面中，依序選擇 [上傳範本檔案]、[瀏覽] 然後選擇範本檔案。
6. 輸入版本標題與說明。
7. 選擇下一步。
8. 在 [檢閱] 頁面上，確認摘要是否正確，然後選擇 [確認並上傳]。該產品會新增至您的產品組合。有權存取產品組合的最終使用者即可使用。

使用 AWS CloudFormation StackSets

> **Note**
>
> AutoTags 目前不支援AWS CloudFormation StackSets。

您可以使AWS CloudFormation StackSets 用跨多個帳戶AWS 區域和帳戶啟動AWS Service Catalog產品。您可以指定產品在其中依序部署的順序AWS 區域。在多個帳戶中，產品為平行部署。啟動時，使用者可指定容錯能力和最大帳戶數量，以用來進行部署。如需詳細資訊，請參閱使用 AWS CloudFormation StackSets。

堆疊集與堆疊執行個體

堆疊集可讓您使用單一AWS CloudFormation範本在不同AWS區域的AWS帳戶中建立堆疊。

堆棧實例是指一個AWS區域內的目標帳戶中的堆棧，並且僅與一個堆棧集關聯。

如需詳細資訊，請參閱 StackSets 概念。

堆疊集限制

AWS Service Catalog 中，您可以使用堆疊集限制來設定產品的部署選項。

AWS Service Catalog支持兩種產品的堆棧集約束AWS GovCloud (US) Regions：AWS GovCloud（美國西部）和 AWS GovCloud （美國東部）。

如需詳細資訊，請參閱 < AWS Service Catalog堆疊集合約束 > 。

管理預算

您可以使用 AWS 預算在 AWS Service Catalog 中追蹤您的服務成本和用量。您可以將預算與 AWS Service Catalog 產品和產品組合建立關聯。

> **Note**
>
> AWS Service Catalog不支援 Terraform 開放原始碼產品的預算。

AWS 預算可讓您設定自訂預算，並在成本或用量超過 (或是預測超過) 預算金額時提醒您。如需 AWS 預算的詳細資訊，請參閱https://aws.amazon.com/aws-cost-management/aws-budgets。

任務

- 必要條件
- 建立預算
- 關聯預算
- 檢視預算
- 取消關聯預算

必要條件

使用 AWS 預算之前，您需要在 AWS Billing and Cost Management 主控台中啟用成本分配標籤。如需詳細資訊，請參閱《AWS Billing and Cost Management 使用者指南》中的啟用使用者定義的成本分配標籤。

> **Note**
>
> 標籤最多需要 24 小時才能啟用。

您也需要為將使用預算功能的任何使用者或群組，啟用 AWS Billing and Cost Management 主控台的使用者存取權。您可以為使用者建立新的政策來執行此作業。

若要允許 使用者建立預算，您也必須允許使用者檢視帳單資訊。如果您想要使用 Amazon SNS 通知，可以讓使用者建立 Amazon SNS 通知，如以下政策範例所示。

建立預算政策

1. 開啟位於 https://console.aws.amazon.com/iam/ 的 IAM 主控台。
2. 在導覽窗格上選擇 Policies (政策)。
3. 在內容窗格中，選擇 Create policy (建立政策)。
4. 選擇 JSON 標籤並從下列 JSON 政策文件複製文字。將此文字貼上至 JSON 文字方框中。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1435216493000",
            "Effect": "Allow",
            "Action": [
                "aws-portal:ViewBilling",
                "aws-portal:ModifyBilling",
                "budgets:ViewBudget",
                "budgets:ModifyBudget"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "Stmt1435216552000",
            "Effect": "Allow",
            "Action": [
                "sns:*"
            ],
```

```
            "Resource": [
                "arn:aws:sns:us-east-1"
            ]
        }
    ]
}
```

5. 完成時，選擇 Review policy (檢閱政策)。Policy Validator (政策檢查工具) 會回報任何語法錯誤。
6. 在 Review (檢閱) 頁面上，為您的政策命名。檢閱政策 Summary (摘要) 以查看政策授予的許可，然後選擇 Create policy (建立政策) 來儲存您的工作。

   新的政策會出現在受管政策清單中，並且已準備好連接至您的使用者和群組。如需詳細資訊，請參閱AWS Identity and Access Management使用指南中的建立和附加客戶管理策略。

建立預算

在AWS Service Catalog管理員主控台中，「產品清單」和「產品組合」頁面會列出現有產品和產品組合的相關資訊，並可讓您對其採取動作。若要建立預算，請先決定要與預算產生關聯的產品或產品組合。

若要建立預算

1. 在 https://console.aws.amazon.com/servicecatalog/ 開啟 Service Catalog 主控台。
2. 選擇產品列表或產品組合。
3. 選取您要新增預算的產品或產品組合。
4. 開啟「作業」功能表，然後選擇「建立預算」。
5. 在 Budget creation (預算建立) 頁面上，將一種標籤類型與預算建立關聯。

   有兩種類型的標籤： AutoTags 和 TagOptions。 AutoTags 識別啟動產品的產品組合、產品和使用者。 AWS Service Catalog將這些標籤自動套用至已佈建的資源。A TagOption 是在中管理的系統管理員定義的索引鍵值組。AWS Service Catalog

   為了讓產品組合或產品上的花費能夠反映相關預算，它們必須擁有相同的標籤。請注意，第一次使用的標籤鍵可能需要 24 小時才能啟用。如需詳細資訊，請參閱 the section called “必要條件”。
6. 選擇「建立於」AWS Budgets。系統會將您導向至「設定預算」頁面。依照建立預算中的步驟，繼續設定預算。

> **Note**
>
> 建立預算之後，您必須將其與產品或產品組合產生關聯。

關聯預算

每個產品組合或產品都可以有一個與其相關聯的預算。每個預算可以與多個產品組合和產品相關聯。

當您將預算與產品組合或產品建立關聯時，即可從該產品組合或產品的詳細資訊頁面檢視預算的相關資訊。為了讓投資組合或產品發生的支出能夠反映在預算上，您必須在預算和投資組合或產品上建立相同的標籤關聯。

> **Note**
>
> 如果您從中刪除預算AWS Budgets，則與AWS Service Catalog產品和產品組合的現有關聯仍然存在。 AWS Service Catalog將無法顯示有關已刪除預算的任何信息。

關聯預算

1. 在 https://console.aws.amazon.com/servicecatalog/ 開啟 Service Catalog 主控台。
2. 選擇產品列表或產品組合。
3. 選取您要與預算產生關聯的產品或產品組合。
4. 開啟「作業」功能表，然後選擇「關聯預算」。
5. 在「預算關聯」頁面上，選取現有預算，然後選擇「繼續」。
6. 產品或產品組合表格現在會包含您剛新增預算的資料。

檢視預算

如果預算與產品相關聯，您可以在「產品詳細資訊」與「產品清單」頁面上檢視預算的相關資訊。如果預算與投資組合相關聯，您可以在「投資組合」和「投資組合」詳細資訊頁面上檢視預算的相關資訊。

「組合」與「產品清單」頁面會顯示現有資源的預算資訊。您可以看到顯示 Current vs. budget (目前與預算) 和 Forecast vs. budget (預測與預算) 的欄。

當您選擇產品或產品組合時，系統會將您導向至詳細資料頁面。「產品組合詳細資訊」和「產品詳細資訊」頁面包含相關預算的詳細資訊的區段 您可以查看預算金額、目前花費和預測費用。您也可以選擇檢視預算詳細資訊以及編輯預算。

取消關聯預算

您可以取消預算與產品組合或產品的關聯。

> **Note**
>
> 如果您從「預算」刪除AWS預算，與AWS Service Catalog產品和產品組合的現有關聯仍然存在。 AWS Service Catalog將無法顯示有關已刪除預算的任何信息。

取消關聯預算

1. 在 https://console.aws.amazon.com/servicecatalog/ 開啟 Service Catalog 主控台。
2. 選擇產品列表或產品組合。
3. 選取您要取消預算關聯的產品或產品組合。
4. 選擇動作。從下拉式清單中選擇「取消預算關聯」。確認警示隨即出現。
5. 確認要取消產品或產品組合的預算之後，請選擇「確認」。

管理佈建產品

AWS Service Catalog 提供界面以供管理佈建產品。您可以根據存取層級為目錄檢視、更新以及終止所有佈建產品。請參考下列章節的範例程序。

主題

以管理員身分管理已佈建產品

若要管理帳戶的所有佈建產品，您必須具有`AWSServiceCatalogAdminFullAccess`或同等的 IAM 權限，才能存取已佈建的產品寫入作業。如需詳細資訊，請參閱 AWS Service Catalog中的 Identity and Access Management。

> **Tip**
>
> 對於靜態佈建的產品鏈結，在佈建產品之前，您必須參考產品成品範本中已佈建的產品輸出。如需包括範例在內的詳細資訊，請參閱下列內容：
>
> - AWS::ServiceCatalog::CloudFormationProvisionedProduct (在 AWS CloudFormation 使用者指南中)
> - DescribeProvisioningParameters (ProvisioningArtifactOutputKeys) 在AWS Service Catalog開發人員指南中。

檢視並管理所有佈建產品

1. 請在以下位置開啟AWS Service Catalog主控台。 https://console.aws.amazon.com/servicecatalog/

   如果您已經登入AWS Service Catalog主控台，請選擇 Service Catalog，然後選擇使用者。

2. 如有必要，請向下捲動至佈建的產品區段。
3. 在「啟動設定的產品」段落中，選擇檢視：清單，然後選取您要查看的存取層級：使用者、角色或帳戶。此動作會顯示目錄中所有佈建的產品。
4. 選擇佈建產品，以檢視、更新或終止。如需更多有關此檢視中提供的資訊，請參閱 Viewing Provisioned Product Information (檢視佈建產品資訊)。

變更佈建產品擁有者

您可以隨時變更佈建產品的擁有者。您必須知道要設為新擁有者之使用者或角色的 ARN。

根據預設，使用`AWSServiceCatalogAdminFullAccess`受管理策略的管理員可以使用此功能。您可以在 AWS Identity and Access Management (IAM) 中授予最終使用者`servicecatalog:UpdateProvisionedProductProperties`權限來為使用者啟用此功能。

變更佈建產品的擁有者

1. 在 AWS Service Catalog 主控台中，選擇 Provisioned products list (佈建產品清單)。
2. 找到您要更新的佈建產品，然後選擇其旁邊的三個點，然後選擇「變更佈建的產品擁有者」。您也可以在授權產品的詳細資訊頁面的 「動作」功能表中找到「變更擁有者」選項。
3. 在對話方塊中，請輸入要設為新擁有者之使用者或角色的 ARN。ARN 以 `arn:` 為開頭，並包括以冒號或斜線分隔的其他資訊，例如 `arn:aws:iam::123456789012:user/NewOwner`。
4. 選擇提交。更新擁有者後，您將會看到成功訊息。

另請參閱

- UpdateProvisionedProductProperties

更新已佈建產品的範本

您可以將已佈建產品的目前範本變更為其他範本。例如，如果您在 Service Catalog 中有 EC2 產品，則可以更新該 EC2 產品以保留相同的佈建產品 ID，但將範本變更為 S3 儲存貯體。

> **Note**
>
> 已佈建的 Terraform 開放原始碼或 Terraform 雲端產品不支援更新範本。如果您要為現有的 Terraform 產品使用不同的範本，您必須刪除該產品，然後使用所需的範本建立新產品。

若要更新已佈建產品的範本

1. 在左側導覽功能表中，選擇已佈建的產品。
2. 在佈建的產品中，選擇已佈建的產品，然後選取動作，更新。

   請注意，您也可以在已佈建的產品詳細資訊頁面中選取動作、更新。
3. (選擇性) 在產品詳細資訊中，選擇 [變更產品]。

   在變更產品中，請注意以下警告：

   變更產品會將此佈建的產品更新為不同的產品範本。這可能會終止資源並建立新資源。

   您可以將已佈建的產品更新為相同產品中的不同版本。
4. (選擇性) 在「產品」中，選擇您要使用不同範本更新的產品。然後選擇「更改」。

   在產品詳細資訊中，請注意以下警告：

   [產品名稱] 將從 [當前模板名稱] 更新為 [新模板名稱]。但是，您已佈建產品的名稱 [佈建產品名稱] 不會變更。

   您可以將已佈建的產品更新為相同產品中的不同版本。
5. 在產品版本中，選擇您想要的產品版本。
6. 在參數中，選擇適當的參數。
7. 選擇更新。

   在佈建的產品詳細資料中，您可以查看更新的詳細資料。佈建的產品名稱不會變更，但佈建的產品現在具有不同的範本。

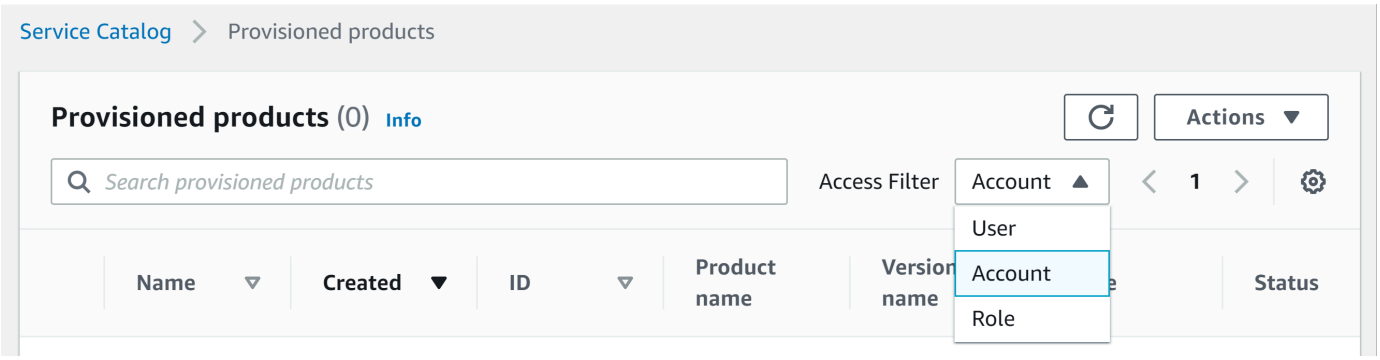
教學：識別使用者資源分配

您可以識別使用 AWS Service Catalog 主控台產品關聯佈建產品與資源的使用者。本教學可協助將此範例翻譯為您自己特定的佈建產品。

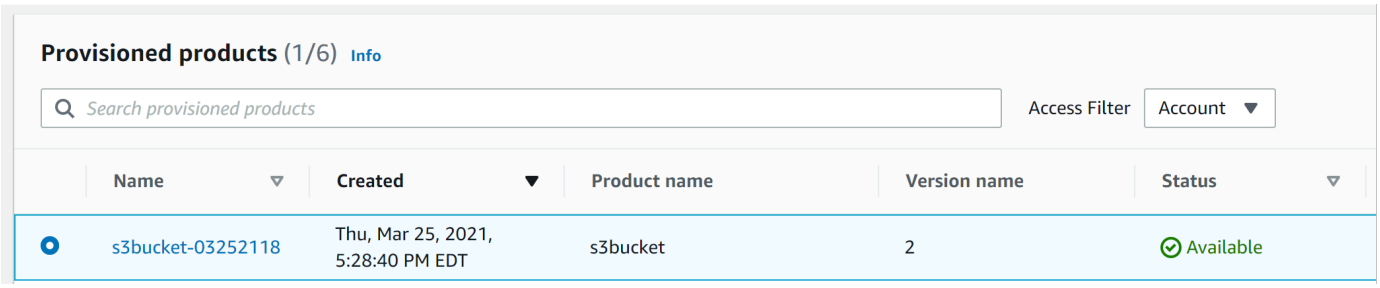
若要管理帳戶所有的佈建產品，您需 AWSServiceCatalogAdminFullAccess 或佈建產品寫入操作的相同存取。如需詳細資訊，請參閱《管理指南》中的AWS Service Catalog〈Identity and Access Management〉

為了識別佈建產品及相關資源的使用者

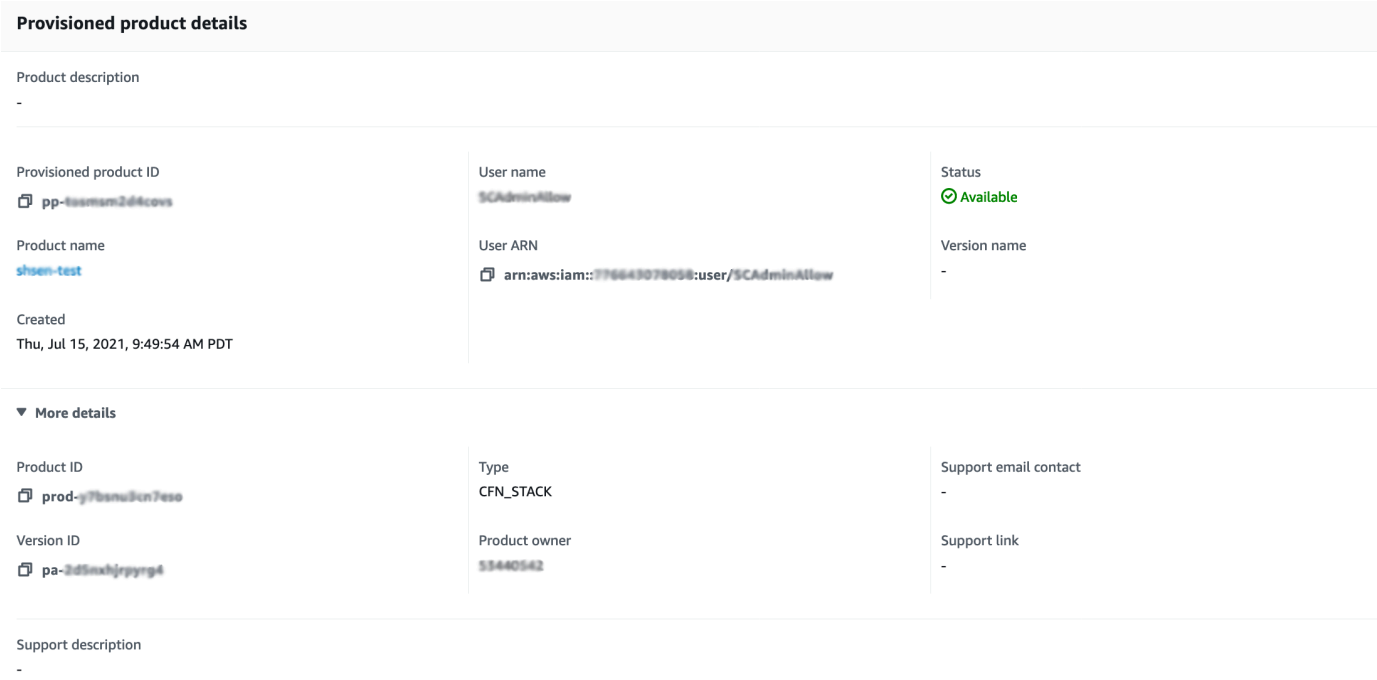
1. 打開以下位置。https://console.aws.amazon.com/servicecatalog
2. 在左側導覽功能表中，選擇已佈建的產品。
3. 在 [存取篩選] 下拉式選單中，選擇 [帳戶]。



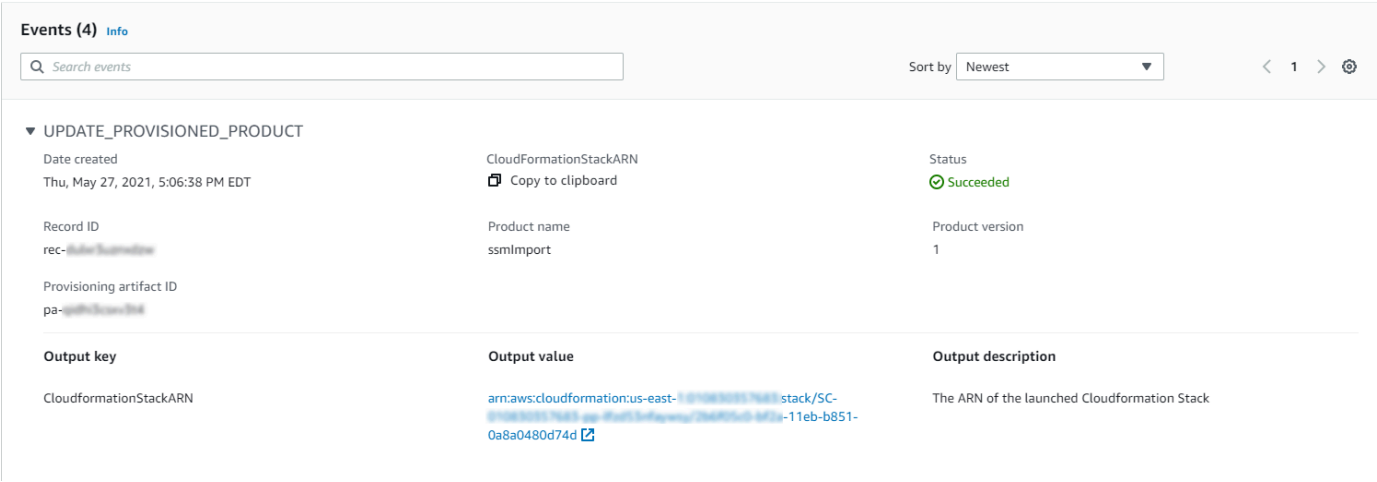
4. 在帳戶檢視中，選擇並開啟已佈建的產品以顯示其詳細資訊。



您可以查看已佈建產品的詳細資訊。



5. 向下捲動以展開「事件」區段。請注意Provisioned product ID和CloudformationStackARN值。



6. 使用佈建的產品 ID 來識別與此次啟動對應的AWS CloudTrail記錄，並識別要求的使用者 (通常是您在聯合期間輸入電子郵件地址)。在此範例中為「steve」。

```
{
  "eventVersion":"1.03","userIdentity":
  {
    "type":"AssumedRole",
    "principalId":"[id]:steve",
    "arn":"arn:aws:sts::[account number]:assumed-role/SC-usertest/steve",
    "accountId":[account number],
```

```
    "accessKeyId":[access key],
    "sessionContext":
    {
      "attributes":
      {
        "mfaAuthenticated":[boolean],
        "creationDate":[timestamp]
      },
      "sessionIssuer":
      {
        "type":"Role",
        "principalId":"AROAJEXAMPLELH3QXY",
        "arn":"arn:aws:iam::[account number]:role/[name]",
        "accountId":[account number],
        "userName":[username]
      }
    }
  },
  "eventTime":"2016-08-17T19:20:58Z","eventSource":"servicecatalog.amazonaws.com",
  "eventName":"ProvisionProduct",
  "awsRegion":"us-west-2",
  "sourceIPAddress":[ip address],
  "userAgent":"Coral/Netty",
  "requestParameters":
  {
    "provisioningArtifactId":[id],
    "productId":[id],
    "provisioningParameters":[Shows all the parameters that the end user entered],
    "provisionToken":[token],
    "pathId":[id],
    "provisionedProductName":[name],
    "tags":[],
    "notificationArns":[]
  },
  "responseElements":
  {
    "recordDetail":
    {
      "provisioningArtifactId":[id],
      "status":"IN_PROGRESS",
      "recordId":[id],
      "createdTime":"Aug 17, 2016 7:20:58 PM",
      "recordTags":[],
      "recordType":"PROVISION_PRODUCT",
```

```
      "provisionedProductType":"CFN_STACK",
      "pathId":[id],
      "productId":[id],
      "provisionedProductName":"testSCproduct",
      "recordErrors":[],
      "provisionedProductId":[id]
    }
  },
  "requestID":[id],
  "eventID":[id],
  "eventType":"AwsApiCall",
  "recipientAccountId":[account number]
}
```

7. 使用此CloudformationStackARN值來識別AWS CloudFormation事件，以尋找有關已建立資源的資訊。您也可以使用 AWS CloudFormation API 取得此資訊。如需詳細資訊，請參閱 AWS CloudFormation API 參考。

您可以使用 AWS Service Catalog API 或執行步驟 1 到 4 AWS CLI。如需詳細資訊，請參閱AWS Service Catalog開發人員指南。 和AWS Service Catalog指令行參考。

管理地形開放原始碼產品狀態錯誤

Terraform 開放原始碼ProvisionProduct失敗會路由至TAINTED狀態，以允許每個佈建的產品繼續執行。UpdateProvisionedProduct發生這種情況時：

- UpdateProvisionedProduct不會嘗試更新或更正標籤，也不會嘗試建立或修改資源群組。
- UpdateProvisionedProduct決定是否應將佈建的產品設定為AVAILABLE或時，不會考慮先前佈建作業的失敗TAINTED。

AWS Service Catalog僅在期間套用標籤ProvisionProduct。因ProvisionProduct作業失敗而導致的任何失敗標籤都不會自動解決。

狀態錯誤範例

範例 1：在期間AWS Service Catalog不建立資源群組 ProvisionProduct

在以下案例中，即使沒有支援的資源群組，且沒有套用任何標籤至資源，您的已佈建產品仍處於AVAILABLE狀態。

1. 您的動作會啟ProvisionProduct動。
2. Terraform 佈建引擎會回ProvisionProduct應工作流程失敗，但不提供. ResourceIdentifier
3. ProvisionProduct工作流程不會建立資源群組，然後將已佈建的產品狀態設定為ERROR。
4. 然後啟動作UpdateProvisionedproduct業。
5. Terraform 佈建引擎會回應指出「成功」。
6. 因此，UpdateprovisionedProduct工作流程會將已佈建的產品狀態設定為AVAILABLE，但不會建立資源群組，也不會嘗試套用任何標籤。

範例 2：在期間AWS Service Catalog建立新資源 UpdateProvisionedProduct

在以下案例中，即使新資源沒有套用任何標籤，您仍然擁有已佈建產品的AVAILABLE狀態。

1. 您的動作會啟ProvisionProduct動。
2. Terraform 佈建引擎會回應指出「成功」並提供. ResourceIdentifier
3. ProvisionProduct工作流程會建立資源群組，並將標籤套用至所有已識別的資源。
4. 您可以UpdateProvisionedProduct在建立新資源的新成品上啟動。
5. Terraform 佈建引擎會回應指出「成功」。
6. UpdateProvisionedProduct工作流程會將已佈建的產品狀態設定為，AVAILABLE但不會嘗試將任何其他標籤套用至新資源。

狀態錯誤解決

AWS Service Catalog確保為設定為「TAINTED來源」的所有佈建產品建立資源群組ProvisionProduct。如果 Terraform 佈建引擎未傳回ResourceIdentifier，或AWS Service Catalog無法建立資源群組，則佈建的產品會設定為ERROR狀態，強制您終止。

管理地形開放原始碼產品狀態檔

每個 Terraform 開放原始碼佈建的產品都有一個單一狀態檔案。佈建的產品與其狀態檔案之間有 1:1 的關係。這些檔案會存放在名為的 Amazon S3 儲存貯體中sc-terraform-engine-state-${AWS::AccountId}-${AWS::Region}。狀態檔案會儲存在AccountID或ProvisionedProductID物件索引鍵下。

狀態檔案存取僅限於`GetStateFile`AWS Lambda和 Amazon EC2 啟動範本。 AWS Service Catalog管理員無法直接存取 Amazon S3 中的狀態檔案。管理員必須使用 Amazon EC2 存取檔案。依預設，AWS Service Catalog管理員可以看到狀態檔案清單，但無法讀取或寫入檔案內容。只有 Terraform 佈建引擎可以讀取或寫入檔案內容。

在 AWS Service Catalog 中管理標籤

AWS Service Catalog 提供標籤，讓您可以分類資源。有兩種類型的標籤： AutoTags 和 TagOptions。

AutoTags 是標籤，可識別中已佈建資源來源的相關資訊，AWS Service Catalog並自動套用AWS Service Catalog至已佈建的資源。

TagOptions 是在中管理的鍵值對AWS Service Catalog，用作建立AWS標籤的範本。

主題

- AWS Service Catalog AutoTags
- AWS Service Catalog TagOption 圖書館

AWS Service Catalog AutoTags

> **Note**
>
> AWS Service Catalog不支援 AutoTags 地形開放原始碼產品。

AutoTags 是標籤，可識別中已佈建資源來源的相關資訊，AWS Service Catalog並自動套用AWS Service Catalog至已佈建的資源。

AutoTags 包含產品組合、產品、使用者、產品版本和佈建產品的唯一識別碼的標籤。此項目提供一組標籤，反映客戶在目錄中設定的 AWS Service Catalog 結構。 AutoTags 請勿計入客戶的 50 標籤限制。

> **Note**
>
> AWS Service Catalog不支援 AutoTags 地形開放原始碼產品。

AWS Service Catalog AutoTags 有助於為您的資源提供一致的標記，這在設定產品組合、產品或使用者的預算時非常有用。您也可以使用 AutoTags 來識別啟動後作業的資源，例如設定AWS Config規則。 AutoTags 您可以在用於佈建的下游服務 (例如 Amazon EC2 和 Amazon S3) 的下游服務的「標籤」區段中檢視已佈建資源。AWS CloudFormation

> **Note**
>
> AWS Service Catalog套用 AutoTags 至佈建的資源 AutoTags 後，不會更新。如果您將已佈建的產品更新為不同的產品、已佈建的成品或新的啟動路徑，則現有產品 AutoTags 仍會顯示原始值。

AutoTag 細節

- aws:servicecatalog:portfolioArn – 啟動佈建產品之產品組合的 ARN。
- aws:servicecatalog:productArn – 啟動佈建產品之產品的 ARN。
- aw: 服務目錄：provisioningPrincipalArn-建立已佈建產品之啟動設定主體 (使用者) 的 ARN。
- aws：服務目錄：provisionedProductArn-佈建的產品 ARN。
- aws：服務目錄：provisioningArtifactIdentifier-原始佈建成品（產品版本）的 ID。

AWS Service Catalog TagOption 圖書館

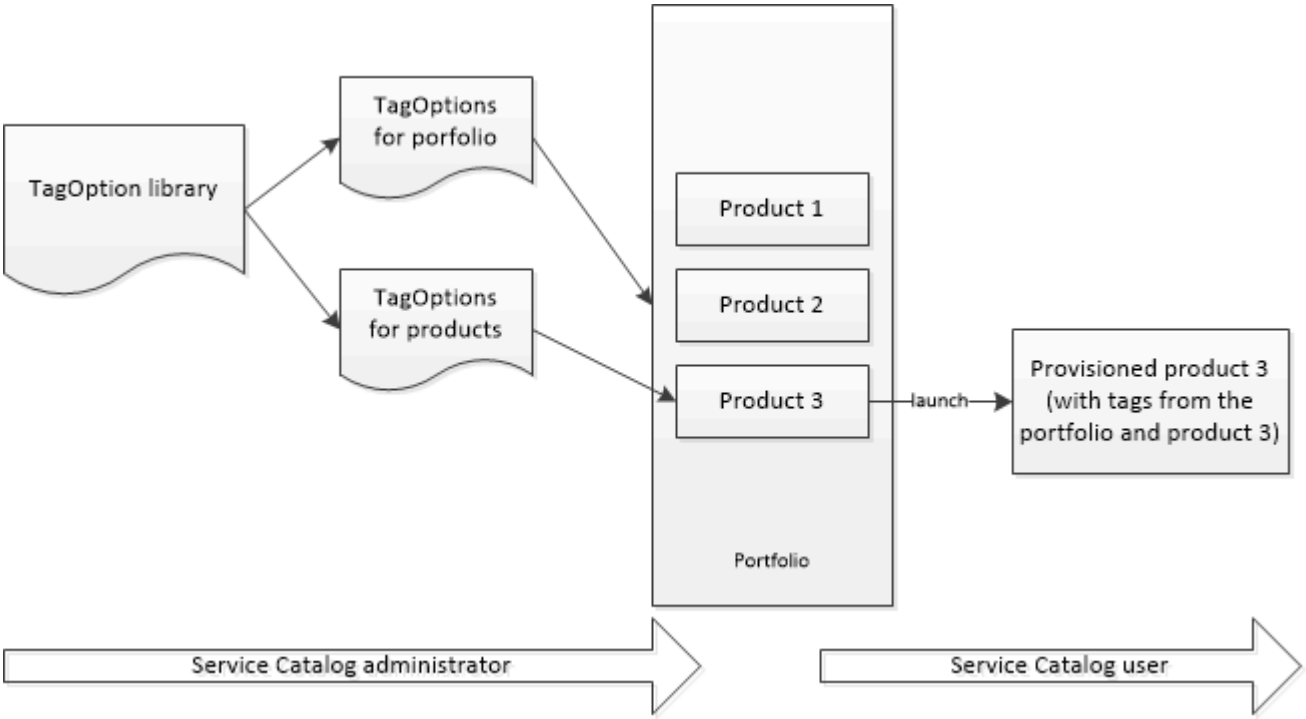
為了讓管理員能夠輕鬆管理已佈建產品的標籤，請AWS Service Catalog提供 TagOption 程式庫。A TagOption 是在中管理的AWS Service Catalog鍵值對。它不是AWS標籤，而是做為基礎建立AWS標籤的範本 TagOption。

AWS Service Catalog不支援 TagOptions 地形開放原始碼或地形雲端產品。

該 TagOption 庫可以更輕鬆地執行以下操作：

- 一致的分類
- 針對 AWS Service Catalog 資源建立適當的標記
- 針對允許的標籤定義使用者可選的選項

管理員可以 TagOptions 與產品組合和產品相關聯。在產品啟動 (佈建) 期間，AWS Service Catalog彙總相關聯的產品組合和產品 TagOptions，並將其套用至已佈建的產品，如下圖所示。



透過資 TagOption 料庫，您可以停用 TagOptions 並保留其與產品組合或產品的關聯，並在需要時重新啟用它們。這種方法不僅有助於維護庫的完整性，還允許您管理可 TagOptions 能間歇性使用或僅在特殊情況下使用的內容。

您可以使 TagOptions 用AWS Service Catalog主控台或程式 TagOption 庫 API 進行管理。如需詳細資訊，請參閱 Service Catalog API 參考。

目錄

啟動產品 TagOptions

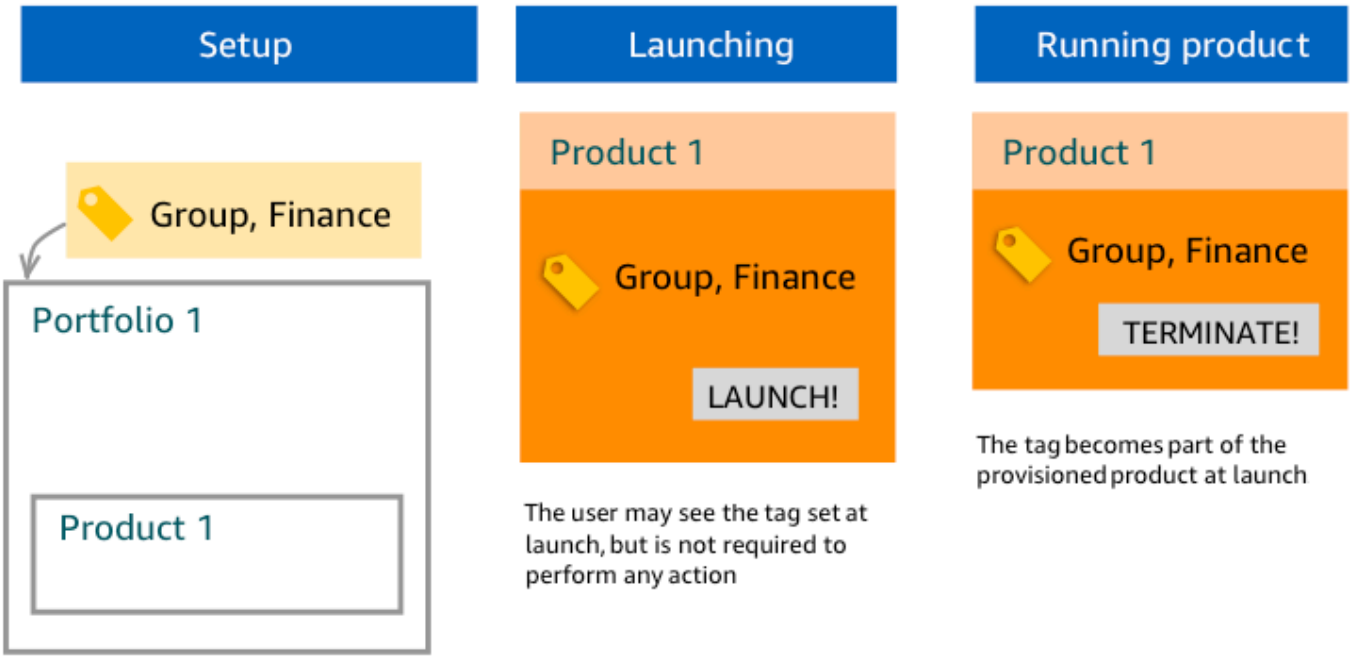
當使用者啟動具有的產品時 TagOptions，AWS Service Catalog會代表您執行下列動作：

- 收集所有 TagOptions 的產品和發射產品組合。
- 確保僅 TagOptions 在佈建產品的標籤中使用唯一金鑰。使用者會得到金鑰的多重選擇值的清單。在使用者選擇值以後，此值就會變成佈建產品上的標籤。
- 允許使用者在進行佈建時，將不衝突的標籤新增到產品。

下列使用案例示範啟動期間的 TagOptions 運作方式。

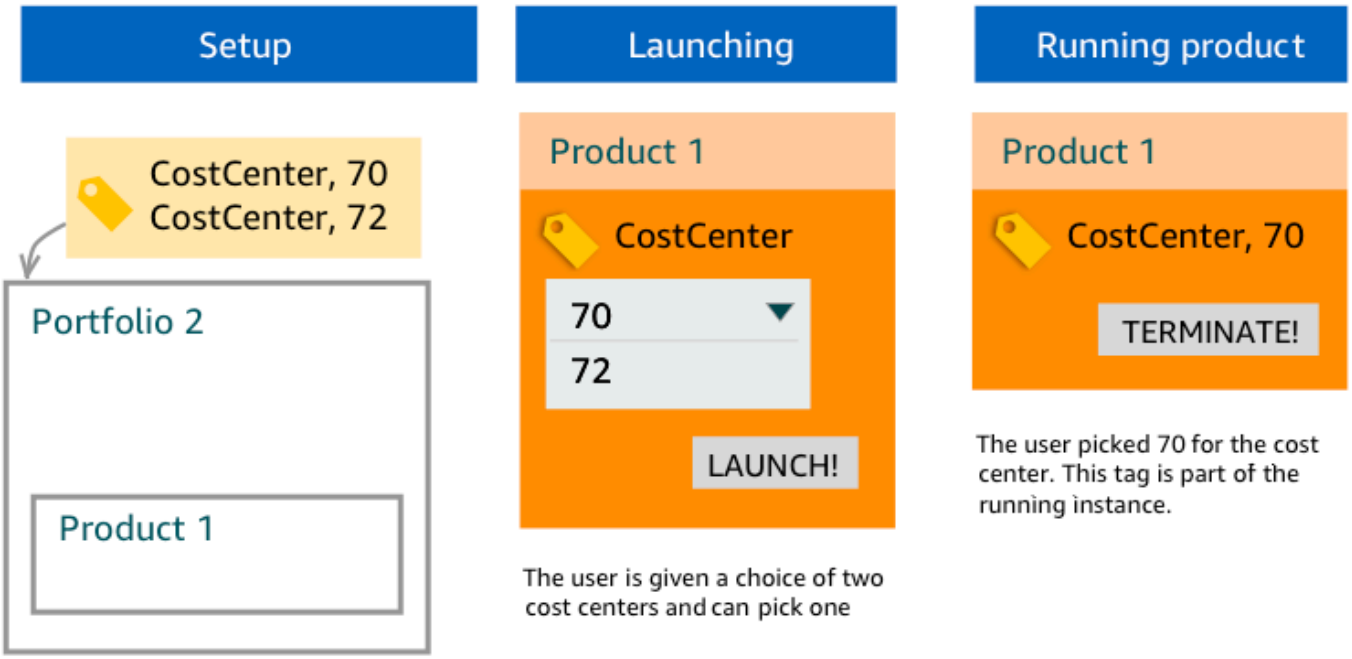
範例 1：唯一 TagOption 金鑰

管理員會建立 TagOption[群組 = 財務]，並將其與產品組合 1 產品 1 產品 1 產生關聯，但沒有。TagOptions當使用者啟動已佈建的產品時，單一產品 TagOption 會變成「標籤 [群組 = 財務]」，如下所示：



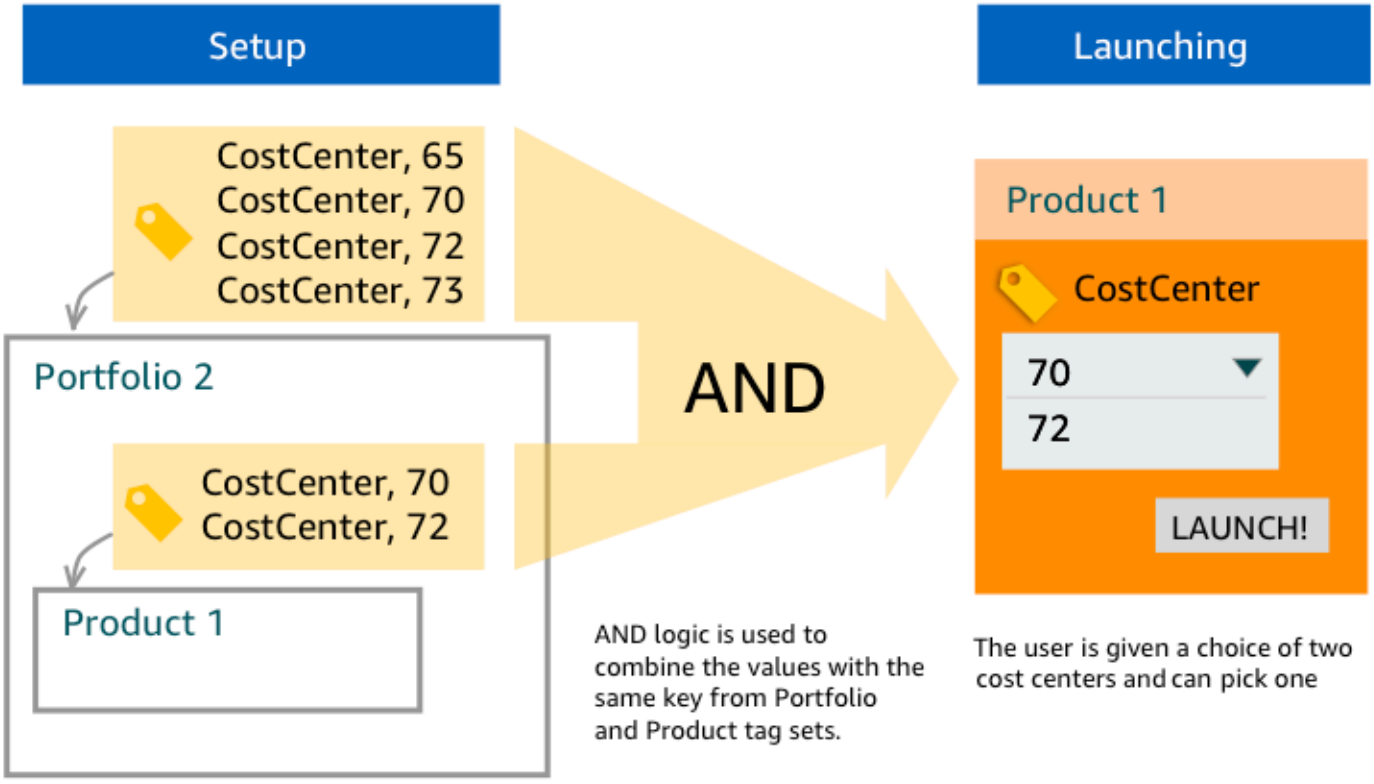
例子 2：投資組合中 TagOptions 具有相同密鑰的一組

管理員在產品組 TagOptions 合中放置了兩個具有相同金鑰的產品，而該產品組合中的任何產品都沒有 TagOptions 使用相同金鑰。在啟動時，使用者必須選擇兩個值的其中一個，來與該金鑰建立關聯。然後就會以該金鑰和使用者所選取的值，來做為佈建產品的標籤。



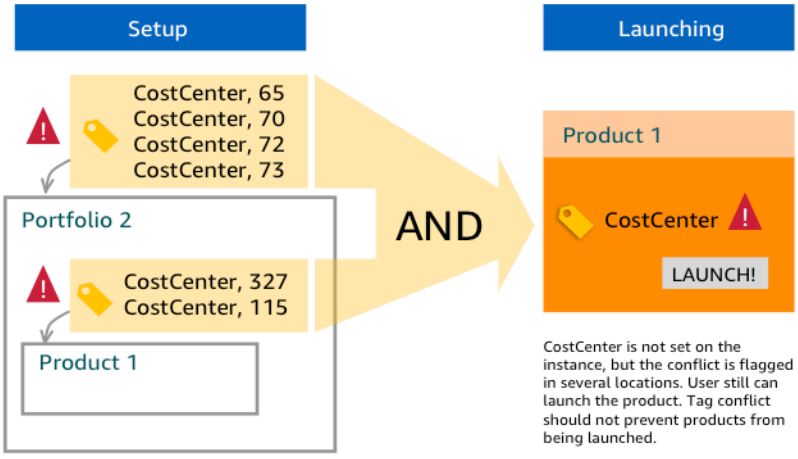
例子 3：一組在投資組合和該投資組合中的產品 TagOptions 具有相同密鑰的

管理員在產品組合中放置了多個 TagOptions 使用相同金鑰的產品組合，而且在該產品組合中也有幾個 TagOptions 擁有相同金鑰的產品。 AWS Service Catalog從的彙總 (邏輯 AND 運算) 建立一組值 TagOptions。當使用者啟動產品時，會看到這組值並從中選擇。然後就會以該金鑰和使用者所選取的值，來做為佈建產品的標籤。



範例 4： TagOptions 具有相同索引鍵和衝突值的多個

管理員在一個產品組合中放置了幾個 TagOptions 具有相同金鑰的金鑰，而且在該產品組合中也有幾個 TagOptions 使用相同金鑰的產品。 AWS Service Catalog從的彙總 (邏輯 AND 運算) 建立一組值 TagOptions。如果彙總功能找不到金鑰的值，則 AWS Service Catalog 會使用相同的金鑰和 `sc-tagconflict-`*`portfolioid`*`-`*`productid`* 的值來建立標籤，其中 *`portfolioid`* 和 *`productid`* 是產品組合與產品的 ARN。這可確保佈建的產品是使用正確的金鑰來做為標籤，而且管理員可以找到和修正其值。



管理 TagOptions

身為管理員，您可以執行下列動作以在物件 TagOptions 庫 TagOptions 中管理：

- 建立和刪除
- 啟用或停用
- 關聯或取消關聯
- 編輯

在主控台 TagOptions 中建立

1. 在 https://console.aws.amazon.com/servicecatalog/ 開啟 Service Catalog 主控台。
2. 在左側導覽選單中，選擇「TagOptions資料庫」。
3. 在 [建立新的] 中 TagOption，輸入機碼和值，然後選擇 [新增]。

   建立新 TagOption 項目之後，會依鍵值配對分組，並在清單中依字母順序排序。TagOptions

   若要 TagOption 使用 AWS Service Catalog API 建立，請參閱CreateTagOption。

在主控台 TagOptions 中刪除

1. 在 https://console.aws.amazon.com/servicecatalog/ 開啟 Service Catalog 主控台。
2. 在左側導覽功能表中，選擇 [TagOptions 資料庫]，然後選擇 [動作]。
3. 選取刪除並確認刪除。

TagOptions 在主控台中啟動或停用一或多個

1. 在 https://console.aws.amazon.com/servicecatalog/ 開啟 Service Catalog 主控台。
2. 在左側導覽功能表中，選擇 [TagOptions 資料庫]，然後選擇 [動作]。
3. 若要啟動，請選擇 TagOption 您想要的非作用中。然後選擇「動作」並從下拉式功能表中選取「啟用」，然後確認您的選取。

   若要停用，請選擇 TagOption 您想要的作用中。然後選擇「動作」並從下拉式功能表中選取「停用」，然後確認您的選取。

若要在主控台中建立一或多個產品組 TagOptions 合的關聯或取消關聯

1. 在 https://console.aws.amazon.com/servicecatalog/ 開啟 Service Catalog 主控台。
2. 在左側導覽選單中，選擇學檔，然後開啟您要建立關聯或取消關聯的學檔。
3. 選擇索TagOptions引標籤，然後選取一或多個 TagOptions 要與學檔產生關聯或取消關聯。
4. 選擇動作。然後選取「關聯」或「取消關聯」並確認您的選取。

若要在主控台中將一或多個產品 TagOptions 與產品建立關聯或取消關聯

1. 請在以下位置開啟AWS Service Catalog主控台：https://console.aws.amazon.com/servicecatalog/。
2. 在左側導覽功能表的「管理」下，選擇「產品」。然後開啟您要關聯或取消關聯的產品。
3. 選擇索TagOptions引標籤，然後選取一或多個 TagOptions 要與學檔產生關聯或取消關聯。
4. 選擇動作。然後選取「關聯」或「取消關聯」並確認您的選取。

> **Note**
>
> 若要使用 AWS Service Catalog API TagOptions 與產品組合或產品建立關聯，請參閱AssociateTagOptionWithResource。
> 若要 TagOptions 使用 AWS Service Catalog API 移除 (取消關聯)，請參閱DisassociateTagOptionFromResource。

在控制台 TagOptions 中編輯值

1. 在 https://console.aws.amazon.com/servicecatalog/ 開啟 Service Catalog 主控台。
2. 在左側導覽選單中，選擇「TagOptions資料庫」。
3. 選擇一個 TagOption 並打開值。(此值會超連結。) 然後選擇 Edit (編輯)。
4. 在「值」欄位中，編輯值並選擇「儲存變更」。

TagOptions 搭配AWS Organizations標籤原則使用

本主題提供的AWS Organizations和 TagOptions 標籤原則的簡要概觀AWS Service Catalog。它還建議如何在同時使用這兩個功能時防止標記衝突。

TagOptions 適AWS Service Catalog用於套用至佈建的產品 (CloudFormation堆疊)，而標籤原則AWS Organizations適用於AWS帳戶和組織單位 (OU) 或組織根目錄。例如，如果您將標籤原則附加至 OU，則相同的標籤原則會套用至該 OU 中的所有帳戶。如果您同時使用這兩個標記功能，則應對其進行配置，以使其不會發生衝突。

標籤政策

標籤策略可讓您定義如何在中的帳號中使用AWS資源標籤的規則AWS Organizations。您可以使用標籤策略來建立和維護一致的方法，以在帳戶層級標記AWS資源。

標籤策略提供了一種簡單的方法，可確保使用者套用一致的標籤、稽核標記資源，以及維護適當的資源分類。您也可以定義標籤鍵的大寫方式，以及您要允許的值。例如，您可以要求帳戶中的所有 EC2 執行個體都必須將標籤金鑰集為**`CostCenter`**和該標籤的值為**`Data Insights`**或**`Marketing`**。

標籤策略可讓您選取強制執行標記規則的選項、防止標記不相容作業，以及指定強制套用的資源類型。如果您未選擇強制執行選項，標籤原則可讓您建立或變更不相容的標籤，但在主控台中將其報告為不符合標籤。AWS Organizations

如需有關如何設定帳戶層級標記強制執行的詳細資訊，請參閱中的標籤政策AWS Organizations。

TagOptions

TagOptions 是一種標記功能，如果已佈建的產品AWS Service Catalog套用至相關產品，則套用至 CloudFormation 堆疊層級的已佈建產品。 AWS Service Catalog提供 TagOptions 資料庫，您可以在其中定義要與AWS Service Catalog產品相關聯的索引鍵值配對。當您啟動AWS Service Catalog產品時，您必須選擇與該產品組合或產品相關聯的現有 TagOption 金鑰 TagOption 值，才能啟動該產品。由於您是 TagOptions 在產品組合或產品層級設定，因此您可以強制執行一致的分類法，以標記跨帳戶和區域共用的產品組合。

如需有關如何在 TagOptions 中設定的詳細資訊AWS Service Catalog，請參閱AWS Service Catalog TagOption 元件庫。

避免標AWS Organizations籤政策和 AWS Service Catalog TagOptions

如果您為組織中的帳戶設定AWS Organizations標籤原則，建議您執行下列動作：

- 與同時管理產品組合和產品的管理 TagOptions員共用符AWS Service Catalog合標籤的需求。
- 與一般使用者共用符合標籤的需求，這些使用者可能會在其產品發佈中啟動產品，AWS Service Catalog並將選用的使用者標籤附加到其產品發佈時。

假設您想要在中啟動使AWS Service Catalog用金 TagOption 鑰的產品`city`，而且您的標籤政策要求標籤鍵具`city`有美國城市的標籤值，例如**`AtlantaSan Francisco`**、或**`Austin`**。 AWS Service Catalog不允許您在未為產品所需 TagOption 金鑰選取 TagOption 值的情況下啟動產品。

在此情況下，如果您具有包`city`含南美洲城市的 TagOption 金鑰 TagOption 值，例如**`Rio de Janeiro`**或**`Buenos Aires`**，AWS Service Catalog將不會啟動產品。相反地，您必須在啟動期間選取包含美國城市的 TagOption 值，以符合標籤政策。

下表提供的案例說明如何解決您 TagOptions 在使用標籤原則的同時可能遇到的標記衝突問題。

案例	原因	解決方案
如果在標籤原則中核取了標籤強制執行，則產品因為不符合標籤而無法啟動。	TagOptions 使用您尚未新增至標籤原則中允許的合規標籤清單中的金鑰和值來指定。 新增不符合標籤原則的選擇性自訂標籤。	如果您在標籤原則標籤金鑰大寫強制執行中設定特定的大小寫結構描述，請確定您的 TagOptions 標籤金鑰和選用的自訂標籤金鑰與您在標籤原則中指定的內容一致。 請注意，如果在標籤原則中取消勾選標籤金鑰大寫強制方塊，則會導致所有小寫標籤金鑰都符合規範，並確保您的 TagOptions 標籤金鑰和選用的自訂標籤金鑰與您在標籤原則中要求的內容保持一致 (例如全部小寫)。
由於不符合標籤密鑰大寫，產品無法啟動。	在 TagOptions 金鑰中指定與標籤原則大寫強制規則不一致的大寫。	正確設定標籤原則。如果您未指定標籤鍵大寫符合性，則預設的標籤金鑰大寫全部為小寫。 此外，如果您未在標籤原則中指定標籤金鑰大小寫符合性，請確定中的 TagOptions 標籤

案例	原因	解決方案
		金鑰全部AWS Service Catalog為小寫，以符合強制規則。 如果您使用的標籤原則未啟用大小寫符合性，則該標籤原則只會將所有小寫標籤金鑰視為相容。
由於標籤值不相容，產品無法啟動。	針對不在您的 TagOptions 標籤原則標籤值符合性允許清單中的產品發佈選取標籤值。	關聯 TagOptions 至您的產品和產品組合，這些產品和產品組合與您在清單標籤原則標籤值合規允許的標籤值中所需的內容一致。

AWS Service Catalog 中的監控

您可以使用 Amazon 監控AWS Service Catalog資源 CloudWatch，Amazon 將原始資料收集並處理AWS Service Catalog成可讀指標。這些統計資料記錄會保留兩週，讓您可存取歷史資訊，且能更清楚服務的執行方式。AWS Service Catalog 指標資料會在 1 分鐘期間內自動傳送至 CloudWatch 。如需有關的詳細資訊 CloudWatch，請參閱 Amazon CloudWatch 使用者指南。

如需一份可用指標及尺寸的清單，請參閱AWS Service Catalog CloudWatch 度量。

監控是維護 AWS Service Catalog 及您 AWS 解決方案可靠性、可用性和效能的重要部分。您應該收集 AWS 解決方案全面的監控資料，以便在出現多點故障時更輕鬆地進行偵錯。在開始監控 AWS Service Catalog 之前，應先建立監控計畫，為下列問題提供解答：

- 監控目標是什麼？
- 要監控哪些資源？
- 監控這些資源的頻率為何？
- 要使用哪些監控工具？
- 誰將執行監控任務？
- 發生問題時應該通知誰？

監控工具

AWS 提供您可用來監控 AWS Service Catalog 的多種工具。您可以設定其中一些工具來進行監控，但有些工具需要手動介入。建議您盡可能自動化監控任務。

自動化監控工具

您可以使用 Amazon CloudWatch 警示來監控AWS Service Catalog和報告中斷情況。

CloudWatch 警示會監視您指定期間內的單一量度，並根據指定臨界值在數個期間內相對於指定臨界值的測量結果值執行一或多個動作。動作是傳送至亞馬遜簡單通知服務 (Amazon SNS) 主題或 Amazon EC2 Auto Scaling 政策的通知。 CloudWatch 警示不會僅因為處於特定狀態而叫用動作；狀態必須已變更並維持指定數目的期間。若要了解如何建立警示，請參閱建立 Amazon CloudWatch 警示。如需搭配使用 Amazon CloudWatch 指標的詳細資訊AWS Service Catalog，請參閱AWS Service Catalog CloudWatch 度量。

AWS Service Catalog CloudWatch 度量

您可以使用 Amazon 監控AWS Service Catalog資源 CloudWatch，Amazon 將原始資料收集並處理 AWS Service Catalog成可讀指標。這些統計資料記錄會保留兩週，讓您可存取歷史資訊，且能更清楚服務的執行方式。AWS Service Catalog 指標資料會在 1 分鐘期間內自動傳送至 CloudWatch 。如需有關的詳細資訊 CloudWatch，請參閱 Amazon CloudWatch 使用者指南。

主題

啟用 CloudWatch 指標

預設情況下會啟用 Amazon CloudWatch 指標。

可用的指標與維度

AWS Service Catalog傳送至 Amazon CloudWatch 的指標和維度如下所示。

AWS Service Catalog 指標

`AWS/ServiceCatalog` 命名空間包含下列指標。

指標	描述
`ProvisionedProductLaunch`	在指定期間針對給定產品和佈建成品而啟動的佈建產品數量。 單位：計數 有效統計資訊：下限、上限、總和、平均數

AWS Service Catalog 指標的維度

AWS Service Catalog將以下尺寸發送到 Amazon CloudWatch。

維度	描述
State	此維度篩選您對以此指定狀態啟動的所有佈建產品所請求的資料。這可協助您依啟動狀態將資料分類。 有效狀態：SUCCEEDED、FAILED
ProductId	此維度只篩選您針對已識別的產品 id 所請求的資料。這可協助您精確指出要啟動的確切產品。
ProvisioningArtifactId	此維度只篩選您針對已識別的佈建成品 id 所請求的資料。這可協助您精確指出要啟動的確切產品版本。

檢視 AWS Service Catalog 指標

您可以在 Amazon CloudWatch 主控台中檢視 Amazon CloudWatch 指標，該主控台提供精細且可自訂的資源顯示，以及服務中執行的任務數量。

主題

- 在 Amazon CloudWatch 主控台中檢視AWS Service Catalog指標

在 Amazon CloudWatch 主控台中檢視AWS Service Catalog指標

您可以在 Amazon CloudWatch 主控台中檢視AWS Service Catalog指標。Amazon 主 CloudWatch 控台提供AWS Service Catalog指標的詳細檢視，您可以根據需求量身打造檢視。有關 Amazon 的更多信息 CloudWatch，請參閱 Amazon CloudWatch 用戶指南。

若要在 Amazon CloudWatch 主控台中檢視指標

1. 在以下位置打開 Amazon CloudWatch 控制台 https://console.aws.amazon.com/cloudwatch/。
2. 在左側導覽中的 Metrics (指標) 區段，選擇 Service Catalog (服務目錄)。
3. 選擇要檢視的指標。

使用 AWS CloudTrail 記錄 AWS Service Catalog API 呼叫

AWS Service Catalog與 (提供中的使用者AWS CloudTrail、角色或服務所採取的動作記錄) 的AWS服務整合AWS Service Catalog。 CloudTrail 擷取AWS Service Catalog作為事件的所有 API 呼叫。擷取

的呼叫包括從 AWS Service Catalog 主控台進行的呼叫，以及針對 AWS Service Catalog API 操作的程式碼呼叫。如果您建立追蹤，您可以啟用持續交付 CloudTrail 事件到 Amazon S3 儲存貯體，包括 AWS Service Catalog. 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，您可以判斷提出的要求AWS Service Catalog、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。

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

AWS Service Catalog中的資訊 CloudTrail

CloudTrail 在您建立AWS帳戶時，已在您的帳戶上啟用。當活動發生在中時AWS Service Catalog，該活動會與事件歷史記錄中的其他AWS服務 CloudTrail 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。

如需您 AWS 帳戶中正在進行事件的記錄 (包含 AWS Service Catalog 的事件)，請建立線索。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，您還可以設定其他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，請參閱下列內容：

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

CloudTrail 記錄所有AWS Service Catalog動作。例如，呼叫`CreateProduct`和`UpdateProvisionedProduct`動作會`CreatePortfolio`在 CloudTrail 記錄檔中產生項目。

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：

- 該請求是否透過根或 AWS Identity and Access Management (IAM) 使用者憑證來提出。
- 提出該請求時，是否使用了特定角色或聯合身分使用者的暫時安全憑證。
- 該請求是否由另一項 AWS 服務提出。

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

了解 AWS Service Catalog 日誌檔案項目

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。事件代表來自任何來源的單一請求，包括有關請求的動作，動作的日期和時間，請求參數等信息。 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 `CreateApplication` API 的 CloudTrail 記錄項目。


```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "account",
        "arn": "arn:aws:iam::12345789012:user/dev-haw",
        "accountId": "12345789012",
        "accessKeyId": "keyId",
        "userName": "dev-haw"
    },
    "eventTime": "2020-09-23T21:07:58Z",
    "eventSource": "servicecatalog-appregistry.amazonaws.com",
    "eventName": "CreateApplication",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "205.251.233.48",
    "userAgent": "aws-cli/1.18.140 Python/3.6.11
 Linux/4.9.217-0.1.ac.205.84.332.metal1.x86_64 botocore/1.17.63",
    "requestParameters": {
        "name": "hawTestCT",
        "clientToken": "6f36d650-a086-47cf-810a-fbfab2f8ad33"
    },
    "responseElements": {
        "application": {
            "applicationArn": "arn:aws:servicecatalog:us-
east-1:12345789012:application/app-02ocuq2cie2328pv64ya78e22f",
            "applicationId": "app-02ocuq2cie2328pv64ya78e22f",
            "creationTime": 1600895277.775,
            "lastUpdateTime": 1600895277.775,
            "name": "hawTestCT",
            "tags": {}
        }
    },
    "requestID": "1b6ad353-3b06-421b-bcb4-00075a782762",
    "eventID": "0a2ca224-cdfd-4c4b-a4ed-163218ff5e2d",
    "readOnly": false,
    "eventType": "AwsApiCall",
```

```
    "recipientAccountId": "12345789012"
}
```

主控台品牌偏好

AWS Service Catalog可讓管理員指定帳戶的主控台品牌偏好設定。管理員可以使用主控台品牌，為各種網站元件指定公司名稱、標誌影像以及主要和次要 (重音色) 顏色。使用主控台時，管理員和使用者都可以看到這些品牌偏好設定。

主控台品牌偏好設定可增強帳戶的外觀並完成下列作業：

- 在控制台和內部應用程序之間創建無縫的視覺轉換
- 區分同一公司內不同內部團隊使用的帳戶
- 在多個環境中區分帳戶，例如開發、預備或生產環境

> **Note**
>
> 管理員會在帳戶層級指定主控台品牌偏好設定。

指定主控台品牌偏好設定

1. 在左側導覽選單中，選擇「偏好設定」。
2. 針對淺色模式或深色模式品牌偏好設定選擇 「編輯」。
3. 上傳「標誌」，輸入「品牌」名稱，然後選取「主要顏色」和「次要顏色」。
4. 選擇儲存。

如需AWS Service Catalog支援主機品牌化的地區清單，請參閱主機品牌AWS 區域支援。

AWS 區域支援主機品牌偏好設定

AWS Service Catalog支援下表AWS 區域所列的主控台品牌偏好設定。

AWS 區域 name	AWS 區域 身分	
美國東部 (維吉尼亞北部)	us-east-1	
美國東部 (俄亥俄)	us-east-2	

AWS 區域 name	AWS 區域 身分	
美國西部 (加州北部)	us-west-1	
美國西部 (奧勒岡)	us-west-2	
非洲 (開普敦)	af-south-1	
亞太區域 (香港)	ap-east-1	
亞太區域 (雅加達)	ap-southeast-3	
亞太區域 (孟買)	ap-south-1	
亞太區域 (大阪)	ap-northeast-3	
亞太區域 (首爾)	ap-northeast-2	
亞太區域 (新加坡)	ap-southeast-1	
亞太區域 (雪梨)	ap-southeast-2	
亞太區域 (東京)	ap-northeast-1	
加拿大 (中部)	ca-central-1	
歐洲 (法蘭克福)	eu-central-1	
歐洲 (愛爾蘭)	eu-west-1	
歐洲 (倫敦)	eu-west-2	
歐洲 (米蘭)	eu-south-1	
歐洲 (巴黎)	eu-west-3	
歐洲 (斯德哥爾摩)	eu-north-1	
中東 (巴林)	me-south-1	
南美洲 (聖保羅)	sa-east-1	

AWS 區域 name	AWS 區域 身分	
AWS GovCloud (美國東部)	us-gov-east-1	
AWS GovCloud (美國西部)	us-gov-west-1	

文件歷史記錄

此表格說明AWS Service Catalog文件的重要新增項目。

功能	描述	發行日期
AWS Service Catalog	若要瞭解 Hashicorp 對 Terraform 授權的變更，以及更新為外部產品類型，請檢閱。將現有的 Terraform 開放原始碼產品和佈建的產品更新為外部產品類型	2023 年 10 月 20 日
AWS Service Catalog	若要瞭解如何與之共用產品組合AWS Organizations並AWS Service Catalog允許同步處理AWS Organizations，請參閱AWSServiceCatalogOrgsDataSyncServiceRolePolicy政策和AWSServiceRoleForServiceCatalogOrgsDataSync服務連結角色。	2023 年 4 月 14 日
AWS Service Catalog	要了解如何管理 git 連接的產品以及允許AWS Service Catalog將外部存儲庫中的模板同步到您的AWS Service Catalog產品，請參閱AWSServiceCatalogSyncServiceRolePolicy策略和AWSServiceRoleForServiceCatalogSync服務鏈接角色。	2022 年 11 月 18 日
AWS Service Catalog AppRegistry	若要瞭解如何 AppRegistry 協助儲存您的AWS應用程式、其關聯的資源集合以及應用	2022 年 6 月 15 日

功能	描述	發行日期
	程式屬性群組，請參閱AWS Service Catalog AppRegistry。	
AWS Service Management Connector	若要瞭解適用於 Jira 服務管理的連接器 ServiceNow，請參閱AWS服務管理連接器。	2022 年 6 月 9 日
用於 Jira 服務管理的連接器	若要瞭解 Jira 服務管理連接器的更新，請參閱 Jira 服AWS務管理的服務管理連接器。	2021 年 5 月 25 日
用於連接器 ServiceNow	若要瞭解連接器的更新 ServiceNow，請參閱的AWS服務管理連接器 ServiceNow。	2021 年 4 月 7 日
用於連接器 ServiceNow	若要瞭解連接器的更新 ServiceNow，請參閱的AWS服務管理連接器 ServiceNow。	2020 年 9 月 24 日
AWS Service Quotas	若要瞭解如何使AWS Service Catalog用 AWS Service Quotas，請參閱AWS Service Catalog預設服務配額。	2020 年 3 月 24 日
入門資源庫	若要瞭解由AWS Service Catalog提供的架構良好的產品範本資料庫，請參閱 入門資源庫	2020 年 3 月 10 日
版本指南	若要瞭解產品版本指南，請參閱版本指南。	2019 年 12 月 17 日

功能	描述	發行日期
吉拉服務台用連接器	若要開始使用 Jira 服務台的連接器，請參閱 Jira AWS 服務台的服務管理連接器。	2019 年 11 月 21 日
用於連接器 ServiceNow	若要瞭解連接器的更新 ServiceNow，請參閱的AWS 服務管理連接器 ServiceNow。	2019 年 11 月 18 日
新增安全性章節	若要瞭解中的安全性AWS Service Catalog，請參閱中的安全性AWS Service Catalog。	2019 年 10 月 31 日
變更佈建產品擁有者	若要瞭解如何變更已佈建產品的擁有者，請參閱變更佈建的產品擁有者。	2019 年 10 月 31 日
新資源更新限制	若要瞭解如何使用 RESOURCE_UPDATE 限制來更新已佈建產品中的標籤，請參閱AWS Service Catalog 標籤更新限制。	2019 年 4 月 17 日
用於連接器 ServiceNow	若要開始使用的連接器 ServiceNow，請參閱的AWS 服務管理連接器 ServiceNow。	2019 年 3 月 19 日
支援AWS CloudFormation StackSets	若要開始使用 AWS CloudFormation StackSets，請參閱使用AWS CloudFormation StackSets。	2018 年 11 月 14 日

功能	描述	發行日期
自助式動作	若要開始使用自助式動作，請參閱AWS CloudFormation服務動作。	2018 年 10 月 17 日
Amazon CloudWatch 指標	若要進一步了解 Amazon CloudWatch 指標，請參閱AWS Service CatalogAmazon CloudWatch。	2018 年 9 月 26 日
Support TagOptions	若要管理標籤，請參閱AWS Service Catalog TagOption資料庫。	2017 年 28 月 6 日
匯入一個產品組合	若要匯入從其他AWS帳戶共用的學檔，請參閱匯入學檔。	2016 年 2 月 16 日
許可資訊更新	若要授與終端使用者主控台檢視的存取權，請參閱終端使用者的主控台存取權。	2016 年 2 月 16 日
初始版本	這是《AWS Service Catalog 管理員指南》的初始版本。	2015 年 7 月 9 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。